HUBLI ELETRICITY SUPPLY COMPANY LIMITED

(Wholly owned Govt. of Karnataka undertaking)

IT/OT/IOT SECURITY POLICY

&

CYBER SECURITY POLICY

Disclaimer

This document is strictly private, confidential, privileged and only for use by the intended recipient. The document shall not be used, disclosed, copied, published, distributed or reproduced in whole or in part without the prior written consent of Hubli Electricity Supply Company Limited (HESCOM) which may be withheld in HESCOM's sole discretion.

The information contained / opinions expressed are in good faith and while every care has been taken in preparing the document, HESCOM makes no representations and gives no warranties of whatever nature in respect of the document, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

HESCOM, its directors, personnel and/or agents shall not be liable for the use or reliance on the opinions, information and/or findings contained in the document. Additionally, under no circumstances shall HESCOM be liable for any special, direct, indirect, incidental and/or consequential damages relating to any use and/or consideration of and/or reliance upon information in the document.

HESCOM reserves the right to change this policy document at any given time.

Document Control

Policy Details	
Policy Name	IT/OT/IoT Security Policy and Cyber Security Policy for HESCOM

Policy Stakeholders	
Role	**Name**
Director (Technical)	Sri. A H Kamble
Superintending Engineer (IT & MT) & Chief Information Security Officer (CISO)	Sri. Vrushabendrappa S

Document control		
Date	**Version**	**Description**
20.12.2021	1.0	Initial version released as approved by HESCOM BoD

Approved by HESCOM BoD

Table of Contents

Approved by HESCOM BoD

Approved by HESCOM BoD

1. Background

1.1 Hubli Electricity Supply Company Limited (HESCOM), an Electricity distribution company is vested with the responsibility of providing uninterrupted and quality power to the consumers across 7 districts of Karnataka. To meet the ever-increasing needs of the consumers and to efficiently manage and optimize the business operations, HESCOM is abreast in leveraging the digital technology landscape and has deployed several Information Technology (IT), Operational Technology (OT) and Internet of Things (IoT) systems namely : RAPDRP Part-A (17 integrated modules), Non-RAPDRP web based billing software system, Paperless Office(PLO), Consumer Self-service online portals, Customer Call Centre, Biometric Attendance System, Anytime payment (ATP) Counters, Mobile Cash Counters, Solar Rooftop online services, Electric Vehicle Charging stations etc. Some of the applications are co-hosted and some are hosted on cloud. The cyber space of HESCOM is expected to grow even more in future with extension/revamp of existing services and addition of new services under various projects with emerging technologies such as Integrated Power Development Scheme (IPDS), Revamped Enterprise Resource Planning (ERP), Smart Metering, HESCOM's own Shared OFC infrastructure etc.

1.2 Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of IT, OT and IoT devices and networks. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses and critical information infrastructure in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

In the light of rapid growth of IT, OT and IoT services, providing focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, is one of the compelling priorities for the company and country at large. Such a focus necessitates creation of a suitable cyber security eco-system for the company and country, in tune with globally networked environment.

Though cyberspace has eased the living and simplified the way business is handled, Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by the involved actors. Cyber-attacks that target the infrastructure or underlying economic well-being of a nation/company can effectively hamper the business and undermine confidence in their supporting structures.

1.3 A cyber related incident of national/business significance may take any form - an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets.

Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. HESCOM's information infrastructure is part of the National Critical Information Infrastructure (CII) as defined in The Information Technology Act, 2000.

Approved by HESCOM BoD

The Information Technology Act, 2000 defines Critical Information Infrastructure (CII) as "... those computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".

1.4 Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hacktivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and safeguarding of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

1.5 Central Government organizations like National Critical Information Infrastructure Protection Center (NCIIPC), Computer Emergency Response Team – Distribution (CERT-D) and state government has mandated HESCOM and other organizations which own CII to prepare and publish policies to protect the same and hence, the IT/OT/IoT Security and Cyber Security Policy for HESCOM is prepared.

1.6 The policy is prepared by BESCOM in coordination with their IT consultants by incorporating the inputs/suggestions/recommendations provided by the renowned organizations/institutions having experience in the field of security policy and same is adopted by HESCOM.

- International Institute of Information Technology – Bangalore (IIIT-B)
- National Critical Information Infrastructure Protection Center (NCIIPC)
- Center for Development of Advanced Computing (C-DAC)
- Indian Institute of Science (IISc)

Approved by HESCOM BOD

2. Executive Summary

The policy document for HESCOM has been prepared with an intent to provide relevant direction and value to the personnel. The policy document aims to reflect the risk appetite of the HESCOM and serves to establish an associated security mind-set within HESCOM.

The first component of the policy deals with the IT/OT/IoT Security Policy that focuses on ensuring all users or landscape of the IT/OT/IoT structure within the organization's domain abide by the instructions/directions regarding the security of data and information stored digitally within the boundaries of the organization to ensure confidentiality, integrity and availability of data and information. The Information security policies laid down correlate to the objectives and controls outlined in the ISO/IEC 27001, ITIL, NERC-CIP, COBIT, etc. industry standards, with adjustments tailored to HESCOM's operating and security environment.

The second component of the policy outlines the Cyber Security policies that focuses on informing the personnel, contractors and other authorized users of the organization, of their obligatory duty to protect the technology, data and information assets of the company. The policy helps mitigating the threats to technology and information assets.

The IT/OT/IoT Security and Cyber Security landscape of HESCOM must also comply to the various tenets & sections of Indian acts & legislations and their amendments published, as applicable.

Approved by HESCOM BoD

SECTION I: IT/OT/IoT Security Policy

Approved by HESCOM BoD

3. Introduction

3.1. Purpose

HESCOM intends to develop IT/OT/IoT Security Policy to ensure all users or networks of the IT/OT/IoT landscape within the organization's domain abide by the instructions/directions regarding the IT/OT/IoT security within the boundaries of the organization.

IT/OT/IoT security is deemed to safeguard three main objectives:

- Confidentiality – data and information assets must be confined to people authorized to access and not be disclosed to others;
- Integrity – keeping the data intact, complete and accurate, and IT systems operational;
- Availability – an objective indicating that information or system is at disposal of authorized users when needed.

A fundamental requirement of an IT/OT/IoT Security Policy is the development of an Information Security Management System (ISMS) to meet the objectives for IT security. The purpose of this policy is to:

- Explain the need for IT/OT/IoT security.
- Enumerate the elements that constitute IT/OT/IoT security.
- Indicate, in broad terms, the IT/OT/IoT responsibilities of the various members.
- Establish and organize IT/OT/IoT Security Governance framework through a set of policy statements

3.2. Scope

The policy is intended to apply as a high-level policy document to HESCOM. The areas mentioned below and covered in the policy correlate to the objectives and controls outlined in the ISO/IEC 27001 industry standard, with adjustments tailored to HESCOM operating and security environment

1) **Security Policy** – Describes the need and methodology to protect HESCOM's information and technology assets to ensure compliance with regulatory and contractual obligations and any additional national policies, standards and local security policies.

2) **Organisation of IT security** – The management of security within HESCOM, encompassing the state-wide security model framework; third party access to HESCOM resources and security requirements for outsourced service providers.

3) **Asset Management** – classification and security of HESCOM information assets and systems, including data classification.

Approved by HESCOM BoD

4) **Physical and Environmental Security** – building access control, clear desk policy, laptop security - with the overall aim of ensuring adequate protection of the information and technology assets that reside within HESCOM.

5) **Access Control** – to ensure that correct and appropriate access is assigned to HESCOM's information and technology assets based upon a data classification scheme and assigned roles and responsibilities.

6) **Information Systems Acquisition, Development and Maintenance** – development and maintenance of information systems to ensure adequate security controls are included during the conceptual design phase.

7) **Security Incident Management** – controls that must be implemented to ensure minimum impact to HESCOM in the event of a security breach.

8) **Business Continuity Management** – business continuity and disaster recovery planning based upon service level agreements and recovery time objectives with the overall aim of ensuring minimal impact to the HESCOM's business in the event of a disaster.

9) **Compliance** – outlines controls that measure and monitor compliance of HESCOM's processes and systems to ensure the compliance with this policy and other relevant security controls as agreed via the policies and standards process. Includes additional controls required to determine compliance with applicable regulations and legislation such as data protection specified in the IT Act 2000 and subsequent amendments thereof.

3.3. Need for IT/OT/IoT Security

Confidentiality of information is mandated by common law, formal statute, explicit agreement or convention. Different classes of information warrant different degrees of confidentiality. The hardware and software components that constitute HESCOM's IT/OT/IoT assets represent a valuable investment that must be protected.

The threats associated to IT/OT/IoT assets may be human, natural, accidental or deliberate. Some of which include:

1. Error
2. Fraud
3. Malicious Software
4. Embezzlement (Theft or misappropriation of funds)
5. Sabotage (deliberately damage or destroy)
6. Terrorism
7. Espionage (spying)
8. Privacy Violation
9. Service Interruption
10. Natural Disaster

Approved by HESCOM BoD

11. Hackers

Therefore, it is essential to develop a baseline security program across HESCOM. Core areas pertaining to Information security including Physical Security, Data protection, Business continuity planning, Intellectual Property & data protection, access control, regulatory compliance and user awareness are addressed through the program.

3.4. Elements of IT/OT/IoT Security

"Security" can be defined as "the state of being free from unacceptable risk". The risk concerns losses in the following categories:

1. Confidentiality of Information – refers to the privacy of personal or HESCOM related information. This includes issues of copyright.
2. Integrity of data - refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.
3. Protection of Assets – The assets that must be protected include:
    a. Computers and Peripheral Equipment.
    b. Communications Equipment.
    c. Computing and Communications Premises.
    d. Supplies and Data Storage Media.
    e. System Computer Programs and Documentation.
    f. Application Computer Programs and Documentation.
    g. Any other Information asset.

3.5. IT/OT/IoT Security Policy Framework

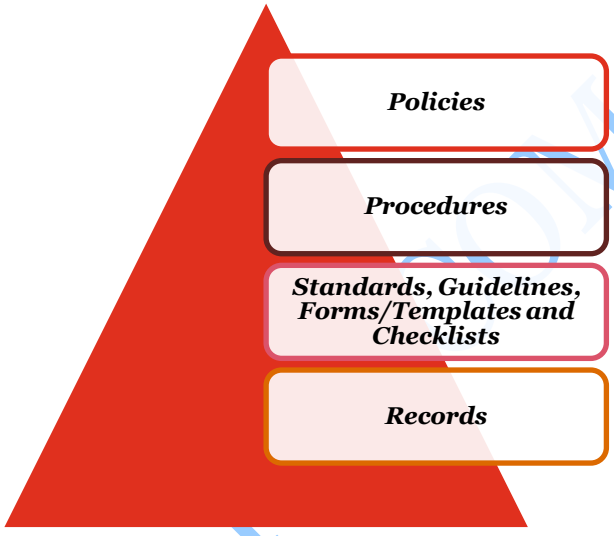
A security policy is the essential basis on which an effective and comprehensive security program can be developed. The primary purpose of a security policy is to inform all users of the essential requirements for protecting various assets including people, hardware, and software resources, and data assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy. This also allows for the subsequent development of operational procedures, the establishment of access control rules and various application, system, network, and physical controls and parameters.

This policy will deal with the following domains of security:

Approved by HESCOM BoD

1. ***Computer System Security:*** CPU, Peripherals, OS. This includes data security.
2. ***Physical Security:*** The premises occupied by the IT/OT/IoT team personnel and equipment.
3. ***Procedural Security*** by IT/OT/IoT team, vendor, management personnel, as well as end users.
4. ***Communications Security:*** Communications equipment, personnel, transmission paths, and adjacent areas

The various layers in the document are:



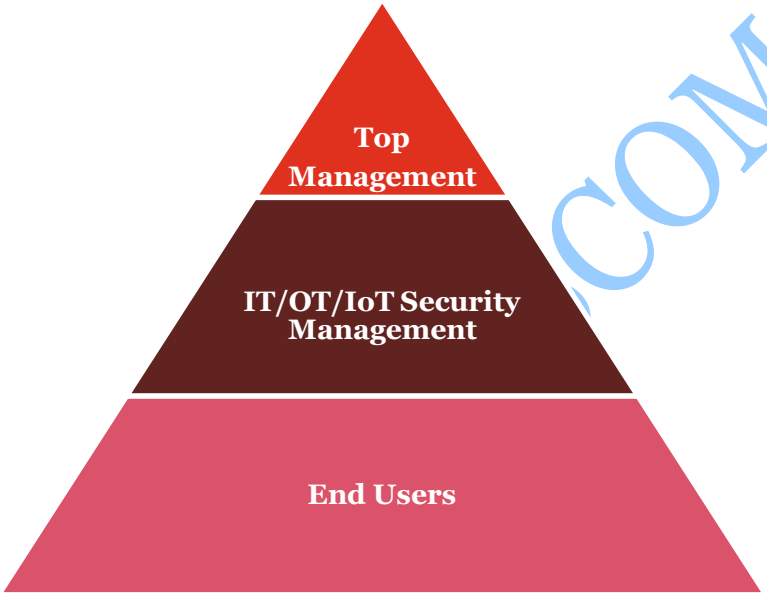
1. ***Policies*:** Policies are overall declarations of organization intent for information security. They would also be in accordance with the IT Act 2000 and the subsequent amendments. A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities. Policies set out the HESCOM's position on, and responsibilities for, IT/OT/IoT team Security and state the overall results required. They are mandatory throughout all the verticals of HESCOM.
2. ***Procedures***: Specific step-by-step instructions to carry out a process in compliance with the policies. Procedures are mandatory for particular processes; but also, can be used as examples to build other procedures.
3. ***Standards, Guidelines, Forms/Templates and Checklists***:
   - Standards shall be introduced as applicable based on the information security policies to establish the baseline/benchmark for the technical/operational procedures against which the compliance could be measured uniformly.
   - Guidelines are suggestions for carrying out the activities stated in the procedures.
   - Forms and Templates shall be used to document the execution of the activity.
   - Checklists are triggers to ensure that the activities in the procedures are effectively carried out

Approved by HESCOM BoD

4. ***Records:***
    - Records are tangible objects or digital information
    - Record is defined as a document or other data that is regarded as complete and unchangeable. It may exist as paper, as a scanned image or electronically. They are evidence of an organization's activities

3.6. Policy Stakeholders

An ideal information security organization will typically have three levels:



1) ***Top Management*** - The people who approve the security policy and security budgets; review the security implementation efforts, take note of the effectiveness of various measures and decide on the priorities. Involvement of top management will induce the organization to take security matters seriously.

   HESCOM officials may explicitly delegate the executive responsibilities and accountability to the Chief Information Security Officer (CISO) of HESCOM and respective Information Security Managers of the system. In case of any breach in policy, HESCOM shall take measures as per the regulations of IT Act, 2000 and subsequent amendments.

2) ***IT/OT/IoT security Management*** – IT/OT/IoT Security Management within HESCOM should be comprised of the following people and teams. These people or teams can be drawn from the personnel or some of these activities can be outsourced to suitable third parties.

    a. **Security Policy Owner(s):** People with good knowledge of business and IT/OT/IoT must author and own the security policies, in order to make policies practical and enforceable.

Approved by HESCOM BoD

b. **Security Maintenance Team**: This team should consist of core IT/OT/IoT, Information Science technical experts. The responsibility of this team is to understand various security alerts issued by manufacturers or independent security organizations. They should assess the need for implementing the requisite patches after proper testing. This team should also track exploits that could be used to expose the vulnerabilities faced by organizations due to new weaknesses revealed by either manufacturers or various security organizations like SANS, CERT, NCIIPC and Security Focus etc. This team should comprise of IT/OT/IoT/IS technology experts with specialized knowledge of various security measures. The team should also be responsible for reviewing various logs like firewall logs, intrusion detection system logs and detecting if there has been an attack on the organization.

c. **Security Incidence Response Team**: This team should decide the steps to be taken in case of an incident/attack/penetration. They should try to identify, isolate and contain the incident to ensure that it does not spread to other devices or units. The security incidence response team may also have to liaise with local law enforcement bodies, Internet service providers, and telecommunication bodies for better coordination during a crisis.

d. **Disaster Recovery Team**: The disaster recovery team should be involved in keeping the disaster recovery plans ready and periodically test them so that they are not outdated when needed.

e. **Security Training Team**: The responsibility of this team is to provide security awareness training at all levels in the organization. This team could also be made responsible to prepare do's and don'ts, security awareness posters, security competitions, observing security week, anti-virus day and all such things, which keep security in the limelight.

3) ***End Users***: End users include officers, employees on the payroll and others acting in a similar capacity, such as consultants, trainees, contract employees etc. Any user failing to comply with the security policies could be subject to disciplinary action as per the company regulation.

This policy document takes into consideration the below four categories of users in HESCOM:

1. HESCOM Management
2. Corporate Users
3. IT/OT/IoT Core Users
4. Field Users

The most effective attacks to end users on information are social engineered attacks. A con artist posing as an authorized person can get any information, including passwords from unsuspecting end users.

Other areas of concern are noncompliance of the security policies. Organization may have framed elaborate policies about e-mail, Internet connections and so on, but if end users do not observe these policies, they may put information security to risk.

Approved by HESCOM BoD

End users and all in the IT/OT/IoT team must be informed about their job responsibilities, the information security policy and the penalties for breaching the policy. Non-disclosure agreements, confidentiality agreements, password secrecy policy etc. should be part of the appointment letter. This will create seriousness about information security and also help if an investigation needs to be done to probe a cyber-crime.

This IT/OT/IoT Security Policy shall be reviewed and updated as and when required or at least once in a year.

Approved by HESCOM BoD

4. IT/OT/IoT Security Policies

4.1. Password Policy

Objective

The following policy shall be considered as the minimum baseline password policy for implementation across all IT/OT/IoT infrastructure and applications in HESCOM. Stringent criteria above the baseline for management of passwords shall be followed for specific business requirement.

Scope

The below policies are applicable to all HESCOM officers/employees.

Policies

Users shall strictly adhere to the password policy as described below:

	User Level Policy
1.	Users shall maintain the confidentiality of passwords.
2.	Users shall create a password of minimum 8 characters.
3.	Users shall create passwords with alphanumeric characters with a minimum of one numeric and one special character.
4.	Users shall ensure weak and easily guessable passwords (example- yourname@123 or HESCOM@123) are not used.
5.	Users shall change password every 90 days
6.	Users shall not use any option such as “Remember Passwords” in any application (at the end user machine or at application level itself) for convenience purposes.
7.	User is responsible for every transaction carried out using their login account.
8.	Users shall use different credentials for business and non-business purposes.

Approved by HESCOM BoD

9.	User shall not type in or read aloud passwords/PINs when others are nearby.
10.	User shall not Disclose passwords/PINs to anyone (including service desk/helpdesk engineer) who may approach claiming he/she needs it for some exigent purposes.
	System Level Policies
11.	The maximum password age i.e. the length of time that users can keep a password before changing it, should be set to a value of 90 days.
12.	System should prevent users from using last 5 passwords while changing password. Users are not allowed to reuse the last five (5) old passwords in his account towards enhancement of the security to maintain the effectiveness of password history by enabling the minimum password age security policy settings.
13.	Password audit should be conducted to track all password changes. This will help them to track potential security problems. This will also ensure user accountability and provide evidence in the event of security breach.
14.	E-mail notifications should be created prior to password expiry to remind users when it's time to change passwords before it actually expires.
15.	All HESCOM systems shall automatically lockdown after five unsuccessful password attempts on it by any user.

Approved by HESCOM BoD

4.2. Email Policy

Objective

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications. The purpose of this email policy is to ensure the use of HESCOM email system only for official communications and make users aware of what HESCOM deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the HESCOM Network.

Scope

The below policies are applicable to all HESCOM officers/employees.

Policies

	User Level Policies
1.	All officers/employees must use their own official email ids to send or receive messages; however, as per business requirement message-forwarding feature can be used.
2.	All third-party e-mail services (like Gmail, Rediff mail etc.) are strictly prohibited for any official communication by all officers/employees
3.	Users shall not involve in initiating or propagating spam emails.
4.	Officers/Employees must treat all electronic mail messages as private information.
5.	Users shall not use their Emails to Forward or send messages that have racial or sexual slur, political or religious solicitations, or any other message that is in-appropriate and/or has the potential to cause harm or embarrassment to HESCOM.
6.	Officers/Employees are supposed to report offensive email messages to the sender/ their supervisors
7.	Files containing classified information when sent as e-mail attachments should be password protected. The password should be sent/given to the recipient through phone or in a separate SMS or email.
8.	Defaming abusing, harassing, stalking, threatening or otherwise violating any legal and privacy laws through electronic mails is prohibited
9.	Users are prohibited from automatically forwarding email to a third-party email system such as Google, Yahoo etc. Individual messages which are forwarded by the user must not contain confidential information or any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Approved by HESCOM BoD

	Admin Level Policies
10.	All emails should have a legal disclaimer notice at the end of the mail content
11.	All emails should be scanned for selected keywords, file-types and other information as found necessary.
12.	Formal exchange policy needs to be maintained related to Password, IP Schema and Network Diagram etc.
13.	All attachments to an electronic message to be limited to 30 MB size.
14.	All mailboxes to have a minimum capacity as follows: All officers/employees below manager/AEs/AAOs level - 500 MB DGMs/EEs/DCAs, AGMs/AEEs/AOs, Managers/AEs/AAOs– 1 GB Managing Director, Directors, CS, CGMs/CEEs/FAs, GMs/SEs/CAs- 2 GB
15.	All HESCOM confidential data contained within an email message or an attachment must be encrypted (TLS encryption)/password protected before transmission.
16.	Email should be retained only if it qualifies as a HESCOM business record. Email is a HESCOM business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
17.	If the mailbox size reaches 90% of the threshold limit, then it must be archived. The archival may be done by user using the Archival option available in the e-mail system of HESCOM. Auto-archival policy may also be enabled by IT team of HESCOM if required in some cases.
18.	Email that is identified as a business record shall be retained according to Record Retention Schedule of Govt. Of India.
19.	Auto save of password in the HESCOM email service shall not be permitted.
20.	In case an email contains encrypted/password protected attachment, there should be an alert message provided to the user since the attachment can't be scanned for malicious content. The

Approved by HESCOM BoD

	user should avoid downloading it unless he knows the sender and is confident that this email is legitimate.
21.	Deactivation of an account means that the account can no longer be accessed. All e-mails sent to a deactivated account shall bounce to the sender.
22.	HESCOM shall publish valid SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance) records in its DNS (Domain Name System) server for email exchange so that the email spoofing can be prevented
23.	The spoofed and malicious emails shall be analyzed, and the IP addresses of the source may be added into the local blacklist of the organization.
24.	In case of any suspicion about the received email, the identity of the sender should be verified by alternate communication channel other than email
25.	Malicious URLs in the incoming emails shall be sanitized in order to protect the email users
26.	IMAP/POP access from outside the HESCOM network/domain may be disabled for security reasons
27.	Email account access should be revoked immediately after the resignation, retirement and re-employment of the officers/employees

4.3. Internet Policy

Objective

To provide rules and guidelines about the appropriate usage of company equipment, network and internet access.

Scope

The below policies are applicable to internal HESCOM users.

Approved by HESCOM BoD

Policy

1.	Users are prohibited from using HESCOM systems and internet resources for personal use
2.	All access to internet (exception of official electronic mail) must be approved from respective department heads in writing in advance.
3.	Unless authorized by supervisor/senior officer, users are forbidden from using HESCOM information systems and participating in internet discussion groups, chat groups, public electronic forums
4.	Respective users shall be held accountable for the information downloaded from the internet.
5.	All materials downloaded from the internet should be checked for virus signatures, malicious code, Trojans, spyware etc.
6.	Users are not allowed to misrepresent their identity on internet while using the HESCOM information systems
7.	Access to internet sites that are deemed inappropriate in office include categories related to Adult contents, pornographic sites, violence, games & gambling, special interest groups, trading and personal emails. Categories are subject to change based on evolving internet sites.
8.	HESCOM will routinely log all web sites visited, times spent on site, web usage, and files downloaded by users
9.	Source code must always be encrypted before being sent over the internet.
10.	Credit card numbers, log-in passwords, and other parameters that are sensitive and can be misused by hackers, must not be sent over the Internet in readable form.
11.	Access to proxy websites (Web Proxy), internet websites hosting the torrent files, audio files, video files and other malicious software shall be blocked.
12.	No free and open-source software shall be downloaded and installed without prior permission of competent authority
	Web browser Security
13.	Users should clear browser cache periodically to flush potentially damaging information. It can be done manually or automatically such as when closing the browser

Approved by HESCOM BoD

14.	Users should only be using licensed browser for web browsing.
15.	Passwords should not be automatically saved in browser
16.	Auto-fill should be turned-off for any confidential or personal details
17.	Third Party Cookies should be disabled entirely, or only enabled if user visits a trusted site that requires them
18.	Plug-ins/Add-ons should be blocked from running automatically, or the browser should ask each time a website wants to install or run a plugin/add-on
19.	Pop-up Windows should be blocked from running automatically, or enabled only for trusted websites and/or have the browser ask each time a site wants to open a window
20.	Flash ads should be prevented from playing until the user specifically allows them
21.	Scripts on websites must be blocked until the user specifically enables them

4.4. Data Security Policy

Objective

Rules and guidelines about the transmission, storage and disposal of confidential/restricted/private/sensitive data. Privacy, Sensitivity and Confidentiality of data is as defined in Data Sharing policy of HESCOM.

Scope

The below policies are applicable to all internal HESCOM users.

Policy

1.	The Data sharing policy of HESCOM shall be followed while sharing the data pertaining to HESCOM with any external stakeholders.
2.	Department heads must identify and maintain a current list of vital records that are needed to restore the normal operation of their individual departments in case of a disaster
3.	Sensitive information pertaining to HESCOM can only be downloaded from a multi user system to a personal computer (PC) or a workstation only when the following two conditions

Approved by HESCOM BoD

	are met: i. The data transfer must take place for a clear business need, AND, ii. Advance permission from the information owner is obtained.
4.	Unauthorized Users are prohibited in taking backups of critical files in USB drives or any other available media.
5.	Disposal of electronic media (hard drives, CDs/DVDs, tapes, etc.) , hardware devices etc. should be done in caution and under the supervision of concerned HESCOM authority to ensure that no information is transferred to unauthorized users by any means.
6.	In case of replacement/disposal of any kind of media/hardware, appropriate sanitization mechanism such as overwriting storage space on the media with non-sensitive data, Degaussing and destruction by Disintegration, Pulverization, Melting, Incineration and Shredding may be undertaken. This is applicable to the following types of media: a. Hard Copy Storages: Paper and microfilms b. Hand-held devices c. Networking devices d. Magnetic disks such as hard drives, SCSI drives, USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives e. Magnetic Tapes f. Optical Disks such as CDs, DVDs g. Memory such as Compact Flash Drives, SD, RAM, ROM

4.5. Anti-Virus Policy

Objective

HESCOM is responsible for appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

Scope

Approved by HESCOM BoD

This policy applies to all IT/OT/IoT assets that HESCOM is responsible to manage. This explicitly includes any system for which HESCOM has a contractual obligation to administer. This also includes all server systems setup for internal use by HESCOM, regardless of whether HESCOM retains administrative obligation or not.

Policy

HESCOM operations staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate

A.	***Anti-Virus Deployment and its integration with other tools***
1.	Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.
2.	Implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralised management and monitoring.
3.	In a networked environment, an antivirus server must be deployed and all HESCOM workstations should have corresponding antivirus client. All the clients must be configured from the central antivirus server for routine tasks such as scheduled scanning of the client workstations and updation of antivirus signatures. The management of the client workstations must be done centrally from the antivirus server in order to have a centralized monitoring of all the activities.
4.	IT/OT/IoT Security Team must identify all the possible entry points in the network through which a virus attack is possible and all the traffic entering the network through these points should be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP, FTP, SMTP or POP3. This ensures that the risk of any virus entering the network by any means is greatly reduced.
5.	It is also recommended that firewall with Anti-virus support be installed for additional security for the network
6.	All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions: • Non-administrative users have remote access capability • The system is a file server • NBT/Microsoft Share access is open to this server from systems used by non-

Approved by HESCOM BoD

	administrative users • HTTP/FTP access is open from the Internet • Other "risky" protocols/applications are available to this system from the Internet at the discretion of the Security Administrator • Outbound web access is available from the system
7.	***Mail Server Anti-Virus***: If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.
8.	***Anti-Spyware***: All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions: ▪ Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet ▪ Any system where non-technical or non-administrative users have the ability to install software on their own
B.	***Technical Controls and System Admin level Policies***
1.	The latest version of the antivirus with the latest signature is required to be loaded in all the machines of the organization. This is important as new and more potent viruses are discovered every day and even a few months old antivirus program may be ineffective against newer viruses.
2.	For standalone PC's the anti-virus software should be automatically enabled for checking viruses.
3.	For a networked environment, there must be a central server to check for viruses in all the machines automatically.
4.	There must be a scheduled full-scan of the PC's: a. Server: Daily b. Workstations: Daily. The scan shall be scheduled when there is minimum human interactions with the work station.
5.	The anti-virus software should auto-update signatures automatically from the service providers as and when an update of signature or virus engine is available.
6.	Since all online viruses arrive from the internet, a good antivirus software should be loaded at the logical gateway of the network.
7.	The latest patches for web browsers should be applied or else simply visiting a compromised web site can cause infection.

Approved by HESCOM BoD

8.	If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
9.	Always keep patch level up-to-date, especially on computer that host public services and are accessible through the firewall. Such as HTTP, FTP, mail and DNS services.
10.	Anti-virus logs should be maintained for a period of 10 days. Ideally a weekly analysis of the logs should be done to obtain an infection profile of viruses and the machines infected
11.	In the case of a virus attack the following steps are required to be taken - a) The network share of the machine has to be stopped and disconnect/isolate the infected machine from the network. b) The contact person for cleaning the machine of virus has to be notified c) There must be a mechanism where an authorized expert/work station is notified automatically in case of a virus attack.
12. .	The mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block or remove email that contains attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr, .ssh, .applescript files.
13.	Do not allow user to execute software downloaded from internet unless certified safe by system administrator
14.	All network shared folders must have restricted access (read/write permissions should be given only to intended users and admin)
C.	***User Level policy***
1.	All officers/employees must scan all external media (CD/ Pen drives/ Removable drives) for viruses before use in HESCOM environment. IT Team shall place controls to prevent auto-run of the devices.
2.	Users shall refrain from opening emails from malicious and unknown sources.
3.	Malware incidents shall be escalated through appropriate channels efficiently, and malware contained, investigated and removed as securely as possible

Approved by HESCOM BoD

4.6. Physical Security Policy

Objective

To provide rules and guidelines about security of physical assets.

Scope

The policies are applicable to all IT/OT/IoT assets maintained by HESCOM

Policy

1.	Critical business and sensitive information processing facilities shall be protected with appropriate security barriers and/or access controls.
2.	Sensitive areas (server rooms, communication equipment rooms etc.) shall be located away from public access and protected in locked rooms to prevent tampering and unauthorized usage.
3.	All information storage media (hard drives, magnetic drives, floppy drives, CD ROM's etc.) and portable laptops containing sensitive information must be physically secured when not in use.
4.	Documents and media containing the sensitive or critical information shall be secured by storing in lockers or safes. Access to sensitive areas shall be granted on a "need to enter" basis.
5.	All movement of office materials (desktop materials, FAX machines, LAN servers, network hubs etc.) must be approved from the involved GM (ICT & MIS).
6.	All HESCOM computer centers must be equipped with fire, water, and physical intrusion alarms that automatically alert concerned personnel to take remedial action
7.	Sensitive areas shall be protected from fire, flood, explosion, civil unrest, or any other man-made disaster.
8.	Sensitive areas shall be located away from public access and protected.
9.	All incoming and outgoing material shall be inspected by Security guard for potential hazards with the help of existing technology

Approved by HESCOM BoD

Note: All user access privileges and login access to be revoked within 24 hours in case of personnel separation from HESCOM. For personnel joining in, access will be provided with approval from manager, and every user will be provided with a user ID with limited access as needed by business.

4.7. Process Policy

Objective

To provide process related guidelines in case of security incidents as well as proactive measures by HESCOM users to prevent such incidents

Scope

The below policies are applicable to all HESCOM officers/employees.

Policy

1.	Any computing system that is used for conferences, meetings, related activities inside HESCOM premises should have an owner who is an officer/employee of HESCOM and should be responsible for the data/information and safety of the system itself.
2.	All officers/employees (officers, employees, consultants, contractors, temporaries etc.) must be provided with sufficient training and reference material to allow them to properly protect HESCOM's information resources.
3.	Every officer/employee must understand HESCOM's policy and procedures about information security and must agree in writing to perform his/her work according to such policies and procedures.
4.	All suspected information security incidents must be immediately reported as quickly as possible through the correct internal channels.
5.	All apparent software malfunctions must be immediately reported to line management or the vendor/ administrator responsible for managing that software.
6.	Responsibility for Information Security on a day to day basis is every officer's/employee's responsibility.
7.	Every HESCOM multi user computer system (including LAN's) must have a designated security administrator to define user privileges, monitor access control logs, and perform similar activities

Approved by HESCOM BoD

4.8. Administrator Policy

Objective

Establishes acceptable use of Administrator Policy for HESCOM. Provides requirements and guidelines to System Admins for the ethical and acceptable use of their administrative access and the tasks required to be performed.

Scope

The below policies are to be implemented by all System administrators in HESCOM.

Policy

1.	Prior Approvals are necessary for all User-ID creation. a) New user id creation: approval from immediate supervisor. b) Access to business application systems: approval from information owner c) Installation of software on operational systems d) Advanced system access: approval from head of the department
2.	All privileges to HESCOM information systems & programs should be restricted on a need to know basis
3.	Multiuser system administrators must have two user IDs, one for privileged access and should be logged; other ID can be a normal user ID for day to day work of a normal user
4.	Usage of administrator and administrator equivalent account privileges to be allowed only from selected and secured workstations
5.	All user ID must automatically have all privileges revoked after 30 days period of inactivity
6.	Users must be clearly informed as to what all actions constitute security violation and users must also be informed that all such security violations will be logged
7.	Information security department must establish, maintain and periodically test the communication system in place that allows other officers/employees to promptly notify any information security incidents like; virus infestations, hacker break-ins, disclosure of internal information to outsiders, system service interruptions and other events with serious information security implications.
8.	The internal system addresses, configurations and systems design of HESCOM systems must have a restricted access from unauthorized usage.
9.	A clear backup periodicity of all the identified critical documents, programs and data as identified in HESCOM must be defined. The backup process must be carried out as per the defined periodicity which should never exceed one-month time frame.

Approved by HESCOM BoD

10.	Periodic testing of the backup process and the backed-up data must be carried out by the administrator.
11.	Backups of essential business information, software's, programs must be stored in an environmentally secure access-controlled site that is at a sufficient distance away from the production system so as to escape a local disaster
12.	The admin passwords of all the servers should be written and kept in sealed envelopes in a safe fireproof place under lock and key.

4.9. User and Work Station Security Policy

Objective

To provide guidance for workstation security for HESCOM workstations in order to ensure the security of information the workstations may have access to.

Scope

This policy applies to all officers, employees, contractors, workforce members, vendors and agents with a HESCOM-owned or personal-workstation connected to the network.

Policies

1.	Workforce members using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.
2.	Each workstation used to support multiple simultaneous users or to provide file and print sharing services are considered servers and must run approved server operating system software.
3.	Reporting of Inappropriate or Unauthorized Use - Users suspecting any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to concerned security official
4.	Protection from Malicious Software - Users must use and keep active current versions of HESCOM's approved malicious software scanning tools to detect and remove malicious software from workstations and files. Users must not disable these tools unless specifically

Approved by HESCOM BoD

	directed by systems support personnel to do so in order to resolve a particular problem.
5.	Users will use the access control features supported by the workstations. This includes, but is not limited to, the use of User ID and password controls, password protected screen savers and appropriate logical access permissions for files and other computer resources.
6.	A user must protect and use their individual User ID and password. A user is responsible for all activity performed using their User ID. Users must not disclose or share User IDs and passwords. A user may hand over his credentials to designated/identified individual as part of transfer of charge. In such scenario, the user taking over the charge is responsible to change their account credentials immediately.
7.	Workstations that have critical information must have password-protected screen savers with an inactivity time-out period approved by the HESCOM Security team. Inactivity time-out periods shall not exceed 1 minute for workstations in publicly accessible areas and in no case shall exceed 15 minutes. Users must either log off or activate the password protected screen saver whenever their personal computing device is left unattended.
8.	Appropriate measures must be taken to protect workstations from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.
9.	Users must protect workstation software from theft, unauthorized use, and/or unauthorized copying. Diskettes, CDs, and other removable media containing software programs must be locked in secure file cabinets or desks when not in use.
10.	Keeping food and drink away from workstations in order to avoid accidental spills.
11.	Installing privacy screen filters or using other physical barriers to alleviate exposing data.
12.	Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
13.	Exit running applications and close open documents
14.	If wireless network access is used, ensure access is secure by following the Wireless Communication policy

Approved by HESCOM BoD

15.	The personal computer (desktops, laptops) connected to the network should be locked/logged off when unattended.
16.	All shared folders over a network should be password protected.
17.	No games must be stored or played on a HESCOM workstation
18.	All official computers and workstations should only be used for business purpose. All personal uses must be through approved permissions from SEE(IT&MT)
19.	Users are prohibited from installing/upgrading software's on their workstations, network servers and other machines without prior approval from CISO (Chief Information Security Officer)
20.	HESCOM documents, software, and any internal information must never be sold or transferred to any third party (Non-HESCOM user) for any purpose other than business needs. For every other requirement an authorization would be necessary in advance and shall adhere to HESCOM Data Sharing Guidelines for this.
21.	In case of loss of sensitive information or its suspected loss/disclosure to unauthorized parties, its owner and department heads should be notified immediately.
22.	HESCOM information systems users are prohibited from gaining unauthorized access to any other information systems or in any way damage, alter, disrupt the operation of these services.
23.	Every HESCOM information system user must have a unique user id and password for system access
24.	In case of transfer, retirement, promotion, suspension and untimely death of an officer/employee, IT team shall revoke user privileges and deactivate the account on immediate basis.

Approved by HESCOM BoD

4.10. Network and Firewall Security Policy

Objective

To provide policies for implementing a robust and secure IT/OT/IoT infrastructure in HESCOM. Provides guidelines that needs to be implemented to provide protection from threats such as malware, intrusions and zero-day threats. This helps prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources

Scope

The below policies are applicable to HESCOM IT infrastructure at various divisions and sub-divisions.

Policy

1.	All critical servers accessible via internet must be protected by security equipment such as firewall, etc.
2.	All internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls in a demilitarized zone.
3.	All firewall configuration rules and permissible service rules must not be changed without an approval from the department head.
4.	All connection between HESCOM's internal networks and the internet must only be through an approved firewall and related access controls.
5.	All firewalls should be regularly audited and updated as per new requirements
6.	Changes to firewalls, enabled services, and suspicious activities should be always logged, and the logs should be monitored periodically
7.	Intrusion detection systems should be installed at the firewall to monitor external hacking attempts & to monitor changes within the firewall itself.
8.	A process should exist for monitoring vulnerabilities of the firewall and get new upgrades of the firewall and patches of the firewall.
9.	Have mechanisms to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by HESCOM
10.	Security Operation Centre needs to be setup to monitor the health of enterprise system(DC, DR, network and endpoints)
11.	Deception Technologies like Honeypots should be implemented to detect, analyse, and defend against zero-day and advanced attacks in real time.

Approved by HESCOM BoD

12.	Periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the HESCOM's network including in Data Centres, in third party hosted sites, shared-infrastructure locations.
13.	Boundary defences should be multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network--based IPS and IDS. Mechanism to filter both inbound and outbound traffic to be put in place.
14.	Secured rooms should be provided for the firewalls and physical access to the secured rooms should be restricted and tightly controlled
15.	Network should be segmented into proper subnets.
16.	VLANs must be enabled in all the switches.
17.	All inbound and outbound traffic must be monitored
18.	All suspicious network activities must be monitored and blocked.
19.	All network entry points to HESCOM must be firewall protected and all firewall logs need to be monitored daily. Content inspection must also be enabled at all network entry points.
20.	The content inspection policy should not track government confidential documents and all activities have to be monitored daily
21.	Bandwidth utilization reports should be generated and logged
22.	All ISP entry points must be kept under firewall, IDS and antivirus protection
23.	VPN and dialup connectivity should be provided to external users to connect to HESCOM's information systems
24.	The gateway must be integrated with the antivirus wall.
25.	Appropriate mechanism or a Network Operation Centre (NOC) shall be established in order to ensure the network availability all the time
26.	Critical networks should be redundant in order to ensure the high availability of the networks, in case of any attack or failure
27.	There shall be no single point of failure in the networks. Therefore, networking and security hardware devices shall be redundant
28.	The logs of the networking and security devices shall be analyzed on real-time basis in order

Approved by HESCOM BoD

	to detect and mitigate possible threats and compromises within the network.
	Security Controls for OFC Network Sharing
29.	Separate network domains to be maintained for different clients while sharing OFC networks.
30.	ACLs and firewalls to be put in place to ensure the HESCOM traffic is isolated from other tenant traffic.
31.	Rate limits to be established across the devices to ensure protection in case of one tenant device/network is compromised.

Security Operations Centre (SOC):

Security Operations Centre (SOC) is a team of expert individual and the facility in which the staff deals with security issues on an organizational and technical level. It improves security incident detection through constant monitoring and analysis. HESCOM may establish SOC to prevent cyber security threats and detects and responds to any incident on the computers, servers and networks. It shall carry out the following activities broadly:

1. SOC shall collect, monitor and analyze data feeds from the various security devices/critical servers/selected client machines of its constituents for the purpose of situational awareness, threat forecasting and efficient incident response.
2. The SOC will have the right combination of resources in terms of people, process and technology to conduct necessary analysis for early detection of anomalies and provide customized threat feeds to HESCOM
3. The SOC will act as a central node for collection, examination and preservation of relevant security logs from the Specified IT/Security Infrastructure of its constituents.
4. The SOC will have capability for use of analytical techniques by identification of potential threats and attacks.
5. SOC will have capability of automatic orchestration of incident response to security incidents received from different sources.
6. Vulnerability Management – SOC will have capability to carry out the vulnerability assessment of all its constituents and vulnerability remediation of complete IT infrastructure of HESCOM
7. Brand monitoring - SOC will have capability to monitor, analyze and mitigate malicious traffic and threats which may impact the reputation of the SOC constituents.
8. Security Assessment – SOC will be responsible to carry out a comprehensive security audit of all the tracks of HESCOM. The security audit will include a detailed review of the overall security of HESCOM on the basis of global standards like ISO 27001, NIST cyber security framework, privacy etc.

Approved by HESCOM BoD

9. The systems that NEED to be put in place as a part of the SoC requires the following aspects to be addressed.
    a. Methods to identify root cause of attacks, classify them into identified categories and come out with solutions to contain further attacks of similar types.
    b. Incident investigation, forensics and deep packet analysis need to be in place to achieve the above.
    c. Dynamic Behaviour Analysis. – preliminary static & dynamic analysis and collecting Indicators of Compromise (IOC)
    d. Analytics with good dash board, showing the Geo-location of the IP's
    e. Counter response and Honeypot services

4.11. Remote Access Security Policy

Objective

The objective of this policy is to provide controlled remote access and safeguard Information systems from unauthorized access in HESCOM.

Scope

The scope of this policy applies to all Users who are accessing HESCOM's IT resources using remote access channels.

Policies

1.	Remote access to HESCOM's IT/OT/IoT resources from public network shall be allowed only after successful identification and authentication of users.
2.	Remote access to intranet applications shall be provided only through secured communication channels such as SSL or IPSEC.
3.	Access to critical applications in the intranet shall be granted only with two (2) factor authentications.
4.	In case of user separation from HESCOM's services, user credentials shall be deleted on the last day of the user promptly by the respective Account administration personnel.
5.	VPN access to HESCOM's resources shall be authenticated by the Active Directory.

Approved by HESCOM BoD

6.	User Authentication for establishing VPN session shall be encrypted.
7.	Deny access logs on remote access service shall be monitored by Network/ Security Operations staff for taking appropriate Preventive actions.
8.	Adequate care shall be taken by mobile users when mobile computing facilities are used in public places, meeting rooms and other unprotected areas as defined in Remote access Guidelines.
9.	Trouble shooting of systems remotely by vendors & systems personnel shall be done as per remote access procedure.
10.	Remote access users shall not extend access to HESCOM Intranet resources to others such as friends or family in any form.
11.	Dial-out/Dial-in connectivity from/to the backbone as well as restricted network shall be allowed ONLY with written approval from the Network Operations Manager/Security Operations Manager.
12.	The user IP addresses shall be whitelisted prior to providing the access to critical applications in the intranet
13.	When there is a requirement to troubleshoot the systems remotely by vendors & system personnel, the IP addresses of these users shall be whitelisted for a particular period of time required for troubleshooting

Approved by HESCOM BoD

4.12. Acceptable Removal Media Usage Policy

Objective:

The objective of this policy is to minimize security risks arising out of usage of Removable Media Interfaces for portable storage devices such as USB memory sticks, pen drives, entertainment devices with data storage capacities (with USB, Bluetooth and other interfaces) etc., (herein referred as "Removable Media") within the organization and also establish usage criteria for genuine business requirements.

Scope:

This policy is applicable to all Users in the Organization, and also for all types of removable media devices. HESCOM requirements/agreements detailing the use of removable media shall supersede this baseline policy. Situations warranting the use of Removable Media devices/interfaces for business purposes shall be granted only based on HESCOM's concurrence and with due protection to information.

Policy:

1.	Removable Media ports/interfaces (USB) usage within the organization in general, shall be controlled by disabling the Removable Media Interfaces in the Desktops and Servers.
2.	All removable media devices must be declared at the security register by all users entering/ exiting the premises.
3.	Usage of personal removable media is not encouraged; however removable media may be used with laptops for legitimate business needs, only after ensuring that media is malware free and laptop is adequately protected against accidental infection from the media.
4.	All removable media devices need to be scanned for malicious threats and remove all unnecessary data prior to use further.
5.	Information/Asset owners shall be held accountable for (A) copying sensitive information in to any removable media which could cause confidentiality breach (B) causing transmission of malicious code from removable media in to HESCOM systems (C) execution of unauthorized software programs from removable media even inadvertently which could potentially lead to security incidents with business impact (D) legal Violations.
6.	User must not copy HESCOM sensitive information including but not limited to HESCOM personal contacts, Intellectual property documentation, Non-public personal information such as credit card numbers, social security numbers (Aadhaar number) etc. in to the removable media from HESCOM's assets.
7.	Information stored in removable media devices to address genuine business requirements, shall be in an encrypted format.
8.	Officers/Employees shall keep their official removable devices securely to avoid any theft or unauthorized data access.
9.	Access for enabling/usage of removable media within the server farm area / Data Centre for official purposes shall be permitted only after due authorization from HESCOM
10.	There shall be a formal process with approval from CISO and tracking mechanism for handling genuine business requirement for usage of removable media devices in Desktops, laptops and Servers.
11.	Consider implementing centralised policies through Active Directory or Endpoint

Approved by HESCOM BoD

	management systems to whitelist/blacklist/restrict removable media use.
12.	Limit media types and information that could be transferred/copied to/from such devices

4.13. Acceptable Software Usage Policy

Objective:

The objective of this policy is to

a) minimize risks related to unauthorized software usage (including but not limited to freeware) and
b) establish acceptable usage criteria related to software downloads from internet and subsequent usage of software in HESCOM.

Scope:

a) This policy is applicable to all IT/OT/IoT assets by all HESCOM Users.
b) "Software" as mentioned in the policy includes the software media and licensing components (Paper licenses or electronic keys) required for satisfactory working of the software in HESCOM's computing environment.
c) "Freeware" software as referred in this policy includes free software, shareware, and trial ware software.
d) Software meant for evaluation means trial software or software for demo purposes only and must not be considered for long term usage on production environment.

Policies:

1	***Software Procurement***
1.1	All new software (updates inclusive) required to be used at HESCOM must be purchased through HESCOM's Procurement Process.
1.2	For software purchased by HESCOM, a copy of the software and its associated licenses and media along with procurement documents must be maintained under safe custody.
1.3	Users must not resort to any type of online transactions (E.g.: usage of personal credit cards for purchasing software) to purchase and download official software (for formal usage) from the Product Vendor websites, bypassing HESCOM's procurement process.

Approved by HESCOM BoD

1.4	HESCOM resources (such as software accessed in HESCOM's IT assets) must only be used for business purposes in the course of normal business operations.
2	***Freeware/Shareware software Usage***
2.1	Freeware software, in general are potential carriers of malicious code, spy ware, worms and viruses; hence, outright download and informal installation of these software's in HESCOM's machines is prohibited considering potential security vulnerabilities to HESCOM's IT resources. However, if freeware software is required for any business purpose, then it should have prior approval from CISO.
3	***Software Download from Internet***
3.1	All software meant for evaluation, must be used only for the purpose of evaluation including but not limited to a) Gaining technical knowledge on products b) Understanding working methodology of software c) Gain general product knowledge d) Understand risks of usage of software. Subject to such usages permissible by vendor.
3.2	Software meant for evaluation must not be used for regular use in any type of production requirements.
3.3	Software provided for evaluation purpose must be uninstalled at the end of evaluation period and shall not be re-installed. Software dump shall not be retained in the system.
3.4	Freeware software available on the various internet sites for free or restricted downloads must not be downloaded inadvertently or out of inquisitiveness by Users.
3.5	Freeware software downloads through web sites or file transfers must be monitored by HESCOM for unauthorized downloads and subsequent usage.
3.6	Only HESCOM approved software must be installed in laptops. Users must refrain from installing unauthorized software while they are not directly connected to HESCOM's network. Consider implementing whitelisting of authorised applications/software libraries etc.
3.7	Users must strictly refrain from downloading and using any stealth mode software (Any hidden software which may avoid detection of its own presence or destroy evidences of system usage) which could potentially lead to a hostile working environment. Installation and Usage

Approved by HESCOM BoD

	of such software shall be considered as noncompliance to this policy.
4	***Software Usage and Tracking***
4.1	HESCOM shall track the license usage (Version levels, software accounting, and usage activity) of the software purchased by HESCOM and regulate unauthorized usage.
4.2	Software with expired licenses and pirated or personal software must not be used in the IT environment of HESCOM.
4.3	Users in HESCOM shall not download any software directly. Software shall be tested by HESCOM and authorized for use before installation.
5	***Software Usage - Audit and Compliance***
5.1	HESCOM reserves the right to audit presence of unauthorized software.
5.2	Regular audits shall be carried out using automated tools to understand the usage pattern of software & associated licenses and the type of freeware downloads.
5.3	Users shall report Security issues observed or discovered as an after effect of installation of software.
5.4	IT/OT/IoT Team shall revoke local administrative privileges of Users who do not respond to the request for uninstallation of software
5.5	IT/OT/IoT team shall continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches.
5.6	Users found in noncompliance with this software usage policy will be subjected to an investigation and appropriate disciplinary action to be taken, up to and including termination from services.
5.7	In case of a genuine business requirement, after satisfactory evaluation of the trial software,

Approved by HESCOM BoD

	Users need to take immediate steps either to formally purchase or stop the usage of the software based on the decision of usage of the software for business purposes.

4.14. Change Management and Patch/Vulnerability

Objective:

The objective of this policy is to ensure changes to systems and information processing facilities are controlled and do not adversely affect Confidentiality, Integrity and Availability of Information assets.

Scope:

This policy is applicable to Change activities in HESCOM.

Policies:

1.	Changes in any information processing facilities/systems shall be carried out in a manner that does not compromise the security of existing systems or cause any security failure.
2.	Changes to operational software such as Operating system upgrade, operating system changes, any application module upgrade, and vendor supplied software, product enhancements, recommended patches shall be controlled through change management procedure.
3.	Systems and processes shall be put in place to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.
4.	As a threat mitigation strategy, the root cause of incident needs to be identified and necessary patches to plug the vulnerabilities should be applied.
5.	Requestor, reviewer/approver and implementer responsibilities for addressing the change shall not rest with same user to ensure segregation of duties.
6.	Changes shall be planned and during execution of the change, access shall be granted only to the relevant application and systems.

Approved by HESCOM BoD

7.	Potential impact of any change shall be assessed before accepting a change request and changes shall be authorized and documented.
8.	Environment for carrying out the tests shall be separated from production environment.
9.	In HESCOM there should be separated UAT Platform for patch testing to test the all patches.
10.	Designated staging environment should be there for any development & test for departmental users.
11.	Impacted users shall be intimated before implementation of a change.
12.	Process shall be in place for recovering from 'unsuccessful' changes.
13.	Changes shall be documented; suitable version control and a change log/directory shall be maintained.
14.	Any major changes to operating systems shall be a planned activity and appropriate reviews shall be done before implementation.
15.	Emergency changes shall be analysed for the impact and shall be authorized by the asset owner / custodian. All impacted users shall be notified.
16.	Modifications to Vendor supplied products shall be discouraged. If changes are warranted, vendors shall be intimated to obtain system patches/releases and care shall be taken that security, functionality features are not getting impacted. The original software shall be retained, and changes shall be clearly documented.
17.	Changes in IT/OT/IoT Infrastructure shall be as per the Change management procedure.

Approved by HESCOM BoD

4.15. Cryptography

Objective

To protect confidentiality and integrity of sensitive information during transmission and while at rest using suitable encryption technology.

Scope

This policy will be only applicable to "types of information" identified as needing encryption controls based on organizational, regulatory and contractual requirements.

Policies:

1.	The various needs for encryption of information involved in business transactions shall be derived from (A) Information Security Risk assessment (B) Customer requirement(s) (C) Regulation/Law/Standards compliance requirement(s).
2.	Data transferred through wide area network connections between HESCOM and its Customer(s) through internet as the medium shall be adequately protected with suitable encryption technologies. HESCOM should enforce HTTPS for all the web-based applications.
3.	Based on business requirements, business sensitive & very confidential e-mails shall be encrypted before sending the same to recipients.
4.	Based on business requirements, business and/or customer sensitive and very confidential data stored on IT/OT/IoT systems and applications (including on portable digital media, backup media, and in logs) shall be encrypted.
5.	A secure method shall be adopted for key management while using encryption methodologies in the enterprise.
6.	Passwords to access private keys if any shall be adequately protected from unauthorized intrusion.
7.	Any IT/OT/IoT system utilizing encryption methodologies for protection of confidentiality of information shall be implemented based on approval from authorized personnel
8.	Depending on the business requirements, the information owner and security group shall decide a mutually acceptable encryption methodology for protecting identified critical and sensitive business information. The methodology adopted should be trustworthy in order to generate confidence in the use of information and communications systems.
9.	Import, export and use of encryption methodologies shall be in compliance with the applicable laws and regulations.
10.	Users possessing the private keys (in case of public key cryptographic methodologies) shall be

Approved by HESCOM BoD

	responsible for safety of the keys during usage.
11.	Electronic signatures shall be distributed to Users handling/wanting to access information of sensitive nature as per the information classification policy. HESCOM's data sharing guidelines may be followed regarding the same.
12.	Users shall be accountable and responsible for the transactions and safe maintenance of the electronic signatures if any assigned to them for usage.
13.	Usage of electronic signatures shall provide confidentiality, integrity, traceability and non-repudiation for the transactions involving with identified critical applications.
14.	Specific procedures shall be adopted for electronic signatures issuance, management, revocation and storage.
15.	The public and private keys generated and distributed to the User shall be unique to the User and constitute a functioning key pair corresponding to the electronic signatures.
16.	HESCOM authorized trusted authority shall have the ability to issue or revoke electronic signatures as per business requirements, on behalf of an identified Licensed Certifying Authority (CA).
17.	Encryption controls shall be implemented as required on business-critical applications accessible over internet. Cryptographic keys such as Secret key, Public & Private keys used in the critical IT/OT/IoT Systems and Applications shall be protected against disclosure and misuse.
18.	Usage of electronic signatures for electronic transactions shall be governed by the regulations like Information Technology Act 2000, issued by Government of India.

4.16. Acceptable Data Collection and Usage Policy

Objective:

The objective of this policy is to define the baseline criteria for personal information collection, mass email communication and Tele-calling activities to protect HESCOM's reputation and brand image against public complaints on unsolicited calls, SPAM emails from or on behalf of HESCOM

Scope:

Approved by HESCOM BoD

This policy is applicable to Service functions involved in:

- Mass e-mail processing & communication (using HESCOM's email domain)
- Tele-calling actions done either in-house or through HESCOM's vendors/Service providers.
- Collection of Customer/Prospect's/General public personal information in web portals by HESCOM

Prospect/Customer who subscribes to information through HESCOM websites or contacted by HESCOM as part of the actions above is here by referred in this Policy as 'Subscriber'.

Subscriber data refers to data such as but not limited to – Name, Contact information (Office and mobile telephone numbers), Address, Organization name, Areas of interest, Title, email address, Country etc.

Policies:

1	***Data Collection***
1.1	Personal data (referred as subscriber data) collected by HESCOM for carrying out business processes shall be adequately protected against unauthorized access.
1.2	While collecting personal data of subscribers on websites, (HESCOM website or any other sites on behalf of HESCOM), care shall be taken to ensure that legal/regulatory requirements if any present related to data protection are considered.
1.3	There shall be a clear-cut statement that the data collection is in accordance with the Privacy policy.
1.4	A Subscriber's email address shall be added to a mailing list only after verification of the intention of subscriber in joining the mailing list.
1.5	The initial email to the Subscriber shall clearly state why that email was received by the Subscriber from HESCOM.
2	***Processing and Communication***
2.1	Bulk e-mails must contain accurate subject lines and shall not be deceptive in nature.
2.2	Bulk e-mails must carry proper header information including originating email domain and email address.

Approved by HESCOM BoD

2.3	Bulk e-mails shall be communicated to outside world only through HESCOM approved email system.
2.4	If a Subscriber communicates to HESCOM for unsubscribing his/her email address, with immediate effect, the subscription shall be removed with notification to the subscriber, using either the website or email communication itself.
2.5	The application/system in which email/calling lists of subscribers are stored must be adequately protected against any direct harvesting attacks. The system must have the latest antivirus signature files, latest security patches for the OS including any application specific patches.
2.6	There must be a centralized internal database maintained for reference and used for mass email communication and the same must be updated as and when contact information, subscription status changes happen.
2.7	Email/Calling list must be classified as "Confidential" information and must not be shared with unauthorized parties - either internal or external to HESCOM. However, caution must be exercised while sharing the information internally for official purposes to make sure that data is protected.
2.8	When emails are required to be sent to more than one Subscriber (either one-to-one or as mass email), care must be exercised to ensure that the email is not suspiciously tagged as SPAM either by the Subscriber or the Internet Service Provider (who is relaying the emails).
2.9	If automated scripts are used for sending emails out, care must be taken that the emails reach the right contacts.
2.10	Email lists available for mass broadcast must be verified for existence from time to time, using specific tools available for the same purpose.
2.11	While involved in mass email communication from HESCOM, Changes in SPAM laws in various geographies must be considered and validated with Legal requirements.

Approved by HESCOM BoD

4.17. Data Protection and Privacy Policy

Objective:

The objective of this policy is to protect the Non-Public personal information and safeguard the information as per applicable laws and regulations. Personally Identifiable Information (PII) can be either collected by HESCOM directly or through its vendor as a part of the execution of the outsourced business processes.

Scope:

This policy is applicable to:

- All Users, facilities and IT infrastructure at HESCOM
- Critical and Sensitive data such as HESCOM's officer/employee data and/or Customer/Business partner data including personal data (Personally Identifiable Information or Non-public private information).
- Sensitive data residing in IT assets like desktops, laptops, mobile devices, removable media and servers or in any appliance.
- All Data storage, communication and Transactions.
- Intellectual property information and information classified as Confidential, Very Confidential or Internal & Restricted. [E.g.: Customer list, Key financial projections, Billing information, Source code, System/Design documents, Strategic plans etc.]

'Data' referred in this policy means:

Personal/Private information of an individual [E.g.: Personal identifiers such as Aadhaar numbers, Permanent Account Number, Date of Birth, Passport numbers, Bank Account numbers, Names, Home or mobile phone number, personal E-mail addresses, credit card numbers and personal information such as credit history, medical information, educational and professional certificates, payroll/salary information etc.]

Policies:

Compliance to globally accepted Data Protection Principles and in line with the Personal Data Protection Bill, 2019. HESCOM's data sharing guidelines may be followed wherever applicable.

1.	HESCOM shall process personal data in a fair and reasonable manner ensuring the privacy of the data principal. The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.
2.	Data must be processed for limited purposes. – Clarify Intent of processing.

Approved by HESCOM BoD

3.	HESCOM must provide a prior notice for collection or processing of personal data. The notice should include information mentioned as per Clause 7, Chapter II of the Personal Data Protection Bill, 2019
4.	HESCOM shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.
5.	HESCOM shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing.
6.	Data must be processed in line with the data subject's (End-user's) rights.
7.	HESCOM shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including— (a) use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (c) steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.
8.	Data should not be transferred to jurisdictions without adequate protection.
9.	All non-public personally identifiable information shall be considered as confidential.
10.	HESCOM shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the end user and such data processor.
11.	All non-public personally identifiable information shall be retained & disposed of as per the applicable laws, regulations & customer requirements.
12.	Confidentiality of data must be protected in electronic or physical form by Information owners & custodians in business units and service functions.
13.	Websites collecting personal information (including entities which do on behalf of HESCOM) must provide the intent of data collection, assurance of protection, option for subscription/un-subscription for end-users from whom data is collected. Visitor privacy shall be protected

Approved by HESCOM BoD

	using website privacy policy statements.
14.	Personally Identifiable Information (PII) owner shall authorize and be aware of the information collection and usage purpose.
15.	Third party contract shall have clauses defined to ensure the security and privacy of the PII.
16.	Data protection requirements must be reviewed especially during contractual sign-off with government departments on deals involving sensitive personal data access.
17.	While outsourcing sensitive work to Third party vendors or partnering with vendors especially involving processing of sensitive data must be carried out in line with the Third-party security policy.
18.	While enhancing opportunities for market intelligence and competitive advantage through personalized services to Customers using e-mail, care must be taken to make sure that Customer complaints on spam emails from HESCOM minimized
	Data Lifecycle: Protection
19.	Data must be protected during the major stages of creation, collection, storage, access, disclosure, transmission, retention and deletion.
20.	Classification of data according to the sensitivity level and business impact must be carried out as per the information classification policy and procedures.
21.	Whether accessed locally or through a remote connection, sensitive data must not be copied, moved and stored on laptops, desktops or external storage such as USB hard drives/flash drives without adequate encryption. If there is an exceptional requirement to carry the same, data must be encrypted and confidentiality protection to be ensured by Users.
22.	Users and custodians shall take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
23.	Individuals shall have access to the PII as required by them.

Approved by HESCOM BoD

24.	Users handling sensitive data must be made aware of the repercussions of breach/loss of data to HESCOM and its partners.
25.	Information security risk assessment must be conducted to assess any perceived or on-field risks related to the non-public personally identifiable information and on sensitive applications hosting data, especially hosted on internet segment considering the enhanced need for mobility and collaboration.
26.	Users shall ensure that non-public Personally Identifiable Information accessible to them is safeguarded while deciding the protection level for personally identified information, the associated legal, regulatory and statutory requirements shall also be considered.
27.	User access to personal information processing/storing application resources shall be granted based on official requirements; on a “need to access” and "need-to-know" basis only and the authorization shall be obtained as defined in the application access control matrix as approved by the respective stakeholders.
28.	Audit trails shall be maintained for creation, access and deletion of sensitive data by Information owners.
29.	Appropriate steps should be taken to mask email-ids for display, storage and transmission.
	Data Loss Prevention – Monitoring
30.	Necessary technology controls for monitoring loss of sensitive data through commonly used communication channels like E-mail, Instant Messaging and Internet connection from HESCOM network to outside must be implemented depending on the official requirement.
31.	Workplace monitoring shall be carried out in accordance with privacy laws/regulations with the aim to protect HESCOM sensitive information as per contractual agreements / legal & regulatory requirements.
32.	Any loss/breach/unauthorized access of sensitive data processed by HESCOM must be reported by Users through the Security Incident Reporting process.

Approved by HESCOM BoD

33.	In line with contractual commitments and local regulatory requirements (as applicable), Customers shall be notified of any incident related to breach/loss of data
34.	Information Security Audit shall be carried out to assess the control implementation & effectiveness to safeguard the non-public personally identifiable information

4.18. Acceptable Handheld Devices Usage Policy

Objective

The objective of this policy is to reduce risks related to access and management of information [such as official emails] through handheld devices and to help users take precautionary measures while using handheld devices.

Scope

This policy is applicable for –

1. HESCOM officials who have been provided handheld devices as well as self-purchased devices.
2. Adherence by all Users authorized for accessing and managing information including email through handheld devices.
3. Usage of any type of handheld devices like smart phones, blackberry devices, Personal Device Assistants, Spot Billing Devices, pager, any mobile device with an embedded operating system enabling remote connectivity/storage/ synchronization features.
4. Users shall abide by the Internet & email policy in HESCOM while accessing emails from handheld devices as well.

Policy

1.	***Information Access***
2.	HESCOM shall control information access to handheld devices based on identified users, supported mobile device model & technology solutions.
	User Responsibilities for Self-Purchased Handheld Devices
3.	Users shall be solely accountable for the loss of information from the handheld devices, in case of a theft or loss of device.

Approved by HESCOM BoD

4.	Users shall take due care (Informing GM(IT)/GM(Proc)) of the handheld devices against theft of devices.
5.	Users shall necessarily use a power-on password in their handheld device as the first level protection measure.
6.	Users shall store information which is confidential/very confidential or covered by a privacy or regulatory act, in an encrypted manner ONLY, as per official needs.
7.	Users shall remove any HESCOM specific or customer specific information from their handheld devices in the presence of a HESCOM superior officer, while resigning from organization and surrender the handheld devices, if issued by HESCOM.
8.	User shall keep switched off the unnecessary connectivity options like Bluetooth, Wireless LAN, and Infrared by default and enable on need basis.
9.	User shall not send official sensitive information through short message service offered by telecom operators.
10.	Officers/Employees must not leave their personal computers, laptops, notebooks with a modem turned on.
	Policies for handheld devices issued by HESCOM
11.	Any handheld devices issued by HESCOM shall be used for official purposes and shall be loaded with approved software only.
12.	Officials shall refrain from using social media platforms, IM platforms on their handheld devices etc. using HESCOM user ID, or phone number issued by HESCOM.
13.	All changes to hardware, software, configuration on the telecommuting machine should only be made after prior approvals from the IT department and should be monitored.
14.	All telecommuting machines/laptops/ portables/ notebooks of HESCOM are for the exclusive use of the officer/employee/ person to whom it has been given hence sharing or access or passwords is prohibited.
15.	HESCOM IT team should enforce OS updates in the handheld devices.
16.	HESCOM provided mobile devices should not be synchronized to other personal devices of the official
17.	Officials should not use cloud-based apps or backup that allows HESCOM related confidential data to be transferred to unsecure parties.
18.	Upon termination of the officer/employee, mobile devices should be reset to factory defaults

Approved by HESCOM BOD

	and handed over to IT Team.
	Loss and Theft
19.	Users shall be necessarily aware of the immediate actions and reporting mechanism in case of a loss or theft of handheld device.
20.	If in case of a reported loss or theft of handheld device for a specific User, the user credential shall be changed immediately on reporting the incident to IT Team.
	HESCOM Responsibilities
21.	HESCOM shall ensure the handheld security setting on all handheld devices for effective management and control of security and data protection policies.
	Management of Personal Devices connecting to corporate network
22.	Enabling of time out automatic locking of personal device when not being used for 5 minutes where applicable.
23.	The users of the personal devices cannot extend or connect to non-secure or untrusted networks using wireless, radio, Bluetooth, USB modems etc. while connected to secure enterprise networks and / or devices.
24.	Officers/Employees must be obliged to register any personal devices they may be using for work-related activity with the company's IT department. Officers/Employees must be prompted to keep this list updated so that if they sell on or stop using a device any permissions that may have been granted to it can be revoked and any company-related data must be deleted.
25.	Devices which are not registered with the IT department but trying to connect to HESCOM's corporate network should be automatically rejected. Plugging of USB/removable devices should not be allowed on business devices
26.	Two-factor authentication (2FA) should certainly be required to access any sensitive company data or information, but a company should also remind its officers/employees to enable 2FA on any personal apps or online accounts they have where it is available. This reduces the chances of a hacker successfully gaining access to something like a personal email account that may result in them obtaining information that could allow them to access the individual's work device or accounts, and subsequently the company network.
27.	IT Security Team should install Mobile device management (MDM). MDM software allows a company to secure its data when a device is lost, stolen, or improperly passed on to a new owner. Generally, a device owner must authorize MDM, and through it grant a number of permissions to the company's IT department. MDM software allows IT departments to

Approved by HESCOM BoD

	remotely wipe the device of any company-related activity, and some MDM software can even allow the IT department to reset the device to factory settings or wipe its hard drive entirely. The permissions and capabilities of a company's MDM software should be clearly outlined to officers/employees before they are asked to grant it permissions
28.	Ensure all devices that access company data — corporate devices and personal devices— are adequately protected with security software and antivirus programs.
29.	IT Security team should set up a virtual desktop infrastructure (VDI) or mobile device management protocol to ring-fence HESCOM's data from personal data. Private cloud storage is also a viable option. This ensures not only is the company-owned information protected from outside access, it keeps the officer/employee's personal data private.

4.19. Web Application Security Policy

Overview

Web application vulnerabilities account for the largest portion of attack vectors apart from malware. It is essential that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

Purpose

The purpose of this policy is to define web application security assessments within HESCOM. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of HESCOM services available both internally and externally as well as satisfy compliance with any relevant policies in place.

Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at HESCOM. All web application security assessments will be performed by delegated security personnel either employed or contracted by HESCOM. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of is strictly prohibited unless approved by the Top Management of HESCOM. Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

Approved by HESCOM BoD

Policies

1	***Web applications are subject to security assessments based on the following criteria:***
A	New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
B	Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
C	Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
D	Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture
E	Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by an appropriate manager who has been delegated this authority.
2	***All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.***
A	High – Any high-risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
B	Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure

Approved by HESCOM BoD

C	Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.
3	The following security assessment levels shall be established by the designated organization that will be performing the assessments.
A	Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered
B	Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum
C	Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.
4	Secure coding practices may also be implemented for internally /collaboratively developed applications. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.
5	Software/Application development approach should be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.
6	Consider implementing measures such as installing a “containerized” app on mobile/smart phones for exclusive business use that is encrypted and separated from other smartphone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.
7	XSS vulnerability may be arrogantly used by the hackers to inject data from one website as the scripting allows insertion of java script to the user. So, a website which is in CSS mode should not be kept open to users for editing as that would open the gate to hackers for inserting the malicious java scripts inside the web page. This insertion results in injecting out the data from the website or even the important files from the store can also be injected out

Approved by HESCOM BoD

	by the hackers.
8	Web applications must be reviewed and tested for security vulnerabilities. Applications that store, process or provide access to Level 1 or Level 2 information must be tested to an appropriate level of detail based on assessed risk.
9	Vulnerability assessment must be coordinated with and approved by authorized individuals.
10	All security flaws must be entered into a defect tracking system, clearly identified as a security defect, and categorized according to severity. This information must be protected appropriately, prioritized, and fixed before the application is released. Flaws discovered in applications that are already released must be assessed to determine whether there is a low/medium/high level of exposure due to the following factors: a. The likelihood that the security flaw would be exposed b. The impact on information security, integrity and application availability c. The level of access that would be required to exploit the security flaw
11	Peer-review code with at least one other technically trained individual.
12	Validate all data received via the HTTP Request. Not validating data can result in attacks such as Cross Site Scripting, SQL Injection, HTTP Response Splitting, Log Injection, and Directory Traversal.
13	Pass session IDs and cookies via SSL (HTTPS). Hackers can intercept unprotected session IDs and cookies and use them to compromise the user's session (session hijacking), and the security of your system.
14	Vulnerability scans should be performed before moving application to production or whenever there are changes to the application.
	Policies for SSO based applications
1.	Implementation of two-factor authentication to introduce an additional security layer .
2.	Logon to Active Directory to be secured to restrict when and from which endpoint(s) or IP addresses a particular user account can logon, restriction based on session type (local, RDP etc).

Approved by HESCOM BoD

3.	Logon management to monitor logons for unusual activity such as attempting logon on after hours or from an unusual endpoint
4.	Use of Privileged Session Management (PSM). PSM is a proxy between the user and the system or application with elevated access. Low-level users can request access (by means of a portal) with access granted without providing the password to the user
5.	**Ensure SSO least privilege** – think about the access SSO should provide using the lens of Least Privilege. Define roles for each type of user in the organization, identifying the specific applications they need to do their job, limiting access to only those IT deems absolutely necessary
6.	**Use Modern Authentication Protocols –** Make sure SSO solution is leveraging OpenId Connect or OAuth 2.0**.**
7.	**Limit Device Access** – Put restrictions on which devices with which a user can leverage SSO.
8.	**Enforce Frequent Password Changes –** for accounts with elevated access, consider requiring new passwords more often.

Note:

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the CISO, HESCOM

Approved by HESCOM BoD

4.20. Information Classification

Objective

The objective of this policy is to ensure identification, labelling and handling of information for protection commensurate with the Information Security risks.

Scope

This policy is applicable to electronic and non-electronic information as identified by the Information owner across HESCOM's assets.

Policy

1.	Information assets in HESCOM shall be identified and classified based on its criticality and sensitivity by the Information owner as per the Information Classification, Labelling and Handling procedures.
2.	Classification of information shall be reviewed by the Information owner at appropriate intervals or based on change in criticality and sensitivity, whichever is earlier.
3.	While deciding the protection level for information, the associated legal, regulatory, and statutory requirements shall also be considered.
4.	All information shall be labelled and handled as per Information Classification, Labelling and Handling procedures.
5.	The information labelling shall cover non-electronic media (E.g.: physical documents) and electronic media (E.g.: Emails, CDROM, Tapes, Word Documents etc). The physical labelling format shall be easily distinguishable and readable.
6.	All information for disposal shall be approved and recorded.
7.	After the retention period is complete, the content from the tape and disk shall be erased before reusing or disposing the media.
8.	Any critical information contained in media and sensitive documents shall be stored in fire proof and locked cabinet.
9.	Sensitive documents which are no longer required shall be destroyed as per the Information Classification, Labelling and Handling procedure by Information owner.
10.	Devices containing sensitive information shall be physically destroyed when no longer required.
11.	All Media device being transported shall be protected from unauthorized access, misuse or

Approved by HESCOM BoD

	corruption.
12.	Users shall be made aware of protecting the exchange of sensitive information during voice and video communications.
13.	Sensitive documents stored in soft copy format shall be adequately safeguarded by the information owner through methods like password protection or encryption as deemed appropriate.
14.	All Documents from External Origin should also be classified
15.	If sensitive information is lost, disclosed to unauthorized parties, suspected of being lost or disclosed to unauthorized parties, its owner shall be notified, and a security incident report shall be initiated immediately.
16.	Users shall share the sensitive information through discussions and electronic means only with personnel who are authorized to use the information by Information Owner
17.	Information owner shall be responsible for safeguarding information by exercising appropriate controls.
18.	Information about the existence and nature of significant assets shall be accessible only to those persons with a demonstrable need to know.

4.21. Information Access Control Policy

Objective

The objective of this policy is to control access to information, information processing facilities and official access based on the level of data and security requirements.

Scope

This policy is applicable for access to sensitive information & data residing in processing facility, IT/OT/IoT assets, tools managed by HESCOM.

Policy

Approved by HESCOM BoD

1	***User Access Control***
1.1	User access to IT/OT/IoT infrastructure and applications shall be granted based on an individual's job responsibilities and official requirements; on a "need to access" and "need-to-know" basis and the authorization shall be obtained as defined in the access control matrix.
1.2	Access control matrix shall be maintained for IT/OT/IoT infrastructure and applications.
1.3	Third party access to IT/OT/IoT infrastructure and applications shall be permitted after due authorization from Information Owner.
1.4	Users shall be authenticated before accessing Servers, Network devices, Applications, Desktops, Laptops, mobile devices and managed technical devices such as Attendance readers, smart card readers etc.
1.5	Users shall be made aware of their responsibilities towards acceptable usage of access privileges granted to them.
1.6	User shall protect critical information (documents/media) under their possession, from unauthorized physical and logical access.
1.7	Access control matrix shall be reviewed at appropriate intervals by the Information owner.
1.8	User access shall be disabled on the last working day on separation from the organization or movement to another role.
1.9	Guest accounts shall be removed on installation of systems
1.10	Default system accounts provided by vendor/service provider shall be renamed upon installation of new systems
2	***Sensitive Equipment and Server Sitting Protection***
2.1	Sensitive Equipment and Servers shall be adequately protected through physical and/or logical access controls.
2.2	Internet access shall not be allowed from the Production Servers (Eg: Browsing Internet sites from servers). However, if servers need to connect to internet for operational activities, can be

Approved by HESCOM BoD

	allowed based on the specific requirement.
2.3	Physical and logical access to sensitive equipment and servers shall be reviewed at appropriate intervals and monitored real-time or on need basis.
3	***Operating System access control and application control***
3.1	Operating systems and applications shall be configured to run only the required services and access limited to intended units use.
3.2	System utilities shall be used only after formal validation or testing by HESCOM
3.3	The log-on process on any system shall display only the limited information about that system and its intended use.
3.4	Systems shall not permit the information of internal menu/applications, structure system/application identifiers until the log-on process is successful.
3.5	Systems shall have logon banner stating the system's use is meant only for authorized users and activities are monitored.
3.6	Systems shall not display help screen (automated), during the logon process.
3.7	Unsuccessful log-on attempts if any, shall be logged on the systems, monitored and reviewed at appropriate intervals.
3.8	Access to the system and application shall be based on the unique identifier (e.g. UID, User ID).
3.9	Systems & Applications will Re-authenticate user on more than 5 minutes of idle session.
3.10	Designated System Administrators shall monitor the systems to detect deviation from access control policy and report the violations as defined in Security Incident Management procedure.
3.11	Systems shall be configured to alert on exceptions, and network management alarms.
3.12	Users shall not use any means to clear the logs or cache to delete the evidences of accessing

Approved by HESCOM BoD

	network devices, servers, databases and applications.
3.13	To ensure the accuracy of the audit logs, IT infrastructure and applications shall have the built-in clock synchronization.
3.14	All logs/record evidences will be stored for a minimum period of a 45 days on primary storage (file server) and then three (3) months on secondary storage. In case if necessary, for legal, contractual or for security related incidents the specific logs can be stored for a longer duration.
3.15	Access to critical applications shall only be allowed through Internet after carrying out information security risk assessment and formal authorization by Information owner.
3.16	Audit trail shall consist of user log-on failure, date, time, source IP address, login name. The audit logs shall be reviewed as per Log File Monitoring procedure.

4.22. Information Security

Objective

To recommend/suggest management and provide support for information security in accordance with official requirements and relevant laws and regulations. Data Sharing policy of HESCOM should be followed.

Scope

This Policy is applicable to all users of HESCOM

Policy

HESCOM should commit to serve its customers by ensuring Availability of Information while maintaining Confidentiality and Integrity of data.

1	***Availability***
1.1	Providing Information access without interruption for Authorized users.
1.2	Protection of Information and Assets through regular monitoring and review.

Approved by HESCOM BoD

1.3	Ensuring continuity of critical operations.
2	***Confidentiality***
2.1	Protecting critical information against unauthorized access.
2.2	Safeguarding the privacy of Personal Information.
2.3	Protection of Intellectual Property Rights
3	***Integrity***
3.1	Ensuring the Accuracy and Completeness of information.
3.2	Ensuring statutory, Regulatory & Contractual security compliance
4	***Privacy***
4.1	Personally Identifiable Information shall be considered as confidential and be disclosed on 'need-to-know' basis. Appropriate information handling mechanisms should be adopted to adhere to the applicable Laws and Regulations.
4.2	***Information Security Objectives***
4.3	Set direction in achieving safe and secure environment and security of information to users.
4.4	Maintain high awareness levels of security policies as applicable to various roles, through training and awareness campaigns.
4.5	Comply with applicable legal, regulatory and contractual requirements.
4.6	Prevent and detect malicious code.
4.7	Ensure Security Incident management and prevention.
4.8	Protect client and HESCOM Intellectual property rights.
5	***Review and Update***

Approved by HESCOM BoD

5.1	Information Security policies shall be reviewed at appropriate intervals (at least once a year) and in case of influencing changes, ensure they remain appropriate for the operations.

4.23. Information Security Risk Management Policy

Objective

The objective of this policy is to ensure that information security risks related to critical services are assessed and managed within HESCOM.

Scope

This policy is applicable to critical services managed within HESCOM.

The term 'risk' as referred in this policy deals with Information security risk.

Out of Scope: This policy does not cater to operational risks related to areas such as Market, Human resources, Financial, and Business Plan/Business Process.

Approved by HESCOM BoD

Policies

1.	Information security risk management Program shall comprise of the following steps: a) Risk Assessment b) Risk Treatment c) Risk Monitoring and Control d) Risk Reporting
2.	Information Security Risks and associated threats shall be identified at appropriate intervals.
3.	Risk assessment shall be carried out based on triggers such as major business engagement changes, security incidents, and any internal/external audit findings.

4.	Risk levels shall be identified based on probability of threat occurrence and impact to the process.
5.	Risks shall be prioritized based on the risk rating for effective formulation of risk treatment plans.
6.	Security Controls shall be proposed with due consideration to the existing risk level and effectiveness of the existing controls.
7.	Suitable Controls shall be implemented for treating the identified risks including risk acceptance, risk reduction and risk transfer.
8.	Risk review shall be conducted at appropriate intervals.
9.	Very high and significant risks shall be reported in Management Review Meetings.
10.	CISO shall be responsible for Risk Treatment and any decisions on Risk Acceptance.
11.	Risks identified from risk assessment or audit exercises that are acceptable to the stakeholder / process owners of the initiative / function shall be presented to the Management as part of the MRM (Management Review Meetings).
12.	Risk assessments related to Functions covering the Facility and Physical Security risks shall be carried out by the Facilities and Physical Security teams and documented as part of the risk register.

Approved by HESCOM BoD

4.24. Information Security Training and Awareness

Objective

The objective of this policy is to ensure that users are made aware of Information Security threats & precautionary measures related to various security areas, on a regular basis so that they are adequately trained to support organizational Security policies.

Scope

This policy is applicable to all users of HESCOM.

Policies

1.	Top Management shall articulate to all users the need for Security and communicate the Information Security Policy that needs to be followed.
2.	Users in HESCOM, including the top management and relevant third-party users such as contractors, security staff, housekeeping staff shall receive appropriate security awareness/training.
3.	Updates about Security policies and procedures shall be conveyed to the users.
4.	Responsibility of coordinating and conducting security awareness and training courses shall rest with the CISO
5.	CISO shall be responsible to provide updates on security policies to users in addition to periodic corporate communication on Security bulletins.
6.	Areas of Security awareness shall include but not limited to the following: ○ Overview of Security Policy ○ Physical Security and Physical Access control Procedures ○ Email & Internet usage ○ Roles and Responsibilities related to information security ○ Guidelines for securing the User identity and credentials ○ Reporting of security Incidents ○ Usage of licensed software package ○ Protection of information, Intellectual property ○ Business continuity and disaster recovery preparedness ○ Guidelines (do's and don'ts) to secure working environment and personal computers
7.	Newly inducted users shall undergo a dedicated session on Security as part of induction.
8.	Users shall read and accept the HESCOM Security Policy, Officer/Employee agreement for information security, Officer/Employee undertaking & Authorization and Consent form through electronic acceptance annually.
9.	Users should be encouraged to report suspicious behaviour incidents to the incident management team.
10.	**Training to IT/OT/IoT Security team**: There shall be simulation environment for training related to IT/OT/IoT and cyber security aspects. The simulation environment shall

Approved by HESCOM BoD

	be exact replica of production environment. The internal IT/OT/IoT security team shall be trained both on attack and defence.

4.25. Internal Audit Policy

Objective

The objective of this policy is to assess compliance to established information security policies for IT/OT/IoT systems in an effort to enhance the information security posture in the Organization.

Charter of the Information Security Compliance is broadly listed below:

- Compliance checks as per the ISO 27001 ISMS framework.
- Adequacy and Compliance checks on the existing controls for HESCOM.

Scope

This policy is applicable to service functions across HESCOM.

Policies

1.	Information Security Compliance check constitutes both technical and process assessment.
2.	Technical assessment shall be conducted to assess the configuration of systems and network infrastructure to validate the compliance status against the established standards. Technical assessment consists of Penetration Test/Vulnerability assessment this shall be made possible by the usage of Tools, Scripts, Checklist and Snapshots.
3.	Process Assessments shall be conducted to assess the compliance status against information security policies and standards.
4.	Compliance Activity shall be initiated by independent and trained personnel.
5.	Compliance checks shall be carried out as: **Planned Assessment** • Internal Assessment schedule shall be prepared based on the information security risks perceived or at-least annually.

Approved by HESCOM BoD

	• Based on the schedule, information security Assessment shall be initiated. **Unplanned Assessment** • Unplanned Assessment shall include Implementation checks and Spot checks. • Assessment on implementation checks shall be carried out on random basis. Any new setup or any changes to the existing setup shall be validated under this category on sample basis. • Spot Checks shall be Surprise checks to validate the compliance and adequacy of the information security controls within the organization. Advance information to Auditee may not be provided. **Compliance Check Tracking and Reporting** • All assessments shall be individually tracked for closures and any significant exceptions shall be reported to the respective functional head as well as to the MR. • Auditor shall classify the findings as Major NC, Minor NC or Observation. Auditor shall classify the findings as Non-compliance to the documented procedure or Inadequacy in the system.

Note:

- The data required for assessment shall be shared with the external auditor duly following the data sharing policy of HESCOM.
- Internal audit records shall be documented and maintained

Approved by HESCOM BoD

4.26. External Audit Policy

Objective

The objective of this policy is to assess compliance to established information security policies for IT/OT/IoT systems in an effort to enhance the information security posture in the Organization.

Scope

This policy is applicable to all IT/OT/IoT Systems

Policy

1.	Audit of the IT/OT/IoT systems shall be conducted periodically by external agency appointed by HESCOM or have Cert-IN empanelment.
2.	The audit should comprise of vulnerability assessment and penetration testing of DC, DR, network and endpoints at application level firmware level, network level and hardware level, threat hunt for APTs.
3.	Tasks include independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures
4.	Audit should be performed to validate the following items:
5.	The security controls present during system validation testing (e.g., factory acceptance testing and site acceptance testing) are still installed and operating correctly in the production system.
6.	The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.
7.	The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.
8.	Security performance metrics should be sent to the appropriate stakeholders, along with a view of security performance trends
9.	Monitoring of sensors, logs, Intrusion Detection Systems (IDS), antivirus, patch management, policy management software, and other security mechanisms should be done on a real-time basis where feasible

4.27. Policy for protection from Social Engineering Techniques/ Social Media

Objective:

To address the main security threats to an organization from social media by a general information security policy. This is because the main threats posed by social engineering use related to end-user behavior would be addressed by most organizations' existing security awareness programs.

Policies

Components of a recommended end-user information security program that are directly relevant to social media security.

Approved by HESCOM BOD

1. ***Desktop Security*** - The focus of the desktop security section is to educate users why it is important to use a password-protected screen saver and to lock their computers when the users walk away from them. The computers should also have a screensaver timeout so if the user leaves their computer, the password-protected screensaver comes up after a short time. Again, the idea is to keep out both insiders and outside attackers. If a potential attacker has access to a user's computer that is left unguarded, they could install malware or steal sensitive data. Users should also be wary of shoulder surfing.

2. ***Password Security*** - The password security section should set forth the minimum password requirements of the organization and emphasize selection of strong passwords. Additionally, password security is a crucial concern. Sharing passwords as well as leaving them out where others could discover them should be strongly discouraged.

3. ***Phishing*** - Phishing attacks are very common and, unfortunately, often very effective. Security awareness training should provide examples of phishing attacks and emphasize proper precautions (e.g. disregard and delete suspicious electronic messages and avoid clicking on links provided in e-mail and other communications).

4. ***Malware*** – It is recommended that appropriate malware policies should be defined, and officers/employees should be trained on the various malware categories. The training in this area should emphasize prevention, identification, containment, and eradication of malware and a malware infection

5. ***Internet Privacy*** – Officers/Employees should be prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by HESCOM's Confidential Information policy when engaged in blogging.

6. ***User Level Policy to prevent threats from Instant Messaging Platforms***:

    a. User must ensure that IM account password meets the password policy of the organization as mentioned in Section 3.1

    b. User must download and install security upgrades from IM companies. This software is frequently updated to address security flaws

    c. User should not allow IM program to "remember" their password or automatically sign into their account.

    d. It is not recommended to accept messages from sign-in names not in the contact list of the user unless he/she is known to the user personally/professionally.

    e. User should not accept unknown/ suspicious file transfer under any circumstances. File transfers are an easy way for hackers to launch virus attacks and are not scanned for viruses before reaching the workstation.

Approved by HESCOM BoD

f. User should refrain from clicking links sent in a message even if they appear from someone, he/she might know. Many links often go to a site hosting malware or may be malformed in such a way as to exploit another vulnerability.

g. User should not install IM applications on systems containing confidential data.

h. User should follow HESCOM's Data sharing guidelines while transferring any data using IM platforms.

i. User should refrain from transferring confidential data using IM platforms.

Few of the threats encountered by an organization through Social media are:

a. **Insufficient Authentication Controls**

b. **Cross Site Scripting (XSS)**

c. **Cross Site Request Forgery (CSRF)**

d. **Phishing**

e. **Information Leakage**

f. **Injection Flaws**

g. **Information Integrity**

4.28. Data Retention Retrieval and Archival Policy

Objective:

The purpose of this policy is to introduce data management practices to ensure uniformity in the manner in which every function addresses record management as well as to ensure adequate compliance with all applicable regulations. This policy establishes retention and archival schedules for various data categories defined in this policy with an objective to ensure conformity in the schedules of records which are common in nature in the area of policy/processes notes, business development and business operations, created by individual departments within HESCOM. This policy is framed for the purpose of systematic identification, categorization, maintenance, retention and destruction of documents received or created in the normal exchange business. This policy defines guidelines on determining record category, how long should a document be preserved and in what form, and how and when should certain documents be destroyed.

Approved by HESCOM BoD

Data/Record Categories:

#	Data/Record Categories	Brief Description
1	Accounting records	All records and documents pertaining to accounting entries of income, capital and revenue expense, asset booking, investments, etc. Records include payment records, approval notes, purchase orders, invoices, journal vouchers and any other supporting document. Records also include financial statements, auditor's certificate on financial statements, all accounting and audit records/ annexures/ working prepared for final
2	Agreements/ Work orders/ Collateral documents	Agreements with vendors, clients/ customers as well as inter-company agreements across all departments. Records include contracts, service level agreements, work orders, undertakings, Memorandum of Understanding (MoUs),
3	Approval notes	Records that establish authorization of an activity by a designated authority. Records also include approval notes received from the regulators, Government authorities, etc.
4	Audit records	All records submitted and accepted for audits other than statutory and tax audits, including but not limited to records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analysis, or financial data and other documents relating to such an audit or review, including audit reports and audit plans, which is conducted by auditors
5	Board & sub-board committee documents	Documents prepared for all committees like notices, agendas, minutes, board resolutions, attendance registers and any other record created to comply with secretarial standards
6	Closed Circuit Television (CCTV) records	Records generated from the CCTVs installed for monitoring of activities carried out across all premises/facilities of the organisation
7	Change management	Records generated at the time of facilitating change in any business process, product or application including all records created during identification, implementation, monitoring and review activities

Approved by HESCOM BoD

#	Data/Record Categories	Brief Description
8	Charters of committees	Document containing details of a particular committee, including but not limited to, composition, date of formation/reconstitution, scope of committees, quorum and role of committee.
9	Company incorporation and secretarial records	Documents required to be maintained as per the Companies Act, 2013 and applicable Secretarial Standards
10	Corporate social responsibility (CSR)	All records of CSR projects, including but not limited to, project details, fund requirement letters, progress reports, Non-Government Organization (NGO) selection documents etc. Records include statements of budgets allocated, funds/amounts spent along with impact assessment document of the projects
11	Customer/client/investor queries and interaction	Customer-care/call-centre/helpdesk interactions and records including voice call records. Records also include responses or resolution of queries, including any document/data shared as part of the resolution
12	Customer service requests records	Any Service Requests raised by customer for availing various services provided by the organisation including changes in the existing services
13	Email records	Any messages created, sent or received within an email system that are required by the Organization to control, support, or to carry out operations, to make decisions, document the delivery of programs or to account for activities
14	HR related records	Records submitted by officers/employees at the time of joining the company, including documents prepared by recruitment and talent teams (for e.g. background verification reports, interview assessment notes, salary structures, approval notes, etc.)
15	Facility access and visitor records	All records created/ generated while accessing any facility of the organisation by any officer/employee or any visitor of the facility

Approved by HESCOM BoD

#	Data/Record Categories	Brief Description
16	Information technology and security	Information technology logs comprising Database Administrator (DBA)/ privilege user logs, transaction logs, user activity logs, system logs, network activity logs, server logs including server start-up, load and shut down log (excluding those logs that may affects latency), database logs, system administrator, DBA activity logs, security logs and error logs, etc.
17	Legal records	All records pertaining to cases filed by or defended in the court of law, documents related to Intellectual Property Rights, Power of Attorney, Arbitration, Investor Grievance Redressal, etc.
18	Marketing collaterals and related records	All material created for sales and marketing purposes
19	Media communications and related documents	All records created for press release, social media advertisement, announcements (other than by way of circulars) or any other document created for the public at large
20	Records for managing human resources	Documents include all records maintained for recruitment, training, talent management, officer/employee initiatives, etc. All records other than those associated with individual hired officer/employee
21	Service Level Agreements (SLA)	Inter-departmental agreements containing details, including but not limited to, turn-around-time, metrics, agreed service levels, escalation grid etc.
22	Taxation records	All records and documents pertaining to income tax compliance, including but not limited to tax audit reports and other annexures, assessment notes, notices
23	Meter Data	Billing and grid management, measured every 15/30/60 minutes, stored in the meter and collected every day/week/month. The data necessary for consumer energy efficiency and management, collected by a device or a commercial energy service company that the consumer chooses (in-home display, app, 3rd party) on near real-time (i.e. seconds) basis

Approved by HESCOM BoD

#	Data/Record Categories	Brief Description
24	OT/IoT Data	All the data generated by the sensors of the IoT/OT devices
25	SCADA Data	All data collected by sensors and sent by PLCs(Programmable Logic Controllers) /RTUs (Remote Terminal Units) to SCADA systems

Approved by HESCOM BoD

i. Retention Policy

As per the Record Retention Schedule published by Department of Administrative Reforms & Public Grievances[1], Government of India, in 2012, data is categorized into two broad categories:

A. Physical Records - File may be recorded under any one of the following categories:

1. **Category 'A'** meaning 'keep and microfilm' -
   a. files which qualify for permanent preservation for administrative purposes and which have to be microfilmed because they contain:
      - a document so precious that its original must be preserved intact and access to it in the original form must be restricted to the barest minimum to avoid its damage or loss; or
      - material likely to be required for frequent reference by different parties simultaneously/frequently.

   b. files of historical importance.
2. **Category 'B'** meaning keep but do not microfilm'-This category will cover files required for permanent preservation for administrative purpose. It will, however, exclude the nature of material falling under the category described in (i) or (ii) of sub-para (1) (a) above and therefore need not be microfilmed.

[1] https://darpg.gov.in/sites/default/files/RRS_WC.pdf

3. **Category `C'** meaning `keep for specified period only'. This category will include files of secondary importance having reference value for a limited period not exceeding 10 years. In exceptional cases, if the record is required to be retained beyond 10 years it will be upgraded to B Category.

B. Electronic Records - e-Files/records may be digitized any one of the categories:

1. **Category-I** (e-Files/records to preserved permanently on which are of historical importance) – For 10 years, it will be kept in the Department 's server and thereafter transferred to the server of the National Archives of India.

2. **Category –II** (e-Files/records of secondary importance and have a reference value for a limited period) – 10 years on the Department's server. In exceptional cases, if the record is required to be retained beyond 10 years it will be upgraded to Category-I.

The focus in this document is primarily on Electronic records:

Subject/Records Groups	**Proposed Retention Period**
Category I-The e-files which are to be preserved permanently or which are of historical importance. The e-files included under this category will be as follows: - 1. e-files containing evidence of rights or obligations of or against the government, e.g., title to property, claims for compensation not subject to a time limit, formal instruments such as awards, schemes, orders, sanctions, 2. e-files relating to major policy decisions, including those relating to the preparation of legislation. 3. e-files regarding constitution, functions and working of important committees, working groups, etc. 4. e-files providing lasting precedents for important procedures, e.g. administrative memoranda, historical reports and summaries, legal opinions on important matters. 5. e-files concerning rules, regulations, Departmental guides or instructions of general application. 6. e-files relating to salient features of organization and staffing of government Departments and offices. 7. e-files relating to important litigation or "causes célèbres" in which the administration was involved. 8. e-files relating to the origin of a Department or agency of	For 10 years, it will be kept in the Department 's server and thereafter transferred to the server of the National Archives of India (NAI).

Approved by HESCOM BoD

government; how it was organized; how it functioned; and (if defunct) how and why it was dissolved.

9. Data about what the Department/agency accomplished. (Samples by way of illustration may be enough; but the need for such samples may be dispensed with where published annual reports are available).
10. e-files relating to a change of policy. This is not always easy to recognize, but watch should be kept for (a) summary for a Minister, (b) the appointment of a Departmental or inter-Departmental committee or working group, and (c) note for the Cabinet or a Cabinet Committee. Generally, there should be a conscious effort to preserve all such papers, including those reflecting conflicting points of view. In the case of inter-Departmental committees, however, it is important that a complete set of papers be kept only by the Departments mainly concerned – usually the one providing secretariat.
11. e-files relating to the implementation of a change of policy, including a complete set of instructions to executing agencies etc., and relevant forms.
12. e-files relating to a well-known public or international event or 'cause célèbre', or to other events which gave rise to interest or controversy on the national plane.
13. e-files containing direct reference to trends or developments in political, social, economic or other fields, particularly if they contain unpublished statistical or financial data covering a long period or a wide area.
14. e-files cited in or noted as consulted in connection with, official publications.
15. e-files relating to the more important aspects of scientific or technical research and development.
16. e-files containing matters of local interest of which it is unreasonable to expect that evidence will be available locally or comprising synopsis of such information covering the whole country or a wide area.
17. e-files relating to obsolete activities or investigations, or to abortive scheme in important fields.
18. Any other specific category of records which, according to the

Approved by HESCOM BoD

Departmental instructions issued in consultation with the National Archives, have to be treated as genuine source of information on any aspect of history-political, social, economic, etc., or are considered to be of biographical or antiquarian interest 19. SCADA data, meter data and other IoT/OT devices data	
Category II: This category will include e-files of secondary importance and having reference value for a limited period.	Up to 10 years akin to the retention period of physical files/records on the Department's server. In exceptional cases, if the record is required to be retained beyond 10 years it will be upgraded to Category I.

ii.Data Archival Policy

The Section 6 of NSE (National Stock Exchange) Policy on Data Retention and Archival [2]is taken as reference and referred for this section.

1. Archiving is defined as secured storage of data/documents, such that the same is rendered inaccessible by authorized users in the ordinary course of business, but which can be retrieved by an administrator designated by the top management of HESCOM for the document in question.
2. *Deactivated officer/employee records* – archival period will be eight (8) years after retention period is over
3. *Agreements/ Work Orders/ Collateral documents* – Five (5) years after expiry of the document
4. *Officer/Employee Records* – Five (5) years after retention period is over
5. *Legal Records* – Five (5) years after the dispute is closed
6. *Audit reports*- Five (5) years from the end of the fiscal period in which the audit or review was concluded
7. *Meter Data – Archival period is Ten (10) years after retention period is over*
8. *SCADA data, IoT, OT data – Archival period is Ten (10) years after retention period is over*
9. Departments shall ensure that documents are archived within 30 days from end of the retention period
10. Paper records shall be archived in secured storage onsite or secured offsite location with clear labelling

[2] https://www.nsccindia.com/NSCCL/disclosures/resources/Data_Retention_and_Archival_Policy.pdf

Approved by HESCOM BoD

11. Electronic records shall be archived in a format which is appropriate to secure the confidentiality, integrity and accessibility of data.
12. Departments shall ensure compliance with the appropriate data classification guidelines throughout the archival period.
13. This policy shall also ensure that existing data retention policies of HESCOM should be taken into consideration for cases pertaining to transfer, retirement , termination of officers/employees, untimely death of an officer/employee.

4.29. Database Security Policy

Objective

To provide guidelines for ensuring security of the database being used by individual applications

Scope

Applicable to developers, testers, database administrators and application owners

Policy

1.	Officers/Employees must not have access to the database prompt of the application. Access to the database prompt must be restricted only to the database administrator and / or a person designated only through the client apps provided by OEMs for generating MIS reports using SQL statements. “Super user” rights for the database must only be given to the database administrator and the activities of these accounts must be properly logged.
2.	The database access shall be bound by Device id.
3.	Database access over the public network is prohibited.
4.	Even the super user should not have access to the data stored within the database.
5.	Access to the data from any non-application platform should be strictly prohibited.
6.	Any sub contracted employee shall not have any administrative rights to the Operating system or DBA rights to databases.
7.	The database administrator shall ensure the latest patches released by product vendor are applied in a timely manner.

Approved by HESCOM BoD

8.	The database configuration shall adhere to base line security guidelines released by the product vendor.
9.	Audit at database level should be enabled to keep track of all the modifications at the database end.
10.	DBMS Security - Controls surrounding DBMS resources should be adequately documented
11.	Access to and deletion of data held within the database should be adequately controlled
12.	Adequate controls should exist for monitoring the system usage
13.	Controls over the use of sensitive DBMS functions should be documented
14.	Distributed DBMS components should be subject to adequate access and integrity controls
15.	Recovery and restart controls should be adequate to ensure the integrity and availability of the DBMS data
16.	Controls over the operation of the DBMS and data dictionary systems should be adequate to ensure their integrity and availability
17.	Maintenance and emergency support procedures should be adequately documented

4.30. IoT Security Policy

Objective:

To provide key measures in order to ensure security across all IoT infrastructure of HESCOM (Smart meters, EV charging systems, IoT Communication infrastructure, Smart gadgets etc.)

Scope:

This policy is applicable across all service functions of HESCOM implementing Internet of Things.

Policies:

1.	Authentication of all entities before they can join using latest public key cryptography certificates signed by a trusted root authority. These keys and certificates should be stored securely in Federal Information Processing Standards (FIPS) compliant hardware security modules.
2.	Data integrity should be verified based on cryptographic hashes like Secure Hash Algorithm (SHA).
3.	Data confidentiality should be implemented using latest encryption standards/protocols like Transport Layer Security (TLS) /Datagram Transport Layer Security (DTLS) (latest versions)

Approved by HESCOM BoD

	for the secure transfer of data over the network.
4.	Digital Signatures should be used while sending a message or a file. This ensures that the file was created by a known sender.
5.	Role Based Access Control(RBAC) should be implemented across all the services offered by the applications
6.	All data should be classified based on security levels and criticality as per the policies in Information Classification mentioned in section 3.20. For e.g. user authentication data should be stored in an encrypted manner in storage systems.
7.	Strong security controls must be in place for all software and firmware or devices to prevent in threats.
8.	All centralized infrastructure should be protected against DDOS (Distributed Denial of Service) attacks.
9.	All computing systems should receive latest security patches updates against known vulnerabilities.
10.	Advanced security should be implemented to protect critical IT infrastructure in cloud and data centres including Anti-APT(advanced persistent threat) systems, intrusion protection systems, network behaviour analysis tools, anti-virus and anti-malware systems, next generation firewalls, security information and event management, email security systems, data loss prevention systems, etc.
	IOT Device Security
11.	**Mapping and monitoring all connected devices** Security management team should keep track of all settings, firmware versions, credentials, and recent patches. This step shall help assess which devices may have to be replaced or updated. They may create asset maps to list out all of the connected devices as well as all the third-party vendors, hardware and critical areas so that weak spots can be mitigated and watched.
12.	Network Access Control can help in identification and maintain of inventory IoT devices connecting to a network. This will provide a baseline for tracking and monitoring devices.

Approved by HESCOM BoD

13.	IoT devices should be enforced with heightened security through secured boot mechanisms
14.	**Applying Network Segmentation** Network segmentation must be applied to prevent the spread of attacks, and it will also help in isolating possibly problematic devices that cannot be immediately taken offline.
15.	**Network architecture must be secure** Security management team should set up routers with VLAN or a DMZ—segmentation and isolation mechanics which will add an extra layer of security to networks.
16.	Measures should be taken to update the credentials of the devices using a strong password or multi-factor authentication or biometrics wherever possible.
17.	Devices needs to be compliant with Public Key Infrastructure(PKI) and 509 Digital certificates
18.	Proper API security controls should be in place for protecting the integrity of data being sent from IoT devices to back-end systems .
19.	Each device shall be provided with unique identifier to understand what the device is behaving, and what devices are connected to it.
20.	**Hardware security.** Endpoint hardening should be implemented to make devices tamper-proof or tamper-evident. This is important when devices will not be monitored physically.
	***Smart* Meters**
21.	***Encryption:*** Communication between different nodes of the AMI must be encrypted. Depending on the TLS protocol is no longer efficient enough to guarantee data confidentiality. Hence, it is vital to integrate other encryption mechanisms as in RSA at both application and transport layers as well. Possible encryption mechanisms like PUF (Physical Unclonable Function), MAC (Message Authentication Codes) and homomorphic encryptions may be followed.
22.	***Authentication:*** Accurate verification of the source of the data is critical for consumer to authenticate the AMI she/he is communicating with, and for the AMI to validate the authenticity of the legitimate consumers as well. For instance, the consumer is supplied with a password to generate public-private key to build the authentication between the AMI and the power utility. Then, any new appliance asks to join the AMI for the first time is

Approved by HESCOM BoD

	challenged to authenticate itself and to set up the communication channel to control the appliance from within the AMI. Finally, the newly joined appliance, AMI and power utility can decide whether to use the same public-private key used before or to generate a new one for each session to manage the flow of traffic between them.
23.	***Availability Mechanism:*** The availability of the AMI can be severely affected due to several vulnerabilities as in network jamming and packet flooding. A robust AMI can be designed to go through defined channels of alternative frequencies if the default channel is unavailable for specific period of time. Moreover, filtering network traffic would exclude ping requests that overwhelm the network and make it unavailable for legitimate users. Other systematic approach might help in preventing the DoS is through allowing the ARP cache static so that suspicious ARP cannot update its content malicious IP/MAC payloads. Moreover, preventing high speed traffic from reaching the kernel of the meter would significantly overcome the DoS attacks.
24.	Embedded products with physical attack-detection mechanisms should be deployed to detect when a system becomes compromised. These products make use of physical sensors like case open switches, blind switches, motion detectors, and environmental sensors to detect attacks. When a threat is detected, the meter can take action, such as trying to contact the utility or even deleting secret cryptographic keys (it may be better to delete those keys than expose them to an attacker).
25.	Secure on-chip memories can be locked and encrypted so that an attacker has difficulty reading or reverse-engineering the software. Secure bootloaders can lock the device at manufacturing time to make sure an attacker cannot load an unauthorized version of software on the meter.
	Electric Vehicle Charging system
26.	The security of the communications between the charging point and HESCOM must be ensured, so that they cannot be intercepted or altered by third parties. The communication between charging system (EVSE) and the central system should be OCPP 2.0 complaint.
27.	The physical access points of the device must be secure, so that it is impossible to extract any of its internal components, in particular those that could contain a microprocessor or memory
28.	Firmware updates must be supported, so that any vulnerability detected may be corrected.

Approved by HESCOM BoD

29.	Communications with the Charge Point Operator through the WAN should be done implementing the use of digital signatures. In this way various security principles are guaranteed, like the message was sent by a known entity (authentication), the message was really sent by who it says it was (non-repudiation) and that the message was not altered by third parties (integrity).
30.	Additionally the information should be encrypted by means of TLS in order to ensure the confidentiality of the transmitted information.
31.	If a message is detected as having been modified, such message should be rejected. In turn, the device (charging station) should allow for the parties with which it is communicating to be able to verify the integrity of its messages.
32.	The device must be able to detect packet replay attacks and reject such packets. A counter may be used or a nonce may be sent in authentication in order to detect the replay of packets.
33.	Detection and registration of any attempt to physically manipulate the charging station. For this, it is advisable to have sensors that detect any opening or physical manipulation of the devices that shape the station.
34.	Deploy a surveillance system in order to have proof of the physical manipulation the devices have undergone by an attacker.
35.	For electric vehicle user authentication in the terminal, a token should be used that makes use of the challenge-response mechanism. This token will be identified by means of a single UID
36.	At the time of deploying the charging station, it is recommended that a hardening process is followed in the same way that: 1. All services that are not strictly necessary for operation are disabled. 2. Services that have some type of known vulnerability are disabled. 3. Only the communication protocols necessary for the operation of the equipment are used. 4. Direct remote access is only allowed through the WAN interface of the local controller. 5. Unnecessary ports and interfaces must be disabled. In particular, any debug port of the device.

Approved by HESCOM BoD

	6. The default accounts, such as guest or anonymous, must be deleted. Furthermore, any unnecessary user account from the provider will also be disabled. Remote access to administrator accounts should be not be allowed.

4.31. Policies for Procurement of Devices

Objective:

To provide key measures in order to ensure security measures to be taken while procuring new devices and introducing into the HESCOM environment. Software procurement guidelines have already been specified in section 3.12

Scope:

This policy is applicable across all departments/divisions/sub-divisions of HESCOM

Policies:

1.	In case of any system, application, appliance or any other device being introduced into HESCOM, steps should be taken that appropriate system hardening process as per PCI compliance to be followed.
2.	HESCOM shall not allow devices with pre-installed software, applications, services, drivers, features, and settings as this may pose security threats. Therefore steps should be taken to remove the unnecessary functionalities and program and configure the necessary ones for additional security
3.	HESCOM's IT Security shall allow installation of only those software packages with verified source. Alternatively, the IT team shall maintain a repository of whitelisted software packages and allow installation of only those software.

Approved by HESCOM BoD

4.	HESCOM's IT team shall carry out the below tasks as part of the system hardening process: a. Disabling of unwanted ports and stopping unwanted services b. Removing unsafe features of the operating system c. Uninstalling vulnerable and unnecessary software d. Default settings shall be changed and features and applications not needed by HESCOM may be removed e. Ensure that each system's security configurations are set properly f. Ensuring that OS software, applications and firmware are up to date g. Ensuring that the system hardening process should evolve constantly, with maximum automation and updating h. Testing during hardening of the systems in order to make sure anything critical to HESCOM is not impacted i. Updating the hardening process in order to include new patches or software versions in the standard configuration, so the addition of a similar system in future does not come with the old weaknesses
5.	**Network Hardening**: IT security team shall ensure that firewall is properly configured and the rules are regularly audited; remote access points are secured ; any unused or unnecessary open network ports are blocked; unnecessary protocols and services are disabled and removed; ensure access lists are implemented; network traffic is encrypted
6.	**Server Hardening**: Servers should be put in a secure datacentre; hardening should not be tested in the production server; servers to be hardened before connecting to the internet or external networks. Unnecessary software which is not whitelisted by HESCOM's IT team should not be installed on a server
7.	**Database hardening:** Creating admin restrictions, such as by controlling privileged access, on what users can do in a database; encrypt database information—both in transit and at rest; enforce secure passwords; introduce role-based access control (RBAC) privileges; remove unused accounts;
8.	**Operating system hardening:** Apply OS updates, service packs, and patches automatically; remove unnecessary drivers, file sharing, libraries, software, services, and functionality; encrypt local storage; tighten registry and other systems permissions; log all activity, errors, and warnings; implement privileged user controls.
9.	IT security team shall conduct testing of security system on a sandbox environment which shall be a replica of the production environment.

Approved by HESCOM BoD

4.32. Policies for Inspection of IT hardware and Software

Objective:

The purpose of inspection is to look for defects (of understanding, interpretation, translation, etc.), deviations, especially regarding quality clauses, absences or abundances etc., and to provide the elements to make corrections. Inspection of software is a control technique for ensuring that the documentation produced during a given phase remains consistent with the documentation of the previous phases and respects pre-established rules and standards.

Scope:

This policy is applicable across all departments/divisions/sub-divisions of HESCOM

Policies:

1.	In case of any system, software, application, appliance or any other device being procured for HESCOM, inspection to be carried by IT Staff as per IT standards and policies.
2.	Verification and Validation of all software license to be carried as per the requirement initiated.
3.	The document inspection/review:. The inspection will focus on the quality, the correctness, model, program source files, test scenarios, etc. and the relevance of the document(s);

Approved by HESCOM BoD

4.33. Operational Technology Security Policy

Purpose:

The term 'operational technology' (OT) refers to the hardware and software used to control industrial processes. A cyber-attack on an OT environment can have serious and wide-ranging consequences beyond just financial losses – including prolonged outages of critical services, environmental damage and even the loss of human life. There are highly skilled and motivated adversaries actively seeking to exploit the security weaknesses in OT networks, process control systems and critical infrastructure. Their motivations range from economic benefit and espionage through to malicious disruption and destruction. The purpose of this policy is to protect Operational Technology (OT) systems used by HESCOM, monitor OT networks to identify and mitigate security vulnerabilities

Scope:

This policy applies to all Workforce Members, OT Systems, and other resources connected to HESCOM's infrastructure.

Policies to mitigate OT vulnerabilities:

The National Institute of Standards and Technology (NIST) has produced a guide for Industrial Control Systems (ICS) Security (SP 800-82) which explains best practice for businesses to design security into their OT environments (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf).

Sl. No	OT vulnerability	Mitigation Policy
1.	**Publicly accessible OT systems:** OT systems are often directly connected to the internet, in some cases so that third-party vendors can remotely connect to the system to perform diagnostics and maintenance. In many of these instances, the OT systems are not protected by a firewall and are outdated, so they lack modern security features that would typically be used to protect an internet-facing connection (e.g. multi-factor authentication, strong passwords, logging and monitoring). This issue means that potential attackers can directly perform password 'bruteforcing' (a method of rapidly attempting different potential passwords) or probe these interfaces, which can cause OT systems to become unstable or fail completely, resulting in	If remote support is required, an enterprise-grade firewall, a remote access solution and multi-factor authentication should be implemented to control all access to OT devices and systems.

Approved by HESCOM BoD

Sl. No	OT vulnerability	Mitigation Policy
	business disruption. Power and telecommunications cabling carrying data or supporting information services shall have to be protected from interception or damage	
2.	**Insecure Remote Connectivity to OT networks:** A 'jump box' is a remote connection system that gives an operator access to the OT network from the corporate network. The jump box often serves as the single point of entry to the OT network. These jump boxes are remotely accessible and may provide significant access to the OT network; as such they are an attractive target for attackers. Common vulnerabilities that are seen elsewhere also apply to jump boxes. Attackers only require any one of these vulnerabilities to be present in order to gain access to OT systems.	The use of a strong, multifactor authentication mechanism, enforced password policies and appropriate security patching practices can minimise the risk of compromise through these attack vectors.
3.	**Missing Security Updates:** Availability is a key requirement in an OT environment, and unplanned downtime can have significant consequences. This can lead to a conservative approach to deploying software patches and updates, as these new patches can have unintended consequences. The inherent danger of this approach is that OT systems end up running outdated software versions with known security vulnerabilities, leading to increased risk of compromise by an attacker.	Processes and procedures should be established to thoroughly test patches and updates to OT systems
4.	**Poor password practices:** Even those businesses that have strong corporate password standards often fail to apply these to their OT environment. Common issues include: a. operators and administrators using the same usernames and passwords for corporate and	Organisations need to establish and maintain a strict separation between authentication mechanisms and should require separate username conventions for the corporate IT and OT networks. They must also

Approved by HESCOM BoD

Sl. No	OT vulnerability	Mitigation Policy
	OT systems, enabling attackers to easily pivot from the corporate network into the OT network b. Generic user accounts usually having easily guessable passwords or passwords that are identical to the user name. These accounts are used on multiple systems allowing an attacker to propagate through the OT network c. Failure to change default vendor credentials on embedded devices and management interfaces from the initial installation or setup. The use of default credentials is one of the most common ways attackers gain entry into a system.	develop a process to change default credentials from software and devices during initial configuration. Compliance with secure password policies for both IT and OT networks should be enforced through controls such as security audits.
5.	**Insecure Firewall Configuration and management:** Firewalls that segregate OT networks from corporate networks are an essential control in protecting both networks. However, insecure configuration and management of these firewalls significantly increases the potential attack surface of the OT network. Common vulnerabilities include misconfigured access rules allowing unnecessary access between corporate IT and OT networks, and temporary rules that have outlived their purpose. It is also common for support teams to allow excessive access to management interfaces on firewalls. Without properly secured firewalls, security threats to the corporate IT network can easily propagate to the OT network, leaving it susceptible to attack.	A secure firewall configuration and a formal firewall change management program will help to protect OT networks from perimeter attacks originating from the corporate or external network. It is critical to restrict access based on business need, and to perform regular audits of all connections between IT and OT networks.
6.	**OT systems located within corporate IT networks:** Corporate systems usually require some level of interconnectivity with the OT network in order to access operational data or export data to	A strong segregation between corporate IT and OT devices provides a layer of defence to protect OT devices from external

Approved by HESCOM BoD

Sl. No	OT vulnerability	Mitigation Policy
	third-party management systems. OT components such as reporting servers and control stations are frequently placed within the corporate network, connecting through to the OT network, instead of being constrained to the OT network. The increasing frequency of cyber-attacks on corporate IT networks means this type of 'overlap' between the networks poses a serious risk as attackers may be able to use a compromised corporate IT system to then access OT networks.	cyberattacks. Where there is a business reason for the two systems to overlap, a demilitarised zone (DMZ) should be established for all connections between the two networks. It is also advisable to regularly monitor all DMZ activity between the IT and OT networks.
7.	**Lack of segmentation within OT networks:** Many OT networks are designed and configured in a flat and unsegmented configuration to simplify management of the network. Unfortunately, this flat layout increases risk by assuming all systems are of equal importance, function and criticality. A breach of any single device may expose the entire OT network	Defining a clear separation between critical and non-critical systems not only limits the impact of a breach, it also helps to clarify the organisation's OT 'crown jewels' and apply appropriate security controls. Implementing a zoning model that uses a 'defence in depth' approach makes it harder to impact the OT network or services as an attacker must penetrate several layers of defence to compromise critical systems.
8.	**Unrestricted outbound internet access from OT network:** In some instances, direct outbound internet access is enabled from the OT network, usually to allow for patching or for operator maintenance research. As discussed previously, OT systems commonly run outdated software, so enabling direct outbound internet access significantly increases the risk of malware being introduced to the OT network. Unpatched and insecure OT hosts are particularly susceptible to infection by malware and propagation throughout the broader network. Direct internet access from the OT network also increases	Outbound access to the internet from OT systems should be restricted, with any exemptions requiring a formal risk assessment. In the case of such exemptions, OT systems requiring external access must be securely patched, closely monitored and appropriately segregated from the rest of the OT network. Security updates can be downloaded from the internet onto a separate repository outside the OT network and verified

Approved by HESCOM BoD

Sl. No	OT vulnerability	Mitigation Policy
	the risk of external command-and-control attacks, whereby an attacker establishes reverse connections to 'phone home' and issue real-time commands to the compromised OT systems.	in a test environment before they are ported onto OT systems.
9.	**Insecure encryption and authentication for wireless OT networks:** OT networks often use wireless and microwave solutions to connect devices and systems, sometimes over considerable distances. In some instances, radio telemetry technologies such as WiMAX and LTE are used to connect remote stations and field devices when physical communication channels are not available. It is not uncommon for the deployed wireless equipment in OT networks to use deprecated security protocols or technologies, leaving them vulnerable to modern eavesdropping and authentication bypass attacks. An attacker in close proximity may be able to gain direct access to the OT network, allowing them to launch further attacks within the broader network.	Using strong wireless encryption protocols, industry-standard cryptographic algorithms and mutual authentication between communicating OT systems is the best way to minimise the risk of wireless attacks. Any outdated or deprecated communication solutions should be refreshed, and wireless systems should be audited on a regular basis.

Approved by HESCOM BoD

4.33.1. Best Practices to ensure security of OT devices, SCADA Systems:

1.	***Network Monitoring:*** Passive monitoring analyzes network traffic through a span port or tap to identify endpoints and traffic patterns. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible. It can be used to identify whether : a. Unauthorized Device Is Connected to the Network b. Unauthorized Ethernet/IP Scan of the Network c. Unauthorized SSH Session Is Established with Internet-Based Server d. Unauthorized PLC Logic Download e. Undefined Modbus TCP Function Codes Transmitted to PLC f. Denial-of-Service Attack Is Executed Against the ICS Network g. Data Exfiltration Between ICS Devices via UDP h. Invalid Credentials Are Used to Access a Networking Device i. Brute-Force Password Attack Against a Networking Device j. Unauthorized PLC Logic Update – Process Control System

Approved by HESCOM BoD

2.	***Centralized Authentication:*** ***a. Local authentication should be avoided*** • Deploy Active Directory • Dedicated in the OT environment • Separate OT forest (i.e. nlpower.ICS) • No trusts into IT or other networks • Separate DNS ***b. Allows for centralized user management, groups*** ***c. Allows for the use of centralized GPOs(Group Policy Objects)*** • Logon restrictions • No RDP(Remote Desktop Protocol) • No network logon • No cached credentials • No local administrators • No USB ***d. Look at 2FA(two factor authentication) for logins to SCADA workstations*** ***e. Logs should be shipped to a SYSLOG server***
3.	***Hardening of SCADA networks:*** Unused services and network daemons should be removed or disabled to the greatest degree possible to reduce the risk of direct attack.
4.	***Threat Intelligence***: It is critical to monitor vendors for vulnerabilities in their products. Threat intelligence tools should be used for analyzing events recorded from the entire web and empower the team to block attacks before breach occurs.

Approved by HESCOM BoD

5.	***Implement Internal and External intrusion detection systems*** **-** To be able to effectively respond to cyber attacks, it is imperative that IT team establishes an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.
6.	***Physical Security*** **–** Any location especially unmanned and unguarded remote sites that has connection to SCADA networks may be a target. Hence, physical security survey and inventory access point at each facility that has a connection to SCADA system should be conducted. Identification and assessment of any source of information including remote telephone/computer network/ fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience. High-delay-time fencing products, vehicle barriers, retractable bollards, crash-rated gates and sally ports, video surveillance, intrusion detection systems and advanced motion analytics around the entire perimeter should be common elements at critical utility sites. Utilities must also use biometric readers and access control badges for more stringent control of unauthorised physical access prevention and detection. The PLCs and RTUs should not be connected to public networks such as the internet. This eliminates majority of the threats.
7.	***Patching:*** SCADA system owners must insist that their system vendor implement security features in the form of product patches or upgrades. a. Updates must be manually kicked-off so that updates can be verified before being installed b. Orchestration using tools like Puppet shall be used to push patches downloaded manually c. All patching requirements shall be tracked through a centralized asset management inventory d. Formalize a review process to manage patching requirements and remediation plans from penetration testing activities within a centralized ticketing system (e.g.

Approved by HESCOM BoD

	Service Desk)
8.	***Remote Access Security:*** a. Use of HESCOM owned laptops for remote access into the OT devices b. TCP port numbers should be changed for well-known remote access protocols from their defaults c. VPN should be configured such that split tunneling is not allowed by technical policy d. All remote access sessions should be monitored and logged (log user ID, time, and duration of remote access) e. Require multi-factor (e.g. two-factor or greater) authentication for any remote access sessions; f. Ensure that the IDS (Intrusion Detection System) inspects all traffic that enters and leaves the VPN tunnel.
9.	***Establishment of SCADA "Red Teams"*** – A "Red Team" may be established to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, SCADA systems, physical systems, and security controls. People who work on the system every day have great insight into the vulnerabilities of SCADA network and should be consulted when identifying potential attack scenarios and possible consequences.

Approved by HESCOM BoD

5. Definitions

a. **Insufficient Authentication Controls** - An attacker could use a brute-force attack to determine the password of one account; if other accounts are connected to it through a single-sign-on arrangement, the attacker would then have administrative access to a number of systems.

b. **Cross Site Scripting (XSS)** - Cross site scripting is a type of attack in which the victim's web browser is induced to execute malicious code. Depending on the type of attack, the malicious code may steal the victim's personal information, enabling the attacker to impersonate the victim, or cause the victim's computer to launch an attack against a third party without either the victim's or the third party's knowledge

c. **Cross Site Request Forgery (CSRF) -** Cross site request forgery is an attack which causes an end user's web browser to execute actions of the attacker's choosing without the user's knowledge. By embedding a malicious link in a web page or sending a link via email or chat, an attacker may cause the users of a web application to perform unwanted actions. More specifically, the attacker causes the user's browser to make requests to a web site to which it has been authenticated, without the user's or the web site's knowledge. These actions may result in compromised end user data and operations, or even an entire server or network.

d. **Phishing** - Many people view social media sites on cell phones or other mobile devices. This makes it harder to distinguish real and fake web sites. Additionally, social media enables attackers to send phishing messages that appear to come from someone that the victim knows. Having obtained login information for a few accounts, scammers will then send out messages to everyone connected to the compromised accounts, often with an enticing subject line that suggests familiarity with the victims.

e. **Information Leakage** - Social media sites like Facebook and Twitter create the illusion of familiarity and intimacy on the Internet. The result is that people may be inclined to share information on the Internet that their employer would have preferred to keep private. Individuals may not be divulging trade secrets, but the cumulative effect of small, seemingly innocuous details can enable a business's competitors to gain valuable intelligence about that company's business situation and future plans.

f. **Injection Flaws**: The technologies that social media uses make it vulnerable to injection attacks such as XML injection. Additionally, social media applications often rely on client-side code, so they rely heavily on client-side input validation which an attacker can bypass.

g. **Information Integrity** - Data integrity is one of the foundations of information security. Malware introduced on a platform or network can modify user information and databases. Users who do not diligently update their antivirus software can make their systems vulnerable. An attacker could deliberately modify data in transit or storage through malware or direct manipulation, but legitimate

Approved by HESCOM BoD

users also make honest mistakes. Unintentional misinformation is frequently posted on the Internet, which is then taken as fact by many viewers. In social media, data is stored in many places where many different users can access it. Having data accessible to many users increases the chance that a malicious or mistaken user could post inaccurate information, which compromises data integrity.

Approved by HESCOM BoD

6. References

S. No.	Reference
1	SANS Institute- Workstation Security Policy
2	SANS Institute- Web Application Security Policy
3	SANS Institute- Server Malware Protection Policy
4	SANS Institute - Reducing the Risks of Social Media to Your Organization
5	SANS Institute- Email Policy
6	CERT-In Security Guideline CISG -2003-05 – Anti-Virus Policy and Best Practices
7	ISO/IEC 27001
8	Record Retention Schedule- Govt. Of India
9	Information Technology Act-2000 and its amendment
10	Personal Data Protection Bill, 2019
11	https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

Approved by HESCOM BoD

SECTION II: Cyber Security Policy

Approved by HESCOM BoD

7. Introduction

A Cyber Security Policy document is a set of rules outlined for the personnel of an organization who have been given access to the organization's technology and information assets.

The most important purpose of the Cyber Security Document is to inform the personnel, contractors and other authorized users & stakeholders of the organization, of their obligatory duty to protect the technology and information assets of the company. The document helps identify the threats to the technology and information assets.

The Cyber Security Policy highlights on the user's responsibilities and privileges along with user limitations and penalties for violation of the policy.

What are we Protecting?

It is the duty of all the officers/employees of an organization to protect the technology and information assets of the company from unauthorized access, theft and destruction. The technology and information assets include:

- Computer Hardware, CPU, Disk, Applications Servers, Web, PC Systems, Application Software, System Software, E-Mail etc.
- System Software includes: Operating Systems, Database Management Systems, Back-up and restore software, Communication Protocols and so forth.
- Application Software include: Custom written Software applications, and commercial off the shelf software packages.
- Communications Network Hardware and Software includes: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

Approved by HESCOM BoD

8. Policy Stakeholders

This policy takes into consideration the below policy stakeholders:

A. Top Management: The officers who approve the security policy and security budgets; review the security implementation efforts, take note of the effectiveness of various measures and decide on the priorities. Involvement of top management will induce the organization to take security matters seriously.

1. Management
2. Application Owner
3. Asset Owner
4. Business Owner
5. Business Risk Committee
6. Chief Information Security Officer
7. Data Custodians

B. Security Management Team - Security Management within HESCOM should be comprised of the following teams. These teams can be drawn from the personnel or some of these activities can be outsourced to suitable third parties.

1. Emergency Management
2. Enterprise Architecture
3. Enterprise Operations
4. Ethics and Compliance
5. Incident Management Team
6. Information Security
7. Information Technology
8. Internal Audit
9. Legal
10. Managers
11. Risk Owner
12. Service Desk
13. Service Continuance Team
14. Third Party Relationship Owner
15. Third Party Risk Management Program Office
16. Workforce Members

Approved by HESCOM BoD

C. **End Users:** End users include personnel on the payroll and others acting in a similar capacity, such as contractors, consultants, trainees, employees and officers etc. Any user failing to comply with the security policies could be subject to disciplinary action as per the company regulation

This policy document takes into consideration the below three categories of end users in HESCOM:

1. Management
2. Corporate Users
3. IT/OT/IoT Core Users

This Cyber Security policy shall be reviewed and updated as and when required or at least once in a year.

Approved by HESCOM BoD

9. Cyber Security Policy

9.1. Application Security Policy

Purpose:

The purpose of this policy is to ensure that application development activities follow HESCOM development methodology which incorporate information security controls throughout the development process.

Scope:

This policy is applied to all systems and applications that collect, maintain, process, or transmit HESCOM Information.

Roles and Responsibility:

Roles	Responsibilities
Chief Information Security Officer (CISO)	• Establishes requirements for secure application development of HESCOM Information Systems • Coordinates with HESCOM's Information Security and Application Owner to ensure proper application development
Application Owner	• Owns or delegates ownership of applications • Engages technical resources to ensure security requirements for an application are met throughout the development process
Information Security	• Establishes requirements for secure application development and deployment of HESCOM Information Systems • Protect and preserve the confidentiality, integrity, and availability of HESCOM's Information and Information Systems
Information Technology	• Ensures that all desktop applications have been securely developed and tested prior to their installation on HESCOMs managed devices • Provide a secure development environment for developers and approve the software/tools used to develop applications
Service Desk	▪ Provides technical assistance and support for incoming queries and issues related to computer systems, software, and hardware

Approved by HESCOM BoD

Policy:

A. Secure application development

1. Developers must use proper security controls, such as operating system authentication, certified software, and certified encryption processes.
2. A secure environment (i.e., Development, Test, Quality Assurance, and Production Environment), must be provided for development activities and developer access must be limited in the Production Environment.
3. Applications must use standard ports and services.
4. All applications that transmit, process, or store Confidential, Restricted, or Internal information must do so in a secure manner using approved encryption tools and protocols. Refer to Information Protection Policy for further detail.
5. All applications must follow industry standard best practices for System Development Life Cycle (SDLC) process.
6. Applications must be tested for vulnerabilities, including security and other patches, prior to production deployment.
7. Production installations must be properly controlled to minimize the risk of disruption to production Information Systems.
8. Applications must be installed in the Production Environment without disruption to Information processing activities.
9. Prior to an application entering production, Workforce Members responsible for maintenance and administration must complete training on Information security tasks and responsibilities.
10. Applications for PCI (payment card industry) Systems must be developed in accordance with PCI DSS (data security standard) specifications which are based on secure coding guidelines, such as those recommended by the Open Web Application Security Project (OWASP) Guide. Considerations for secure development include, but are not limited to, the following:
    - Prevention of input vulnerabilities (i.e., cross-site scripting, injection flaws, malicious file execution).
    - Proper error handling.
    - Secure cryptographic storage of card holder data (CHD).
    - Secure communications of CHD.
    - Proper restrictions of URL access.
11. All applications purchased from third party vendors for PCI Systems, must adhere to the PCI DSS requirements for secure applications.
12. All downtime requests must follow the downtime notification and approval process.

Approved by HESCOM BOD

B. Secure code development and review

1. Developers must use a secure source code library that has authentication, version control, and logging enabled.
2. Source code may not be accessed or available to anyone except the application developers and owners.
3. Software that is developed by/for HESCOM is considered intellectual property and must be safeguarded and preserved for future reference and use.
4. Developers must be trained annually to write secure code.
5. Source code for applications must be peer-reviewed by a developer who did not write any of the code prior to its deployment into the HESCOM Production Environment.
6. A copy of the source code for all applications developed by third parties specifically for HESCOM must be provided to HESCOM and stored in a secure source code library.
7. All internally developed applications must have a secure code review.
8. All application security issues discovered during the secure code review must be remediated prior to implementation into a Production Environment.
9. All applications must be approved by Information Security before they are permitted for use in Production Environments.
10. To reduce the potential for unauthorized changes to source code and/or software corruption, secure source code libraries must:
    - Restrict access to designated development Workforce Members;
    - Segregate source code for applications under development from source code for applications in production;
    - Periodically archive outdated versions of source code; and
    - Follow formal change management process as referenced in the Asset Management Policy.

C. Minimum access and segregation of duties

1. Development, Test, QA, and Production Environments must be separated physically or logically to reduce the risk of accidental changes or unauthorized access to production software and data.
2. Access to production Information Systems must be limited and controlled in accordance with Workforce Members job responsibilities.
3. Development and production maintenance duties must be assigned to Workforce Members to ensure segregation of duties and limit the risk of unauthorized changes or access to data.
4. If Confidential, Restricted, or Internal information is necessary in Non-Production Environments, per business need, Confidential, Restricted, or Internal data elements must be de-identified or redacted immediately following their use.
5. The amount of Confidential, Restricted, or Internal information used within a Non-Production Environment must be limited to what is required to perform testing.
6. Access to Confidential, Restricted, or Internal information in Non-Production Environments must be limited to Workforce Members with a validated business need.

Approved by HESCOM BoD

7. Developers must be restricted from modifying production source code or production data and engineers must be restricted from modifying system settings, unless approved by Information Security.
8. If test accounts are used in Non-Production Environments, they must be removed before the application is moved into the Production Environment.
9. Test accounts and test data is not allowed to be used in Production Environments.

D. Managing business requirements and risks

1. Business requirements for systems/applications under development or being licensed must be assessed to ensure the information security controls designed into systems/applications are sufficiently aligned with identified risk(s) and system/application criticality.
2. Risk assessments must be performed for applications under development or being purchased to determine the controls required to mitigate application risks to acceptable limits.
3. All outsourced software development efforts must be subjected to the same risk assessment requirements as internal development efforts.
4. Applications based on macro languages, scripting languages, or Third-Party tools must follow approved change management processes prior to installation on production systems.
5. The risk of compromising built-in security controls must be assessed if a software package must be modified. Further analysis must be completed to determine if a change to the application would void the vendor's warranty, support obligations, and/or future updates from the vendor, and assess the impact if HESCOM becomes responsible for maintaining the application.

E. Application testing

1. Information security features and controls must be tested prior to release in a production environment; Confidential, Restricted, and Internal test data must be secured.
2. Security features of new applications or significant changes to existing applications must be properly tested, documented, and reviewed prior to promotion to a Production Environment.
3. All application security features and the results of security verification tests must be reviewed and remediated with Application Owners prior to application installation and use.
4. Evidence of security verification tests must be documented and classified as Confidential. Evidence must include who performed the test, the nature of the tests performed, the results of those tests, and any remediation activities required/performed.
5. Application test data must be adequately safeguarded to ensure unauthorized Workforce Members are not inadvertently granted access to Confidential, Restricted, or Internal data.
6. All applications must be tested to ensure separation of duties controls are appropriately functioning.
7. Vulnerability scans must be performed and identified vulnerabilities remediated prior to an application being deployed into a Production Environment.
8. All new applications or applications that undergo a major update are subject to a vulnerability scan.

Approved by HESCOM BoD

9. Internet-facing or remotely accessible applications must periodically undergo an independent penetration test.
10. Information Security must evaluate and approve the security controls of new applications developed in-house prior to the application being deployed into a Production Environment.
11. Existing applications must be re-evaluated and re-approved by Information Security after a significant change is made to the application or after a predetermined period.

F. Maintenance

1. All necessary patches must be installed on the new application in a timely manner.
2. A version control numbering scheme must be used to reflect when updated versions of the software are installed.
3. All downtime requests must follow the scheduled downtime notification and approval process.
4. All applications must undergo a code review and a security review after major version changes or every two (2) years, whichever comes first.
5. Changes to configuration parameters within the application (where applicable) must go through testing.

G. Disposal

1. At the end of an application's life, all equipment used to host the application or to develop and maintain the application must be disposed of according to the Asset Management Policy.
2. All data used or maintained by an end-of-life application must be destroyed or retained in a secure manner, as determine by Asset Management Policy.
3. For end of life applications, the source code must be archived so that it can still be retrieved by Information Security if necessary.

9.2. Acceptable Use Policy

Purpose:

The purpose of this policy is to outline the information security and privacy requirements for the acceptable use of HESCOM Information, electronic and computing devices, and network resources.

HESCOM established the following policy to:

- Protect against inappropriate use of HESCOM's Assets; and
- Reduce exposure to risks, including virus and ransomware attacks, compromise of network systems and services, and regulatory issues.

Approved by HESCOM BoD

Scope:

This policy applies to all Workforce Members who use HESCOM computing devices, data, or network(s) to conduct business or interact with internal networks and business systems.

Roles and Responsibility:

Roles	Responsibilities
Information Security	• Protect and preserve the confidentiality, integrity, and availability of HESCOM's Information and Information Systems • Verify compliance to this policy through various methods, including but not limited to, business tools reports, internal and external audits, and feedback from Workforce Members
Service Desk	• Provide technical assistance and support for incoming queries, issues related to computer systems, software, and hardware, and potential security incidents
Workforce Members	• Adhere to the information security and privacy requirements outlined in this policy • Promptly report the theft, loss or unauthorized disclosure of HESCOM Assets

Policy:

A. General Acceptable Use

1. HESCOM Information must be protected from unauthorized access with appropriate Safeguards, as defined by Information Security.
2. Workforce Members are responsible and accountable for all activity they conduct when using Business Tools and/or accessing HESCOM Information. Workforce Members must:
    a. Acknowledge and adhere to HESCOM's policies and HESCOM's Code of Conduct prior to, or within 90 days of, commencement of employment or engagement.
    b. Sign the appropriate confidentiality agreement(s) before accessing HESCOM's Information. These may include a Non-Disclosure Agreement (NDA), a Business Associate Agreement (BAA), or other agreements as deemed necessary and appropriate by HESCOM, its counsel, regulations, and/or local, state, and federal laws.
    c. Workforce Members must only access HESCOM Information and Business Tools when required and appropriately authorized to fulfill their job duties.

Approved by HESCOM BoD

d. Use Business Tools for official business purpose; limited personal use of HESCOM Business Tools is acceptable, provided this use does not interfere with the performance of one's job duties, the efficient operation of HESCOM networks or devices, or otherwise conflict with HESCOM interests.
e. Ensure the confidentially of HESCOM Information that may be displayed on their screen in public locations; privacy screens must be utilized.
f. Ensure Business Tools are not be left unattended, unless securely locked, on desks or in automobiles to avoid theft or loss of the device.
g. Report any potential information security and privacy issues to the Service Desk immediately. Examples include, but are not limited to:
    a) Detected viruses or malware;
    b) Any loss of HESCOM's Assets, including Personally-Owned Devices that may contain HESCOM's Information; and
    c) Improper viewing, modification, or inappropriate or unauthorized access to Information or Business Tools.
h. Be aware of, understand, and acknowledge that HESCOM reserves the right to monitor all devices, Business Tools, Electronic Communication, and network traffic for security, compliance, performance, or for any other reason deemed necessary, in accordance with privacy laws and regulations.
i. Acknowledge and accept that HESCOM reserves the right to disconnect, modify, secure, create backups, or perform eDiscovery/forensics analysis on any device, whether HESCOM-owned or personally-owned, that contains HESCOM Information.

3. HESCOM Information stored on any hardware or electronic media, whether leased or owned by HESCOM, Workforce Member, or a third party—remains the sole property of HESCOM. As such, all Information must be categorized and protected in accordance with relevant information security and privacy policies, regulations, and laws.
4. When Confidential electronic Information is printed, the paper copies must be treated with an appropriate level of sensitivity based on the document's classification level as outlined in the Data Classification Policy and securely disposed of when no longer needed.
5. Workforce Members are prohibited from engaging in any Restricted Services using HESCOM-owned Business Tools, devices, or network.

B. Computer Use

1. User Adherence
    a. Workforce Members must surrender HESCOM-owned devices and property (including, but not limited to computers, mobile devices, and access badges) and/or remove HESCOM data upon transferring or leaving the company.
    b. If Workforce Members fail to do so, HESCOM reserves the right to initiate a process to remotely wipe and delete all data on computers that have access to HESCOM Information and/or Business Tools.

Approved by HESCOM BoD

2. Security Safeguards
    a. All computers and applications with access to HESCOM's network and/or Information must be configured to time out in accordance with Information Security thresholds; attempting to bypass this security control is prohibited.
3. Information Storage and Protection
    a. HESCOM prohibits the copying, moving, or storing HESCOM sensitive information onto local hard drives, removable Media Devices, and non-approved HESCOM cloud storage.
    b. HESCOM Information stored on local hard drives or other removable data storage media (e.g. USB, external hard drive, etc.) must have appropriate administrative, technical, and physical safeguards applied, including use of HESCOM-approved encryption methods, in accordance with HESCOM's Information Protection Policy.
    c. Only cloud-based storage solutions approved by Information Security may be used to store HESCOM-owned Information.
    d. Workforce Members must store all Non-Public Information in approved designated network storage locations; storage of Confidential Information on local computer hard drives is strictly prohibited.
4. Unacceptable Use
    a. Computers must not be used for Solicitation or Distribution in compliance with HESCOM's Solicitation and Distribution Policy.
    b. Workforce Members must not use computers to send, upload, or download copyrighted materials, trade secrets, proprietary financial Information, or similar materials, in accordance with the law.
    c. Devices accessing the HESCOM network must not be used for any activity that could cause network congestion and/or disruption of networks and systems due to non-business activities.
    d. Storing non-HESCOM data on HESCOM's assets is prohibited.

C. Internet Use

1. User Adherence
    a. Workforce Members must be responsible for all activity they conduct on the HESCOM provided internet.
    b. All wireless access points must be configured in accordance with Information Security specifications.
2. Unacceptable Internet Usage
    a. Workforce Members are not to give the impression that they are representing or providing opinions on behalf of HESCOM unless otherwise authorized.
    b. Social networking sites, such as Facebook, Twitter, LinkedIn and Google+, must not be used to store, share, or disseminate HESCOM Information.
    c. Accessing websites with objectionable or malicious content is prohibited (e.g., adult/sexually explicit material, gambling, illegal drugs, peer-to-peer file-sharing, personals and dating, violence, intolerance, and hate).

Approved by HESCOM BoD

d. Websites determined to be compromised or contain potentially malicious content must be blocked by Information Security.
e. Illegal use of HESCOM-provided Internet services should be prohibited.
f. The use of anonymized network routing protocols is prohibited on the HESCOM Network.
g. Workforce Member's Personally-Owned Devices authorized to access the HESCOM network are prohibited from connecting to the guest network for business purposes.
h. HESCOM-managed devices are prohibited from connecting to the guest network to bypass security controls, including accessing blocked websites.
i. The use of HESCOM's guest network(s) for any malicious or fraudulent purposes is prohibited.

D. Software Use

1. User Adherence
    a. All software usage must follow applicable user licenses, contracts, and agreements.
    b. HESCOM reserves the right to conduct software audits at any time. Unlicensed software will be removed, and a report shall be provided to management.
2. Unacceptable Use of Software
    a. The following activities are strictly prohibited:
        i. Development of any form of computer virus or malicious code fragment.
        ii. Intentional distribution of a virus, worm, Trojan, or any other malicious code or software, regardless of type (nuisance, destructive, etc.) for any reason or by any method.
        iii. Downloading or installing any unlicensed or malicious software programs or hacking utilities (such as network sniffers, scanners, and password cracking programs) onto any computer that may be attached to HESCOM network, unless approved by Information Security for a valid business need.
        iv. Use of unlicensed or pirated software is prohibited.
        v. Intentional tampering with or altering of software programs from their original form in a manner that violates their integrity and trustworthiness.
        vi. Creation or use of back doors or other technical workarounds which have the intent or effect of bypassing HESCOM security controls.
        vii. Any unapproved or unauthorized modification or reconfiguration of applications installed by HESCOM.
        viii. Workforce Members must not use HESCOM-owned Business Tools, networks, or Media Devices to operate unlicensed software and/or peer-to-peer file transfer services.
    b. The following activities are prohibited unless permitted by Information Security and Information Technology:
        i. Installation of software not licensed to HESCOM, freeware, shareware, and/or software downloaded from the Internet on Business Tools.
        ii. The use of HESCOM-owned software on a Personally-Owned.

Approved by HESCOM BoD

iii. The use of personal software on HESCOM's Business Tools.

c. Disabling or otherwise reconfiguring any security software or control without prior authorization is prohibited. This includes anti-virus software, account lockouts, web content filtering, firewalls, and hardware or software restrictions.

E. Use of Copyrighted material

1. Workforce Members must comply with all laws pertaining to copyright protection.
2. Workforce Members are prohibited from downloading, recording, storing, playing, uploading, transmitting, making available, or otherwise distributing copyrighted material not owned by or licensed to HESCOM.
3. Workforce Members must limit personal use of copyrighted materials owned or licensed by HESCOM on Media Devices.
4. Workforce Members must acquire appropriate licenses before installing or using copyrighted material on a HESCOM-owned computer system and must not use the copyrighted material beyond the scope of the license.
5. Unlicensed copyrighted material on HESCOM's Business Tools, networks, and Media Devices will be removed, without notice, by HESCOM.

F. Electronic Communication

1. User Adherence
    a. Electronic Communications (e.g., electronic mail, instant messages, text messages, and online meeting platforms) conducted on HESCOM's devices, data, or network will be deemed a business record and may be in-scope for monitoring or review in the event of litigation.
    b. All HESCOM Electronic Communications are subject to monitoring, review, inspection, disclosure, and removal without prior notice or permission from the user.
    c. Forwarding or sending electronic email with Confidential Information, to the sender's personal email accounts is prohibited.
    d. Transmission of any Confidential and Restricted Information to any recipient outside of HESCOM's electronic mail system must be encrypted.
    e. Electronic mail must be archived in accordance with HESCOM's Information Protection Policy and local, state, and federal laws; it may be monitored, reviewed, and restored at the discretion of management.
    f. Electronic mails must be professional in all aspects.
    g. HESCOM-initiated web meetings must be conducted via a secure method with both internal and external users provided the following requirements are followed:
        - Pass codes must be required to join the meeting.
        - Confidential Information must only be shared when needed, and it must be the minimum necessary Information.

Approved by HESCOM BoD

- Presentations that contain Confidential Information must not allow attendees to download or record the Information.
- Meeting host credentials must not be included in meeting invitations.

2. Unacceptable Use of Electronic Communication
    a. Forwarding HESCOM electronic mails to external addresses, including personal electronic mail accounts (e.g., Google, Hotmail, Yahoo, AOL, etc.) is strictly prohibited without prior approval and authorization from a Workforce Member's Manager.
    b. Unauthorized access, interception, or disclosure of any Electronic Communication is prohibited.
    c. Workforce Members must not send credit card numbers, passwords, or any other security data that can be used to gain access to services via any Electronic Communications.
    d. When using electronic mail to communicate, Workforce Members must adhere to the following requirements:
        - The use of electronic mail must be consistent with all Information Security policies and all relevant industry standards and applicable local, state, and federal laws.
        - Obscuring, disguising, or otherwise hiding ones' identity or role at HESCOM in an electronic mail is prohibited. External users who have been issued HESCOM electronic mails must not purport to be HESCOM personnel.
    e. Workforce Members must not use personal electronic mail accounts (e.g., Google, Hotmail, Yahoo, AOL, etc.) to send business-related electronic mail; always use a HESCOM-issued electronic mail account.
    f. Workforce Members must not open an unknown or unexpected electronic mail attachment; all unknown or unexpected attachments must be reported to the Service Desk for further investigation.
    g. Electronic mails from unknown senders or suspicious electronic mails that violate this policy must not be opened; they must be reported to the Service Desk.
    h. Workforce Members must not send unsolicited bulk electronic mail (UBE).
3. Subscribing a HESCOM-issued electronic mail address to mailing lists is prohibited unless directly related to HESCOM use.
4. Subscribing other Workforce Members to any electronic mailing lists without their prior permission is prohibited.
5. Workforce Members are prohibited from sending Sensitive Information, or other Non-Public Information via instant message, text message, and paging systems.

G. Bring your own Device (BYOD)

1. Only approved Personally-Owned Devices with HESCOM-managed Mobile Device Management controls are allowed to connect to HESCOM's network.
2. All device users must:
    a. Comply with all applicable regulations and related HESCOM policies, standards, and procedures.

Approved by HESCOM BoD

b. Agree to safeguard the Personally-Owned Devices from unauthorized users by protecting the device/HESCOM Information from unauthorized access and/or disclosure.
c. Be cautious when connecting to an unsecured or public network.
d. Keep devices updated with Information Security approved operating system and security patches.
e. Ensure anti-virus and malware protection software is enabled where technically feasible.
f. Immediately notify the Service Desk of lost, stolen, or potentially compromised Personally-Owned Devices.
g. Not copy Non-Public Information from electronic mail, calendar, contact applications, or any other HESCOM-owned, managed, or installed application to applications on an unregistered Personally-Owned Device.
h. Not store Non-Public Information on the Personally-Owned Device outside of HESCOM approved and/or managed applications.
i. Not modify approved operating system configurations (i.e., jail break a device).
j. Not make any unauthorized reconfigurations to Personally-Owned Devices.

9.3. Asset Management Policy

Purpose:

The purpose of this Policy is to define the minimum requirements HESCOM Workforce Members must follow to ensure proper identification, inventory, handling, and management of Assets that enable HESCOM's business objectives.

This Policy establishes the information security requirements to ensure HESCOM:

- Identifies the devices and systems that enable business objectives;
- Manages Assets in a manner consistent with the asset's relative importance to business objectives; and
- Prevents unauthorized disclosure, modification, removal, or destruction of data stored on media.

Scope:

The Policy is for internal use at HESCOM and is applicable to all Workforce Members. HESCOM computing devices and mobile devices fall within scope of this policy. This Policy also applies to personally-owned mobile devices (BlackBerry, iOS devices, Android, Windows, etc.) that are the property of HESCOM Workforce Members which process, transmit, or store HESCOM Information.

Roles and Responsibility:

Approved by HESCOM BoD

Roles	Responsibilities
Asset Owners	• Owns or delegates ownership of Assets • Oversees the categorization of Assets in coordination with Information Security and Information Technology • Ensures maintenance of HESCOM-owned asset records in the system of record • Communicates any legal, regulatory, or contractual requirements (e.g., data protection, privacy, evidence collection) to appropriate stakeholders, such as IT, Third Parties, and affiliates. • Ensures a new Asset Owner is designated if circumstances warrant a change in ownership • Define and periodically review access restrictions
Chief Information Office	• Delegates ownership and responsibilities to an Asset Owner • Ensures that duties and areas of responsibility are segregated to reduce opportunities of unauthorized or unintentional modification or misuse of Assets
Information Technology (IT)	• Establishes the mechanisms to maintain the inventory of Assets • Manages the status of all centrally-managed assets throughout the asset lifecycle • Communicates Asset ownership roles, responsibilities, and duties • Oversees the categorization of Assets in coordination with the Asset Owner and Information Security • Works with Asset Owners to validate the accuracy of the Asset details
Information Security	• Defines the Asset management information security requirements • Oversees the categorization of Assets in coordination with the Asset Owner and Information Technology

Policy:

A. Ownership of Assets

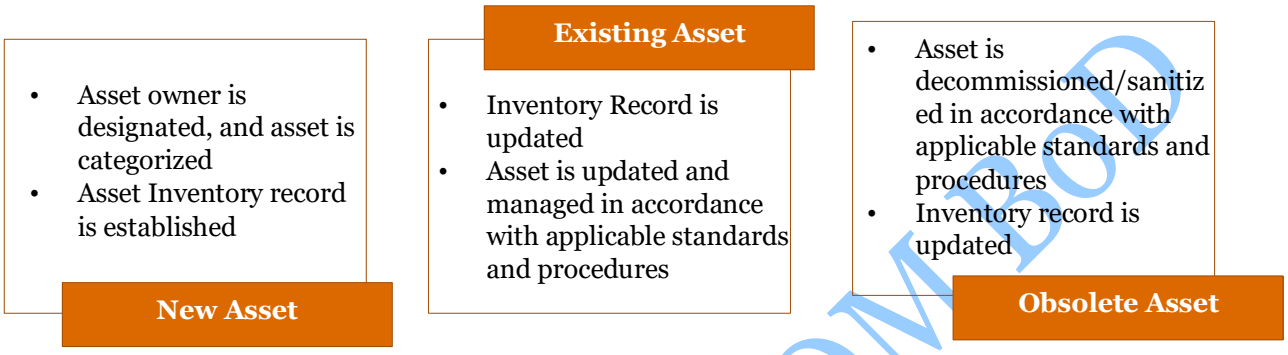
All Assets must have a designated Asset Owner.

B. Inventory of Assets

1. Inventory Lifecycle

Approved by HESCOM BoD

a. HESCOM must record and maintain an inventory of all Assets in accordance with the Inventory lifecycle.



2. Information Technology (IT) must provide a centralized mechanism to maintain an inventory of Assets. HESCOM's Asset inventory must, at a minimum, include:
   a. Physical devices and systems connected to the HESCOM network, including laptop and desktop computers, servers, network devices and appliances (e.g., switches, routers, and firewalls), mobile devices (both HESCOM owned and personally-owned), media containing Non-Public Information.
   b. Software platforms (e.g., operating system) and applications.
   c. External Information Systems (e.g., off-premise/cloud services).
   d. Member and/or customer data storage locations.
3. Each Asset must at minimum have the following information:
   a. Asset name;
   b. Asset tag/serial number;
   c. Asset owner;
   d. Location;
   e. Categorization;
   f. Data Classification; and
   g. Business value.
4. The Asset inventory must be updated in a timely manner throughout the asset management lifecycle.

C. Audit of Asset Inventory

ICT and MIS Section, HESCOM must establish a process to review, at least quarterly, the Asset inventory.

D. Categorization of Assets

1. HESCOM must maintain an appropriate set of procedures to categorize Assets.

Approved by HESCOM BoD

2. Asset Categorization must be conducted with the involvement of Information Security Team, ICT & MIS Section, Business Owners and Asset Owners.
3. Asset Owners must ensure Assets are appropriately categorized based on:
    - Their impact and value to the business if lost or unavailable;
    - The Data Classification, based on classification of data stored, transmitted, or processed by the Asset, in accordance with HESCOM's Information Classification Policy mentioned in Section 3.20;
    - Their accessibility (accessible from Internet; physical).
4. In cases where Information Systems store or process more than one type of data based on its classification level, the highest level of Data Classification label will be used for Categorization purposes.

E. Management of Assets

1. Asset Owners must ensure Assets under their purview are correctly managed in order to protect the Asset's confidentiality, integrity, and availability.
2. Assets are maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance Workforce Members must be required to carry out services for all Assets.
3. All Workforce Members must comply with HESCOM's requirements to protect Assets in accordance with HESCOM's Acceptable Use Policy.
4. Information Technology must establish procedures to control the installation of software on operational systems.
5. All changes (scheduled and unscheduled/emergency) to Information Systems' configuration or lifecycle must be managed and documented through a formal change management process.
    a. Changes must be logged, reviewed, and authorized prior to implementation to protect against improper modifications before, during, and/or after system/application implementation.
    b. A record of changes must be maintained for the purpose of maintaining program, application, and/or system version control.
    c. Records must be maintained in accordance with HESCOM's data retention guidelines.
6. All software changes, including security changes and patch implementation, must be tested prior to deployment in a production environment.
7. Exceptions for software change testing may be made in the event of an imminent critical system failure or security threat. Changes must be reviewed and approved by a change review committee after implementation.

F. Management of Removable Media

1. ICT & MIS, in coordination with Information Security, will designate approved forms of removable media and storage devices (i.e., removable USB flash drives, external hard drives).
2. Only approved removable media and storage devices may be used to store HESCOM Information.

Approved by HESCOM BoD

a. If no longer required, the contents of any re-usable media device must be securely deleted and made unrecoverable.

3. Business Units must provide the Third Party with written termination instructions which detail the requirements for how they Third Party should handle, return, or destroy HESCOM Assets.

G. Return of Assets

1. ICT & MIS section of HESCOM must establish a process to manage and facilitate the timely return of Assets by Business Units and Workforce Members.
   a. Assets must be returned to the Asset management team under ICT & MIS section of HESCOM:
      i. When the Asset is no longer needed by the Business Unit or the Workforce Member;
      ii. When the Asset has reached End of Life; or
      iii. In the case of a termination or change of job role/scope.
   b. When a Workforce Member is terminated, Assets must be returned on or before the Workforce Member's last day.

H. Sanitization of Assets

1. ICT & MIS Section, in coordination with Information Security, must establish and implement appropriate information security requirements to safeguard the Information contained within used Assets prior to disposal or reuse.
   a. Documented plans and procedures must ensure that, where applicable, the Information contained in the Asset is retained and readily retrievable for the record retention period in accordance with HESCOM's data retention guidelines.
2. Assets that store Information, prior to disposal or reuse, must be sanitized
   a) The type of sanitization required will consider the Asset categorization. Information Security approves all sanitization methods.
   b) Data sanitization procedures must include logging details of the destruction, including a date and time stamp and the method of destruction.

I. Disposal or Reuse of assets

1. Assets that have reached End-Of Life status (e.g., due to changes in processes, adoption of new technology, termination of product support) must be securely replaced, destroyed, and/or decommissioned.
2. Use of an Asset after it reaches End of Life status requires approval from Information Security to manage associated risks.

Approved by HESCOM BoD

9.4. Contingency Planning Policy

Purpose:

The purpose of this policy to establish and implement (as needed) the criteria for contingency plans for HESCOM to recover key systems and data in the event of significant events that disrupt the operation of Information Systems.

Scope:

The policy applies to all systems and applications that collect, maintain, process, or transmit HESCOM Information and is applicable to all Workforce Members.

Roles and Responsibility:

Roles	Responsibilities
Information Security Team	• Oversee governance and management of Information Security activities • Oversee the management of the contingency planning procedures and activities • Oversee the training and maintenance of the contingency plans
Service Continuance Team	• Develop, test, and maintain contingency plans • Conduct Business Impact Analysis (BIA) • Help communicate and send contingency plans to appropriate teams • Develop playbooks for IT emergency response procedures

Policy:

A. Contingency Planning Process

1. HESCOM must develop and maintain an effective Information System contingency plan processes. Each contingency plan must:
    a. Contain the Business Impact Analysis (BIA);
    b. Identify preventive controls;
    c. Create contingency strategies;
    d. Ensure plan testing, training, and tabletop exercises; and
    e. Ensure plan maintenance.
2. The Service Continuance Team or other responsible team is responsible for developing, maintaining, and testing of HESCOM's Information System contingency plans and playbooks.

Approved by HESCOM BoD

3. The contingency plan must assign specific responsibilities to designated staff or positions to facilitate the recovery and/or continuity of essential system functions.
4. Workforce Members responsible for critical Information Systems must be trained to execute contingency plans.
5. The contingency plan recovery capabilities must be tested periodically to identify weaknesses of the capability.
6. Contingency plans must be made available in a convenient form for use by the Service Continuance Teams and must be reproduced for distribution to all System Recovery Teams.
7. Where critical services are outsourced, HESCOM must ensure that suppliers agree to have similar suitable plans and contingencies in place to meet the criteria for critical systems.

B. Types of Contingency Plans

The contingency plans include, but are not limited to, the following:

1. Disaster Recovery Plan
    i. HESCOM must implement a disaster recovery plan that details the process to recover HESCOM's Information Systems and Information in the event of a disaster. The plan should include:
        - Notification of proper personnel and authorities;
        - Roles and responsibilities of recovery team personnel;
        - External communication plan (as required);
        - Data and system restoration;
        - Equipment restoration procedures;
        - Security procedures for Confidential and Restricted data during a disaster;
        - Testing and training of recovery procedures; and
        - Maintenance and lessons learned.

    ii. Disaster recovery plans must accommodate for electronic or physical Information to be backed up and stored offsite in a safe and accessible location in case of a disaster.

    iii. Disaster recovery plans must ensure procedures and plans are developed and implemented for critical business systems to ensure timely resumption of essential services.
2. IT Business Continuity Plan
    i. HESCOM must have a business continuity plan that details how Information Systems would function in the event of a disaster or disruption to key operations to continue providing services to the organization.
3. Back-up Plan
    i. HESCOM must implement a backup plan that outlines the requirements for backing up data to recover key systems. The backup plan should document the following:
        a. The frequency of data backup;
        b. The type of data backup;

Approved by HESCOM BoD

- Delta backup (differential or incremental)
- Full backup

c. The media used to store the backup; and

d. The location of the backup storage.

ii. Infrastructure and Operations Department must conduct regularly scheduled backups to maintain the ability to recover from the loss of data caused by adverse events.

iii. All Information Systems containing Confidential must be regularly backed up, tested, and securely stored.

C. Business Impact Analysis

1. The Service Continuance Team must conduct a business impact analysis (BIA) that correlates the Information System with the business processes and services provided.
2. Results from the BIA must be appropriately incorporated into the analysis and strategy development efforts for HESCOM's contingency plans (e.g., disaster recovery plan and contingency plan).
3. The Service Continuance Team must:
   a. Determine business processes and recovery criticality along with outage impacts and estimated downtime. Downtimes must be identified in the following ways:
      i. Maximum Tolerable Downtime (MTD)
      ii. Recovery Time Objective (RTO)
      iii. Recovery Point Objective (RPO)
   b. Identify resource requirements.
   c. Identify recovery priorities for system resources.

D. Identified Preventive Controls

1. The Enterprise Operations Team must identify impacts that can be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impact to the system. Some common measures are listed below:
   a. Offsite storage of backup media, non-electronic records, and system documentation;
   b. Technical security controls; and
   c. Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often they are recirculated and moved to storage.

E. Contingency Strategies

1. HESCOM must create contingency strategies to mitigate the risk arising from use of HESCOM Information Systems and Information.
2. Systems must be backed up annually at a minimum, or as determined by the Service Continuity Team based on the results from Business Impact Analysis.

Approved by HESCOM BoD

F. Plan Testing, Training and Exercise

1. HESCOM must train appropriate Workforce Members to execute contingency plans.
2. The Service Continuity Team must be trained on the following plan areas:
    a. Purpose of the plan;
    b. Cross team coordination and communication;
    c. Reporting procedures;
    d. Security requirements;
    e. Team-specific process; and
    f. Individual responsibilities.
3. The contingency plan (e.g., Disaster Recovery, Backup, and Business Continuity) recovery capabilities must be tested periodically to identify weakness of the capability.
4. The following areas must be addressed in a contingency plan test, as applicable:
    a. Notification procedures;
    b. System recovery on an alternate platform from backup media;
    c. Internal and external connectivity;
    d. System performance using alternative equipment; and
    e. Restoration of normal operations.
5. For each Plan Testing, Training and Exercise activity conducted, HESCOM must document results in an after-action report, and lessons learned after each Plan Testing, Training and Exercise activity.

G. Plan Maintenance

1. HESCOM must review contingency plans for accuracy and completeness at a minimum annually or whenever significant changes occur to any element of the plan or the Information System.
    a. Certain elements, such as contact lists, will require more frequent reviews.
    b. The plans for critical systems should be reviewed more often.
2. At a minimum, plan reviews must focus on the following elements:
    a. Operational requirements;
    b. Security requirements;
    c. Technical procedures;
    d. Hardware, software, and other equipment (types, specifications, and amount)
    e. Names and contact information of team members.

Approved by HESCOM BoD

9.5. Enterprise Security Policy

Purpose:

The purpose of this policy is to define the minimum requirements to safeguard HESCOM Information and Information Systems, regardless of the party responsible for use or management, the physical location, or the medium in which such Assets reside (e.g., electronic, digital, paper, etc.)

This policy establishes the information security requirements to ensure HESCOM protects its Assets from accidental or intentional unauthorized access, disclosure, modification, and destruction, such that:

- Confidentiality of Information is maintained;
- Integrity of Information can be relied upon;
- Information is available when required; and
- Regulatory and contractual obligations are met.

Scope:

This policy applies to all HESCOM entities and subsidiaries and is applicable to all HESCOM personnel

Roles and Responsibility:

Roles	Responsibilities
Management	• Accountable for information security at HESCOM • Ensure that the Chief Information Security Officer has the authority and the resources to establish effective programs and processes to protect HESCOM's Assets and in a manner consistent with HESCOM's strategic goals, organizational objectives, and Risk tolerance • Ensure HESCOM takes appropriate actions to manage and/or mitigate information security and privacy Risks
Business Owner	• Support HESCOM's business objectives by defining the business requirements and needs • Ensure compliance with enterprise and Business Unit-specific information security requirements
Chief Information Security Officer (CISO)	• Ensure a consistent and strategic approach to the use of Information and Information Systems at HESCOM • Facilitate coordination between Information Technology, Information Security, and Enterprise Architecture • Develop, maintain, and promote HESCOM's information security objectives

Approved by HESCOM BoD

	• Oversee the strategy, operations, governance, and support of HESCOM's Information Security program • Commit resources to coordinate, develop, implement, and maintain an organization-wide Information Security program • Determine methods to implement and enforce Information Security policies, standards, and procedures • Advise the enterprise on information security-related issues • Oversee the hiring process of skilled officers/employees to staff Information Security teams and if needed, request Information Security representatives staffed with HESCOM Business Units • Engage externally to outside expertise to help accelerate HESCOM's maturity and leverage proven methods of reducing information security Risks
Enterprise Architecture	▪ Support HESCOM's business objectives by establishing the architectural direction of HESCOM's information technology tools and resources
Ethics and Compliance	▪ Support implementation of, and monitoring of compliance with the information security and privacy policies, standards, and procedures ▪ Provide input on necessary compliance controls relative to the implementation of new Information Systems and controls for existing Information Systems
Information Security	▪ Execute day-to-day information security related activities as defined by the Office of the Chief Information Security Officer ▪ Review, monitor, and manage exceptions to Information Security requirements and controls, as necessary ▪ Engage with Enterprise Architecture and Information Technology to drive adoption of information security best practices and support HESCOM's strategic business objectives ▪ Ensure Workforce Members are appropriately trained on and made aware of their roles and responsibilities with regards to Information Security
Internal Audit	▪ Review HESCOM's compliance with this policy ▪ Report Audit results to Office of the Chief Information Security Officer, and as appropriate to the Management
Legal	▪ Provide guidance on Information Security legal matters that may impact information security requirements and control

Approved by HESCOM BoD

Office of the Chief Information Security Officer (OCISO)	▪ Oversee governance, management, and delivery of Information Security activities ▪ Act as a liaison between HESCOM Workforce Members and the Information Security Department ▪ Develop and drive system-wide information security initiatives

Policy:

A. Information Security Program

1. HESCOM must take all reasonable and appropriate measures to protect its Assets, against accidental or intentional unauthorized access, modification, disclosure, or destruction.
2. The CISO, in collaboration with the Management, must ensure the CISO is endowed with the authority and resources required to effectively implement the Information Security program and support HESCOM's strategic business mission.
3. The CISO must establish, publish, and enforce compliance with information security policies, requirements, and controls.
4. The CISO will delegate responsibility of the day-to-day management and implementation of information security initiatives, requirements, and controls to Information Security staff.
5. Information Security must develop, manage, and maintain Information Security polices, standards, and procedures and make them available to all Workforce Members.
6. The CISO and Information Security staff must stay up-to-date with relevant information security and privacy trends and changes in the threat landscape by participating in information security special interest groups or forums.
7. Information Security will collaborate with external entities, government/state and industry cyber security groups, and major technology vendors to receive periodic alerts on emerging threats and vulnerabilities.
8. Collaboration with external entities will follow communication protocols as established by the CISO.

B. Strategic Planning and Enterprise Architecture

1. Enterprise Architecture must develop and maintain documented strategies and plans that convey a roadmap of projects and initiatives to improve HESCOM's ability to protect the confidentiality, integrity, and availability of its Assets.
2. Current- and future-state information security capabilities will be designed to provide security services to all HESCOM BUs, favoring deployment for system-wide capabilities while also recognizing some BUs have unique needs.
3. Information Security, in coordination with Enterprise Architecture, must ensure that its strategic direction and plans are aligned with HESCOM's enterprise strategy and BU objectives.

Approved by HESCOM BoD

4. Information Security must develop and implement capabilities and solutions that can be leveraged across the system.
5. Information Security, in coordination with Enterprise Architecture, must maintain security architecture documentation to:
    - Guide the design, construction, and maintenance of Information Security solutions; and
    - Manage changes to minimize Risks to the technology environment.
6. Information Security must be integrated into HESCOM's project management processes and System Development Lifecycle (SDLC) to enable information security-related Risks to be identified and addressed during project work and ensure solutions are designed to provide fit-for-purpose security.
7. Project outputs must be designed to be compliant with Information Security requirements and controls.
8. Projects (organization-wide and BU specific) with the potential to impact the confidentiality, integrity, and availability of HESCOM Assets across the organization (e.g., implementation of medical devices and tools, process technology management, and other supporting processes) must include the following:
    - An Information Security Risk assessment during project design stages to determine which controls are required in accordance with HESCOM's Risk Management Policy;
    - Information Security and Enterprise Architecture consultation during development to achieve the control objectives identified and a system security plan to document the required capabilities;
    - Enterprise Architecture may be involved on an as-needed basis during the implementation stage.
    - Project owner and sponsor assignment/designation to identify resources and fund efforts to implement the required controls; and
    - Roles and responsibilities documentation for resources performing information security-related roles and responsibilities throughout the project lifecycle, including post-implementation operations.
9. Information Security and Enterprise Architecture teams must inform project sponsors about unmanaged Risks that have potential to delay projects until mitigating controls are implemented.

C. Communication

1. The Office of the CISO, will maintain awareness of and communicate to the Management, any major changes that may impact HESCOM's Information Security program, including but not limited to changes to:
    - Industry-specific information security trends and leading practices;
    - The threat landscape and/or changes in the healthcare industry Risk posture
    - The regulatory environment related to information security;
    - HESCOM-specific Information Security metrics.
2. Information Security must publish and communicate, in coordination with Business Units (as applicable), Information Security policies, standards, and procedures to all Workforce Members.

Approved by HESCOM BoD

3. Legal must be consulted prior to engaging, notifying, and/or involving law enforcement agencies in Information Security matters.

D. Awareness and Training

Information Security, in coordination with HESCOM Learning and Development, must develop, maintain, and implement an Information Security awareness and training program to educate Workforce Members on the applicable Information Security requirements and control.

Approved by HESCOM BoD

9.6. Identity and Access Management Policy

Purpose:

The purpose of this policy is to manage identities and access levels to prevent unauthorized access to HESCOM's Information Systems and Information.

Scope:

This policy applies to all Information Systems and applications managing Confidential, Restricted, or Internal data, including Third Party and Business Partner systems and applications, which collect, maintain, process, or transmit HESCOM's Information.

Roles and Responsibility:

Roles	Responsibilities
Business Owner	• Accountable for the business functions and system/application access within their line of business and is responsible for all aspects of the enterprise role definitions
Information Security	• Protects and preserves the confidentiality, integrity and availability of HESCOM's Information
Managers	• Approves access requests for Users based on legitimate business need and the Principle of Least Privilege
IT Owners	• Accountable for the functionality, privileges, and technical details assigned within their system

	• Accountable for the security and account access of the systems under their care • Provides directions on the method by which these policy requirements will be followed
Service Desk	▪ Provides technical assistance and support for incoming queries and issues related to computer systems, software, and hardware

Approved by HESCOM BoD

Policy:

A. User Enrollment and Approval

1. All Users of HESCOM's Information Systems or Information must use a unique User ID to authenticate their identity and ensure Users are linked to and held responsible for actions performed using their User ID
2. Access to HESCOM's Information Systems or Information must be granted through Birthright Access, or when a documented and approved business justification is present; all access requests must be formally documented, recorded, approved and retained in alignment with Asset Management Policy.
3. Creation and approval of Service Accounts must be approved by Information Security.
4. IT Owner must approve changes in access permissions and access to HESCOM's Information System.

B. Access Control

1. User access privileges must be granted based on the Principle of Least Privilege; access requests should consider job classification, employment status, role, and function whenever possible; valid approved access requests must provide Users with the minimum level of access required to perform their job responsibilities.
2. Information Systems and applications must have the appropriate controls to enforce the Principle of Least Privilege, as determined by Information Security.
3. Privileged User accounts must be assigned a unique User ID that distinguishes the account as a Privileged Account; Privileged Accounts must not be used for regular business activities.
4. Access granted to Users in bulk, or in mass via scripting, uploads or programmatically outside of normal Provisioning processes must be approved by Information Security.
5. Auto logons accounts are prohibited unless approved by Information Security.

6. Periodic access recertification reviews must occur for all HESCOM Information Systems and Information to ensure the Principle of Least Privilege is followed and unauthorized User IDs have access revoked. Unless required to be more frequent by regulation, law, or applicable industry standards, the following schedule will be followed for periodic access recertification reviews:
7. Access and privileges to systems must be reviewed at the following minimum schedules:
    - Quarterly for Privileged Accounts by Business Owner and IT Owner
    - Annually for Information System User accounts by the User's Manager
8. Users requiring Local Administrator rights to HESCOM's Information System must be approved by the Users Manager and IT Owner; Local Administrator rights will only be considered for Users with a documented business need to perform a part of their job function that cannot be accomplished without local administrator rights.
9. Provisioning access must follow defined and documented processes for granting new or modified levels of Information System access.
10. Access to HESCOM Information Systems and applications must be de-provisioned upon termination or the instance of any changes such as promotion, transfer, or demotion of employment. Any change request must be formally documented and recorded.

C. Authentication and Authorization

1. All User IDs, including User accounts, System Accounts, and Service Accounts, must be assigned to a unique User.
2. User IDs must not be reused.
3. Users must never share their Authentication information or other identity information (passwords, access badges, secret keys, etc.) with anyone. In an event a shared User ID is used, please see Section F Shared Accounts.
4. Users are responsible for all activity logged under their User ID and must report any suspicious account activity to Service Desk, as stated in the Acceptable Use Policy.
5. Users accessing Confidential or Restricted data on HESCOM's systems must Authenticate and Authorize with an User ID and password to verify the person or entity seeking access is the one claimed before access is granted.
6. Users must be authenticated before accessing the HESCOM network via a wired or wireless connection. All exceptions must be approved by Information Security.
7. Only approved methods of Authentication and Authorization, as determined by Information Security, can be used by HESCOM applications and systems.
8. Calls or inquires to the Service Desk Users must be identified and authenticated by the Service Desk in a secure manner.
9. Temporary Authentication credentials, if granted, must be unique to each User.
10. Users must change their temporary Authentication credentials upon first use.
11. Users must immediately change Authentication information or obtain new Authentication information and inform Information Security whenever there is an indication that it may be compromised.

Approved by HESCOM BoD

12. Authentication information (User ID, password, etc.) must never be stored on Information Systems or paper in an unprotected form.
13. Default Authentication information for software products and hardware must be changed before installation.
14. The process for logging a User into a system or application must be designed to minimize the opportunity for unauthorized access. The log-on process must disclose the minimum amount of information about the system or application to avoid providing an unauthorized User with any unnecessary assistance.
15. Controls for Authorization must be in place to minimize the risk of unauthorized or elevated access to Information Systems.
16. Users must not approve their own access.

D. Service Accounts

1. All uses of generic accounts and Service Accounts must be approved by the Business Owner and IT Owner and have a documented business justification.
2. Existing default, system, and Service Accounts must be safeguarded to prevent unauthorized access and must be in accordance with Privileged Account access policies.
3. The use of Service Accounts that require non-standard naming or passwords that do not expire require the following:
    a. Service Accounts must have documented business requirements and approval from the Business Owner and IT Owner and/or designated management responsible for security administration.
    b. Service Accounts must be configured to deny interactive logons, except during documented setup procedures involved in the initial Provisioning of an application or account.
    c. Service Accounts must employ additional access and audit controls as determined by Information Security including restricted logon locations and/or resources, extended account use auditing, time-of-day restrictions, and other applicable controls.
    d. All default accounts must be deleted, disabled, or renamed. In cases where the default accounts may not be deleted, disabled, or renamed, default passwords must be changed prior to being connected to the HESCOM network.

E. Privileged Account Access

1. Privileged Accounts must always be assigned to and used by only a single specific individual and all activity must be logged and traceable to that specific individual User's activity. Privileged Accounts must not be shared or used by any other individual.
2. The use of Privileged Accounts must be limited to those activities that require elevated privileges. Due to the risk associated with Privileged Accounts, access to them must be safeguarded at a level higher than required for typical User accounts and their use must be logged and monitored by Information Security team.

Approved by HESCOM BoD

3. A separate User ID for Privileged Users must be provided for elevated access to administer/configure applications or platforms. Privileged Users must use their standard User IDs for all non-administrative activities.
4. The use of Privileged User IDs must be logged, and the logs must be reviewed on a periodic basis, to deter and govern misuse of Privileged Accounts.
5. Special privileges on each information technology system (e.g., to include administrator and root privileges, backup privileges, operator privileges, ownership change capabilities, etc.) must be restricted to as few individuals as possible. All special privileges must be determined, clearly documented and maintained by the system owner and approved by Information Security.

Approved by HESCOM BoD

F. Share Accounts

Shared Accounts are not permitted unless approved by the Business Owner and IT Owner and require the following:

- Business justification and context for the shared use User ID and enumeration of who will have knowledge of the account details (password, etc.) must be clearly documented and maintained by the IT Owner and approved by Information Security.
- All shared User IDs must have a uniquely identified owner. The owner acknowledges and accepts all responsibilities or actions taken with this account.
- Shared User IDs must not provide access to individual officer/employee data (e.g., personal electronic mail messages, personal data files, etc.). Access to such data within the system where a shared User ID may be used must be approved by Information Security.

G. Account Settings

1. After five (5) unsuccessful attempts to access a User, Service, or System Account, the User ID attempting to gain access must be locked and logged.
    - User accounts must be re-enabled by Service Desk.
    - Service and/or System Accounts must be reviewed by Information Security prior to being re-enabled.
    - Applications or Information Systems requiring more than five (5) unsuccessful logon attempts must be approved by both the Business Owner and IT Owner.
2. If an User ID has not accessed HESCOM's network within the previous 90 days, the User ID must be disabled.

3. Workstation and application sessions must be secured after a reasonable period of inactivity to ensure unattended workstations are not used by unauthorized individuals.

H. Passwords

1. All Users must enable passwords on their devices when accessing HESCOM's Information Systems and Information.
2. Passwords must adhere to the standards set forth by Information Security.
3. Passwords must be stored in a secure manner.
4. The display and transmission of passwords must be controlled to prevent unauthorized parties from observing and/or recovering them.
5. Passwords expiration must adhere to the standards set forth by Information Security.

IT Core users	All Policies applicable

9.7. Incident Management Policy

Purpose:

This Policy establishes the information security requirements and controls HESCOM must have in place in order to ensure a consistent and effective approach to the management of information security Incidents.

Scope:

The policy applies to all HESCOM entities and subsidiaries, and is applicable to all Workforce Members who collect, access, maintain, distribute, process, protect, store, use transmit, dispose of, or otherwise handle Non-Public HESCOM Assets.

Roles and Responsibility:

Roles	Responsibilities
Management	• Accountable for information security at HESCOM • Ensure the CISO has the authority and resources to establish effective programs and processes to protect HESCOM's Assets, consistent with HESCOM's strategic goals, organizational objectives, and Risk tolerance • Ensure HESCOM takes appropriate actions to remediate and/or manage information security and privacy Risks
Business Owner	• Support HESCOM's business objectives by defining business requirements

Approved by HESCOM BoD

Roles	Responsibilities
	and needs • Ensure compliance to enterprise and Business Unit-specific information security efforts
Chief Information Security Officer (CISO)	• Ensure a consistent and strategic approach for the use of Information and Information Systems at HESCOM • Facilitate coordination between Information Technology, Information Security, and Enterprise Architecture • Develop, maintain, and promote HESCOM's information security objectives • Engage appropriate Business Units and subject matter experts, as needed, to participate in Incident response activities • Oversee strategy, operations, governance, and support of the Incident Response Team • Advise the enterprise on Incident response and management related issues
Emergency Management	▪ Communicate to Corporate Emergency Operations Center (EOC) at the beginning and throughout the Incident depending on their judgment of what levels of communication are needed. ▪ Coordinate regular Emergency Operations Center (EOC) meetings as needed.
Enterprise Operations	▪ Provide consultation services to Information Security regarding the protection and management of Enterprise Information Systems (e.g., HESCOM network, data centers, infrastructure) ▪ Participate in the Incident Management Team activities, including but not limited to development, rehearsal, and maintenance of Incident Response Playbooks and management of Incident response procedures.
Incident Management Team (IMT)	▪ Establish Incident management command center, communications and other Incident handling capabilities ▪ Establish central point of contact for IT Leadership and responders for serious Incidents. ▪ Maintain and manage Incident handling capability ▪ Coordinate activities during the response and investigation of security and privacy Incidents ▪ Respond to and investigate all reported thefts, data breaches, and exposures to confirm if a theft, breach or exposure has occurred.

Approved by HESCOM BoD

Roles	Responsibilities
Information Security	▪ Oversee governance and management of Information Security activities ▪ Oversee management of Incident Response procedures and activities, including the formation and training & awareness of the Incident Response Team ▪ Oversee collection and documentation of information related to the reporting of an incident
Internal Audit	▪ Review HESCOM's compliance with this policy ▪ Report Audit results to the CISO, and when deemed necessary by the CISO to the Management
Legal	▪ Provide guidance to Information Security legal matters that may impact information security requirements and control
Service Desk	▪ Perform day-to-day activities related to the collection and documentation of information related to the reporting of an incident ▪ Provide a central point of contact for reporting and communication of incident information

Approved by HESCOM BoD

Policy:

A. General Information Security Incident Management Requirements

1. Information Security must develop an Incident Response program to prepare Workforce Members to identify and systematically handle Incidents.
2. As part of the Incident Response program, Information Security, in collaboration with Information Technology, must develop formal procedures for reporting and monitoring Incidents (e.g., procedures for monitoring alerts from enterprise-wide Information Systems and Networks, process Workforce Members should follow when reporting and observed or suspected Incident).
    a. Any Workforce Members using HESCOM Assets must report all observed or suspected Incidents to the Service Desk.
    b. Incident reporting procedures must:
        - Define the timeliness of response;
        - Identify points of escalation and method of contact;
        - Outline actions to be taken on receipt of an information security Incident;
        - Establish point of contacts for reporting information security Incidents;

- Define the feedback process to ensure that those reporting information security Incidents are notified of results after the Incidents has been acknowledged, resolved, and/or closed.
- Define the priority of the Incident

c. Service Desk shall be the central point of contact for the collection of all Incident reports whether provided by a Workforce Member or collected from an Information Security tool.

d. If a Workforce Member detects and reports an Incident to the Service Desk, the Service Desk must document (as available):

- First and last name of the Workforce Member;
- Reporting Workforce Member's contact information;
- Date and time of discovery;
- Date and time of Incident;
- How the Incident was detected;
- Nature of the Incident;
- Whether or not the Incident is ongoing;
- What Information System is/was affected;
- What troubleshooting actions were taken, the current state of the Information System, and any instructions provided to involved parties;
- Whether Non-Public Information was disclosed; and
- Request a sample of logs or screen shots.

B. Incident Response

1. Information Security, in collaboration with Enterprise Operations, ICT & MIS and other applicable stakeholders, must develop and establish formal procedures to respond to and handle different types and severities of incidents.
2. Established procedures must ensure all relevant or involved parties are informed with necessary information in a timely manner.
3. Incident Response Playbooks must be developed, distributed, and rehearsed via table top exercise for a variety of Incidents, including but not limited to:
   a. Information System failures, outages, or loss of service;
   b. Malicious code infection;
   c. Denial of service;
   d. Errors resulting from incomplete or inaccurate Information;
   e. Breaches of confidentiality and integrity;
   f. Unintentional/unauthorized disclosures of Non-Public Information;
   g. Misuse of Information Systems; and
   h. Identity theft.

Approved by HESCOM BoD

4. Incident Response Playbooks must outline stakeholder roles and responsibilities and step-by-step activities (e.g., reporting, classification, escalation procedures). Incident Response Playbooks must address, at minimum:

    a. Analysis and identification of causes of the Incident;
    b. Containment of the Incident;
    c. Planning and implementation of corrective actions to prevent re-occurrence;
    d. Communication plans outlining how HESCOM will communicate an Incident to: (i) Workforce Members, (ii) the public, and (iii) those directly affected by the Incident; and
    e. Reporting the Incident to appropriate legal and regulatory authorities (if required).

5. Incident Response Playbooks must be reviewed, updated, and rehearsed on an annual basis. Incident Response Playbooks will be updated to address:

        a. Changes to the enterprise;
        b. Changes to the Information System;
        c. Problems that occur during the implantation or testing of the Incident Response Playbook; and/or
        d. Lessons learned from the execution of Incident Response Playbooks.

4. The CISO will chair an Incident Management Team to manage Incident response activities.
    - In addition to Information Security, the Incident Management Team may include members from:
        a. Enterprise Operations Incident Management Team;
        b. Information Technology;
        c. Emergency Management;
        d. Legal;
        e. Privacy;
        f. Communications;
        g. Human Resources;
        h. Supply Chain Services;
        i. Finance;
        j. The affected Business Unit that uses the impacted Asset; and
        k. Additional Business Units based on the Asset involved.

5. When an Incident is suspected or confirmed, Incident Management Team must consider isolating or shutting down the affected Information System(s) from the rest of HESCOM's network to limit exposure, in accordance with applicable Incident Response Playbooks**.**

C. Documentation and Collection of Evidence

Approved by HESCOM BoD

- Within the bounds of local, state, and federal legal requirements, Information Security must collaborate with Legal to define and apply procedures to identify, collect, acquire, and preserve Information which may serve as evidence.
- Evidence retention must comply with HESCOM's data retention guidelines, as well as any applicable laws and regulations.
- If a forensics examination needs to be performed as part of the Incident response process, the forensics examination must only be performed on a copy of the evidential material to protect the integrity of the evidential material.

9.8. Information Protection Policy

Purpose:

The purpose of this policy is to outline the minimum information security requirements HESCOM must have in place to safeguard its data, Information, and Information Systems from unauthorized access, alteration, tampering, corruption, or falsification.

Scope:

The policy applies to all systems and applications that collect, maintain, process, or transmit HESCOM Information and is applicable to all Workforce Members.

Roles and Responsibility:

Roles	Responsibilities
Business Owner	• Support HESCOM;'s business objectives by defining the business requirements and needs • Ensure compliance to enterprise and Business Unit specific information security efforts
Chief Information Security Officer	• Ensure a consistent and strategic approach to the use of Information and Information Systems at HESCOM • Facilitate coordination between Information Technology, Information Security, and Enterprise Architecture
Data Custodians	• Ensure the data is protected as defined by HESCOM's information security policies, standards, and procedures
Legal	• Provide guidance to Information Security legal matters that may impact information security requirements and control

Approved by HESCOM BoD

Information Security	▪ Execute day-to-day information security related activities ▪ Engage with Enterprise Architecture and Information Technology to drive adoption of information security best practices and support HESCOM's strategic business objectives
Information Technology	▪ Execute day-to-day information technology related activities ▪ Engage with Information Security to develop, implement, and drive adoption of IT and information security best practices and support HESCOM's strategic business objectives

Approved by HESCOM BoD

Policy:

A. Information Protection General Requirements

1. HESCOM must sustain the integrity of all Non-Public electronic Information in its possession by using approved mechanisms, whenever available and feasible.
   - Integrity controls must address:
     a. The use of add, modify, and delete functions to implement changes to data;
     b. The procedures to prevent programs running in the wrong order or running after failure of prior processing;
     c. The use of appropriate programs to recover from failures to ensure the correct processing of data; and
     d. Protection against attacks using buffer overruns/overflows.
2. Information Security must develop, document, and disseminate requirements and procedures to maintain the confidentiality, integrity, and availability of HESCOM Assets. Requirements must be reviewed and updated annually.
   a. HESCOM Information Systems must protect the confidentiality and integrity of data at rest based on its Data Classification in accordance with HESCOM's Data Classification Policy.
   b. HESCOM Information Systems must protect the confidentiality and integrity of transmitted Non-Public Information on both internal and external networks based on its Data Classification.
      - Information Systems that transmit data must protect against incomplete transmissions, misrouting, unauthorized message duplication or replay.
      - Cryptographic and/or user authentication techniques must be used when Non-Public Information is transmitted externally.
   c. HESCOM Information Systems must provide mechanisms to protect the authenticity of communications sessions.

B. Data Leak Protection

Information Technology, in coordination with Information Security, must develop, implement, and enforce approved data leak protection procedures to control the flow of data within Information Systems and between interconnected Information Systems

C. Cryptographic Controls and Key Management

1. Cryptographic controls must be implemented to secure Non-Public electronic Information. This includes data at rest and data in transit.
    - Cryptographic controls implemented may be determined by a combination of factors, including, but not limited to:
        a. Level of Risk for data disclosure;
        b. Availability of functionality in the system to encrypt data at rest in transit;
        c. Availability of Third-Party Solutions for encryption; and/or
        d. Impact to business operations.
2. Information Technology must have in place a key management process to support HESCOM's use of cryptographic techniques.
    a. All cryptographic keys must be protected against modification, loss, and destruction.
    b. Cryptographic keys must be limited to the fewest number of Workforce Members necessary. In addition, secret and private keys must be protected against unauthorized disclosure.
    c. Equipment used to generate, store and archive keys must be physically protected.
3. When selecting the cryptographic protocols to use within a given application, Information Technology, in collaboration with Information Security, will consider the business needs and the security objectives of the application. Potential key types and certificates that may be considered include, but are not limited to:
    a. Encryption;
    b. Authentication of End Devices;
    c. Random Number Generators; and
    d. Integrity Protection - Message Authentication Codes (MACs).
4. If manual clear-text key-management procedures are used, Information Technology must split knowledge and control of keys (e.g., requiring multiple individuals to know only their respective portion of the key, which when combined would comprise the whole key).
5. The process to authenticate public keys must be performed using public key certificates issued by an approved certification authority, which must be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.
6. In order to reduce the likelihood of compromise, the process for activation, reactivation and deactivation dates of keys must be defined and tracked so that keys can only be used for a limited period of time. This period of time will be dependent on the circumstances under which the cryptographic control is being used, and the perceived Risk.

Approved by HESCOM BoD

D. Integrity Validation

1. Information Technology must validate the integrity of inputs to and outputs from HESCOM Information Systems. Information Technology will validate data inputs and outputs by:
    a. Implementing procedures to control the installation of approved software on Information Systems;
    b. Establishing detection, prevention, and recovery controls to protect against malware;
    c. Ensuring appropriate user awareness of malicious attacks to HESCOM Assets; and
    d. Deploying integrity verification tools to detect unauthorized changes to software, firmware, and data.
2. Data input to applications and databases must be validated to ensure that the data is correct and appropriate. Where possible,
    a. Web-based applications must be checked for input-validation related vulnerabilities (e.g. Open Web Application Security Project (OWASP).
    b. Input validation checks must be performed with each release that moves into production. This must be tested and approved in the quality assurance staging phase.
    c. During the testing process
        - Dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data must be performed.
        - Review of the content of key fields or data files to confirm their validity and integrity must be performed.
        - Procedures for responding to validation errors must be performed.
        - Procedures for testing the plausibility of the input data must be performed.
        - The responsibilities of all personnel involved in the data input process must be defined.
        - A log of the activities involved in the data input process must be created.
3. Data output from an application must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
   Output validation must include:
    a. Plausibility checks to test whether the output data is reasonable;
    b. Reconciliation control counts to ensure processing of all data;
    c. Providing sufficient information for a reader (i.e., to ensure that the patient they are treating matches the information retrieved, or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information);
    d. Procedures for responding to output validation tests;
    e. Defining the responsibilities of all personnel involved in the data output process; and
    f. Creating an automated log of activities in the data output validation process.

Approved by HESCOM BoD

9.9. Infrastructure Policy

Purpose:

The purpose of this policy is to protect Information on HESCOM's network, monitor network traffic for suspicious activity or incidents, outline requirements for securely connecting to the network and network resources, and reduce the likelihood of network security compromises.

Scope:

This policy applies to all Workforce Members, Information Systems, and other resources connected to HESCOM's infrastructure.

Roles and Responsibility:

Roles	Responsibilities
IT and Application Owners	• Ensures vulnerabilities are remediated or mitigated in a timely manner • Maintains assigned/owned Information Systems, recommending and implementing appropriate modifications in accordance with changes to business or legal/regulatory requirements or technologies
Information Technology	• Executes day-to-day information technology related activities • Reviews, monitors, and manages exceptions to Information Technology requirements and controls, as necessary • Engages with Enterprise Architecture and Information Security to drive adoption of information technology best practices and support HESCOM's strategic business objectives
Information Security	• Establishes requirements to securely implement and manage processes and technologies to monitor and protect HESCOM's infrastructure • Monitors IT and Application Owners' compliance with established security infrastructure requirements • Approves changes to the anti-virus/anti-malware configuration settings (such as rebooting, software updates, hardware changes, policy, and reconfiguration)

Policy:

A. Configuration Management

Approved by HESCOM BoD

1. Baseline Configuration
    a. Information Technology must develop, document, and maintain a secure baseline configuration for Information Systems and system components.
    b. All HESCOM-owned devices, where technically feasible, must be configured with an approved secure baseline configuration. Devices not configured using an approved secure baseline configuration must be reviewed, approved, and configuration settings documented by Information Security prior to being deployed in a Production Environment.
    c. Information Technology must update baseline configurations or create new baselines as Information Systems change over time, minimally considering operating system and software updates, vulnerability patches, and other security updates.
    d. Baseline Configurations must utilize industry best practices and benchmarks.
2. Configuration Change Control
    a. A change control process must be in place to review and approve changes made to all Information Systems.
    b. Information Technology must analyze changes to Information System configurations to determine potential security impacts prior to change implementation.
3. Configuration Settings
    a. Information Technology must establish and document configuration settings for information technology products used within the Information System using security configuration checklists (e.g., lockdown, hardening guides, security reference guides, security technical implementation guides) that incorporate the principle of least functionality by configuring systems to provide only essential capabilities.
    b. Configuration settings must be implemented and validated on Information Systems before the system is installed on the network.
    c. Information Technology must identify, document, and approve any deviations from established configuration settings for Information System components based on operational requirements.
    d. Information Technology must monitor and control changes to the configuration settings.
        - Security configurations must be in alignment with Information Security standards (e.g., PCI systems requirements).

B. Network Security

1. HESCOM's network must be segmented into multiple separate trust zones to provide granular control of network access and additional intranet boundary defenses.
    - The boundaries of each security zone must be defined, documented, and implemented.
    - Public wireless networks must be segregated from internal HESCOM networks and private networks.

Approved by HESCOM BoD

- Servers, networks, and engineering laboratory environments used for research, development, and related activities must be clearly identified and segregated from other networks, in accordance with Information Security standards.

2. Direct external connections to the HESCOM internal network are prohibited. All external connections must terminate in the Demilitarized Zone.
3. Direct connections between segmented HESCOM network zones are prohibited without appropriate authorization.
4. Information Technology team is responsible for maintaining appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connects. Network diagrams should include wireless network components and show connections to all networks, highlighting any Confidential, Restricted, or Internal data locations and wireless networks.
    - Network diagrams and all documentation describing the functions, protocols, capabilities, and configurations of HESCOM's network must be restricted from access by unauthorized internal or external parties or redacted to provide only the information necessary for the defined business purpose.
5. All unnecessary and unsecure services, protocols, ports, etc. must be disabled. Any required unsecure services, protocols, ports, etc. must be reviewed, documented, and approved by Information Security.
6. Vendor-supplied default settings and configurations must be changed before installing a system on the network, including but not limited to default passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
7. Equipment and systems not owned and managed by HESCOM are prohibited from being directly connected to or used to remotely connect to the HESCOM network, unless approved by Information Security.
8. Unused ports on networking equipment and other related devices must be disabled to prevent unauthorized devices from connecting to HESCOM's network.
9. Network Access Control (NAC) must be used to provide access to application and network services using a strong Zero Trust Network. NAC must also detect new devices attempting to connect to the network and devices that drop off of the network.
10. Personally-owned or managed networking equipment (routers, switches, bridges, hubs, repeaters, etc.) must not be connected to the HESCOM network.
11. All Information Systems must employ secure communication protocols to protect confidential information where such data traverses any network segments that are not considered internal company network segments.
12. Network-based intrusion detection and prevention systems must be used to detect and prevent unauthorized activity on HESCOM's network and Information Systems.
13. Information Technology must maintain an up-to-date network diagram with all connections to Cardholder Data Environment (CDE), including any wireless networks, to reflect the current HESCOM infrastructure.

Approved by HESCOM BoD

14. Appropriate mechanism or a Network Operation Centre (NOC) shall be established in order to ensure the network availability all the time
15. Critical networks should be redundant in order to ensure the high availability of the networks, in case of any attack or failure
16. There shall be no single point of failure in the networks. Therefore, networking and security hardware devices shall be redundant
17. The logs of the networking and security devices shall be analyzed on real-time basis in order to detect and mitigate possible threats and compromises within the network

C. Firewall

1. Firewall Controls
    a. The internal HESCOM network must be protected from un-trusted networks, including but not limited to, the Internet and Business Partner networks, using firewalls and/or other compensating technologies.
    b. All network ingress and egress points must be protected by firewalls, with procedures for review of all firewall logs.
2. Firewall Configuration
    a. Unnecessary services and software must be disabled or uninstalled by Information Technology on network firewalls that are not required.
    b. All connections between HESCOM networks and the Internet external networks must utilize a firewall.
    c. Connections originating from within the HESCOM network is permitted through the firewall.
    d. Inbound traffic originating outside of the HESCOM network must be identified and approved on a service-by-service basis by Information Security.
    e. Firewall and router configurations and management activities must conform to Information Security standards (e.g., PCI DSS).
3. Firewall Management
    a. Information Technology must ensure physical access to the firewall is controlled.
    b. Information Technology must regularly monitor and review firewall logs. Logs must be archived.
    c. Firewall rule changes must be subject to change management practices to review, assess, document, and approve or deny rule change requests.
    d. The IT team must review and perform ongoing audits, at least yearly, on the firewall.

D. Wireless Networks

1. All wireless networks must be approved by Information Security. Non-managed, ad-hoc wireless networks are prohibited.

Approved by HESCOM BoD

2. Information Security is responsible for performing quarterly wireless access point scans or deploying appropriate tools to identify rogue wireless access points. All identified rogue access points must be disabled, removed from the network, and investigated immediately.
    - HESCOM's Cardholder Data Environment must be tested at least quarterly for the presence of wireless access points by Information Security.
3. All wireless access points must be configured securely and approved to deny unauthorized access to the corporate network.
4. Access to HESCOM's wireless local area networks (WLANs) must be protected from unauthorized access and use strong encryption and authentication controls.
5. Information Technology (IT) staff members must be properly trained in wireless technologies to enable them to properly setup/configure, deploy, and maintain wireless equipment and technologies.
6. All wireless infrastructure devices that provide wireless internet access for guests or Third Parties must adhere to the controls defined by Information Security.
7. Internet Access Management
    - All gateways to external Internet-based services must be managed by a central authority.
    - All gateways to external networks, including the public Internet, must be implemented and managed by Information Security or an appropriate delegate.
    - All gateways must be configured to protect the HESCOM Network from undesired intrusion, access, or disruption by inbound network traffic.
    - Before implementing network border gateways, gateway configuration and gateway management procedures must adhere to the requirements defined and documented by Information Technology.
    - Only personnel responsible for maintaining the HESCOM Network may provision physical or virtual connections to external networks that terminate inside the HESCOM Network border.
8. SSID (Service Set Identifier) of a wireless access point shall be hidden.
9. MAC (Media Access Control) binding shall be utilized for restricting the access to the wireless networks.
10. Wi-Fi Protected Access II (WPA2) & WPA3 mechanisms shall be used for encrypting and authenticating users trying to associate/connect to a wireless network.

E. Anti-virus and Anti- malware

1. All HESCOM devices capable of supporting anti-virus/anti-malware software, in compliance with regulatory or legal requirements, must have current anti-virus/anti-malware software installed with current virus signature files applied and be actively running.
    - Where anti-virus/anti-malware software cannot be used, appropriate compensating controls (e.g., firewalls, security patching, vulnerability scans, and system monitoring) must be in place.
2. Personally-owned devices used to gain access to the network are expected to use anti-virus/anti-malware software and be configured.
3. Anti-virus/anti-malware software must be configured such that:

Approved by HESCOM BoD

- The auto-protect feature (real-time protection) is enabled.
- Signature files are automatically and frequently updated.
- Logging and alerting are enabled.
- Workforce Members are not permitted to uninstall, reconfigure, disable, or modify the anti-virus/anti-malware software in any way.

4. All newly attached storage devices or removable media must be scanned for viruses.
5. Regularly scheduled signature files and software updates must be performed as frequently as recommended by the vendor.
6. All Workforce Members must notify Service Desk immediately if a device is suspected of being compromised by a virus or malicious software.
    - Infected devices must be removed from the HESCOM network until the virus or malicious software is eradicated.

F. Monitoring, Logging and Auditing

1. Logging for Information Systems
    a. Information Systems that create, store, process, or transmit Non-Public Information must have various levels of logging capability. Minimally, Information Systems capable of generating audit logs must record the following system details:
        - Date/time stamp activity;
        - Account ID;
        - Device location;
        - Device ID (e.g., IP address or workstation ID); and
        - Type of activity (e.g., successful and failed logon attempts, escalation of user privileges, lateral movements between systems, viewing or updating patients' record, printing).
    b. Audit logs must be configured to record as many events and as much detail as reasonably possible above and beyond the preceding minimum requirements, considering system performance and storage requirements. Additional data points to log may include:
        - Event, status, and/or error codes;
        - Service/command/application name;
        - User or system account associated with an event; and
        - Device used (e.g., source and destination IPs, terminal session ID, web browser, etc.)
    c. Audit logs must capture data for the purpose of supporting security incident investigation.
    d. Information Technology must enable firewall logging and altering, if possible. Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious user.

2. Monitoring of System Activity

Approved by HESCOM BoD

a. HESCOM must regularly review audit logs, access reports, failed logon attempts, and security incident reports.
   - System activity monitoring must be performed by Information Security or delegated to another team or Third Party, as appropriate.

b. Network management or system monitoring (Intrusion Detection or Prevention Systems) used for network operations, problem resolution procedures, and security event identification must be in place and located at strategic points on the network to detect anomalies.

c. Anomalous network activity must be reviewed for impact and threat to HESCOM.

d. Detected security events must be recorded and analyzed to determine if sufficient risk is evident. Confirmed incidents must be eradicated, contained, or otherwise remediated as appropriate.

e. HESCOM must designate individuals responsible for conducting network activity log reviews and correlating activity entries on a regular basis.

f. Information Security must:
   - Perform Network Vulnerability Testing using a vulnerability scanning tool on a periodic basis, occurring at a minimum of at least once every year.
   - Perform periodic penetration tests on critical externally facing systems, occurring at a minimum of at least once annually or after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, a sub-network added to the environment, a web server added to the environment).
   - Review the output of the vulnerability and penetration tests and take appropriate action to remediate and/or mitigate any issues identified.

G. Vulnerability Management

1. HESCOM must comply with the following vulnerability management process:

   a. Discover
      - Information Security must identify and verify vulnerabilities using industry research, in-house expertise, and toolsets on a periodic basis on servers and workstations.
      - Information Security must test managed systems continuously for new vulnerabilities that require patching or configuration changes.

   b. Analyze and Prioritize
      - Information Security must assess vulnerabilities to determine remediation methods and prioritization.
      - Information Security must determine the risk and impact introduced by the vulnerability.

   c. Triage and Remediate
      - Information Security must notify IT and Application Owners of identified vulnerabilities.
      - Information Security must coordinate and schedule the application of identified vulnerability treatments (e.g., patches, upgrades, additional/compensating controls).

Approved by HESCOM BoD

- Information Security must test and distribute vulnerability treatments in environments before deploying the treatment to a Production Environment in accordance with HESCOM's Application Security Policy.
    i. IT must test security patches in Non-Production Environment.
    ii. IT must install patches on a non-production system, if available, to verify that a security patch will not adversely impact any user or software which may interact with it.
    iii. IT must install vendor-supplied patches. Installing these security patches ensures the security of HESCOM's data and intellectual property.
- Information Security must communicate and approve vulnerability treatments to appropriate stakeholders before distribution.
- Information Security must communicate monthly maintenance schedules of Information Systems to stakeholders at least seven (7) days in advance except under certain circumstances (e.g., emergency vulnerability treatments or auto-updated applications for critical and high-risk vulnerabilities).
- Information Security must analyze and communicate treatment failures to IT and Application Owners.
- Information Security must document and monitor identified vulnerabilities that cannot be remediated or mitigated adequately. Where possible, additional/compensating controls should be used to mitigate risk of the vulnerability being exploited.
- Information Security, in coordination with IT, must establish an SLA for remediation expectation for each level of vulnerability.

2. Validate
    - Information Security must validate implemented treatments were successful and eliminate identified vulnerabilities.
    - Information Security must record post-vulnerability and configuration assessment results and associated requests for treatments.

3. Monitor and Respond
    a. Information Security must track and report process deviations and aggregated outstanding risks to IT and Application Owners.
    b. Information Security must deploy additional tools (e.g., network- and host-based intrusion detection systems, firewall rules, configuration policies) to provide additional mitigation coverage for vulnerabilities whenever possible.
    c. Information Security must document and track vulnerability treatment deferrals, exemptions, risk acceptances, and corrective action plans.

Approved by HESCOM BoD

9.10. Cloud Security Policy

Purpose:

The purpose of this policy is to define the set of guidelines and controls that must be adhered to by HESCOM to protects its virtualized data, IP, Applications, services and associated infrastructure of cloud computing.

Scope:

This policy applies to all HESCOM entities, subsidiaries, and Workforce Members and considers all the virtualized assets and its associated infrastructure of cloud computing.

Roles and Responsibilities:

Roles	Responsibilities
IT and Application Owners	• Ensures vulnerabilities are remediated or mitigated in a timely manner
Information Technology	• Executes day-to-day Cloud Security related activities
Information Security	• Establishes requirements to securely implement and manage processes and technologies to monitor and protect HESCOM's cloud infrastructure • Monitors IT and Application Owners' compliance with established cloud security infrastructure requirements

Policy:

A. Perform Data Classification

1. The Information Owner must appropriately classify all the information under consideration for use in a Cloud computing environment.

2. Security Controls must be applied based on the Information Classification.

Approved by HESCOM BoD

3. Any Data carrying Personally Identifiable Information must be securely handled and access controlled.

B. Select Security Controls

The classified data must be exposed to appropriate security controls that implement the following:

Standards:

- The Cloud Service Provider must be empanelled by MeitY that meets pre-defined government standards of quality, availability and security
- The Cloud Service Providers must ensure compliance with all the cloud security standards published by MeitY and notified to the CSPs by MeitY as mandatory standards
- The CSP shall meets all the security requirements indicated in the IT Act 2000 and its amendments

Compliance:

- The Cloud Service Provider must ensure compliance with a cloud security standard by conducting an audit by an independent third-party auditor.
- It must also demonstrate compliance with security obligations.

Access Control:

- An access control policy and procedure must be implemented by the Cloud Service Provider that addresses regular access reviews, transition between roles, limits and controls of administrator privileges and inactivity timeouts.
- It must also maintain an accurate inventory of accounts and conduct a periodic review to identify active, dormant, fictitious and unused accounts.
- The Cloud Service Provider must regulate the limits on login attempts and concurrent sessions and also implement a multi-factor authentication for privileged access.

Password:

- The Cloud Service Provider must enforce password complexity, password history and password length for password-based authentication.
- Multi-factor authentication must be used for login activity.

Approved by HESCOM BoD

- The service provider must support single sign-on technology for authentication.

Logging:

- The Cloud Service Provider is required to retain all the logs of the user activity for a period of 90 days online.
- The users must have the online GUI access to the activity logs.
- The Service provider must also provide the technical capability to forward the logs and must monitor and alert on the logs.

Investigations

- All investigation reports related to a security incident must be retained by the service provider for a period of 2 years.
- The Cloud service provider must support e-discovery and legal holds to meet the demands of the judicial requests.

Change Control

- Reasonable industry practices must be followed by the service provider to implement change controls.
- All the changes to the environment must be tested as part of the change management process.
- Production data must not be utilized in test environment.

Configuration/Patch Management/Best Practices

- The Cloud service providers must harden all the systems and servers using proper industry standards.
- All the databases must be secured, logically isolated and encrypted.
- Workstations used in management and provisioning must be patched and secured with anti-virus.
- The Cloud service provider must implement physical security and must resolve vulnerability and patches according to the criticality.
- Applications and interfaces must be developed according to industry standards.

Approved by HESCOM BoD

Asset disposal and Risk Assessments

- All the assets and information must be disposed according to industry best practices.
- Threats and risk assessments must be conducted on new systems and material changes to existing ones.

Security Testing and Security Screening

- Vulnerability scans, web app vulnerability scans and penetration testing must be conducted for new systems and material changes to existing systems.
- All the individuals must be screened before giving access to information systems. Criminal record checks must be conducted on all officers/employees.

Encryption and Logical Separation

- The data in transit and at rest must be encrypted and the services provider must provide technical capabilities to manage encryption keys.
- The information must be logically isolated, and the traffic must be segregated from other management traffic. Security devices must be implemented between zones.

Technical Controls

- Firewalls must be implemented, and remote access must be secured according to industry best practices. The service provider must implement distributed denial of service attack protection.

C. Risk Assessment

A risk management process must be incorporated to balance the advantages of cloud computing with the security risks associated with it. A simplified risk assessment process including the review of the supplier's Statement of Applicability must be enough. All the findings in the review report must be successfully addressed before the supplier is onboarded.

D. Periodically monitor and audit the systems

The Security compliance monitoring and auditing of the supplier must be included in contracts with Cloud service providers.

Approved by HESCOM BoD

9.11. Risk Management Policy

Purpose:

The purpose of this policy is to define the minimum information security and privacy requirements and controls for how HESCOM will identify, manage, and mitigate Risks to its Assets.

Scope:

This policy applies to all HESCOM entities, subsidiaries, and Workforce Members. This policy is applicable to HESCOM Assets, regardless of where they are collected, transmitted, processed, maintained, or stored.

Roles and Responsibility:

Roles	Responsibilities
Office of the Chief Information Security Officer	• Define and update HESCOM's security Risk Assessment methodology, oversee the performance of the security Risk Assessments, maintain records of Risk Assessments that have been performed and engage relevant business units as appropriate • Own and update the Information Security Risk Register
Information Security	• Establish an ongoing process for identifying, assessing, and responding to Risk to enable HESCOM to make informed and prioritized decisions
Information Technology	• Manage changes and mitigate Risks to the technology environment to align with and adhere to the applicable Information controls and requirements
Risk Owner	• Coordinate with Information Security and Information Technology to prioritize and manage Risk to HESCOM's Information
Business Risk Committee	• Manages overall business processes of identifying, assessing, managing and mitigating the risks undertaken • Manages the key strategic and operating risks, performance and metrics
Information Security and Privacy Committee	• Manages and coordinates information security and privacy risk by identifying, assessing, managing and mitigating the risks undertaken • Reports information security and privacy risks to the Business Risk Committee

Approved by HESCOM BoD

Third Party Risk Management Program Office	• Conduct Third Party assessments according to the requirements of this policy and the Information Security Third Party Risk Management Policy

Policy:

A. Information Security Risk Management Overview

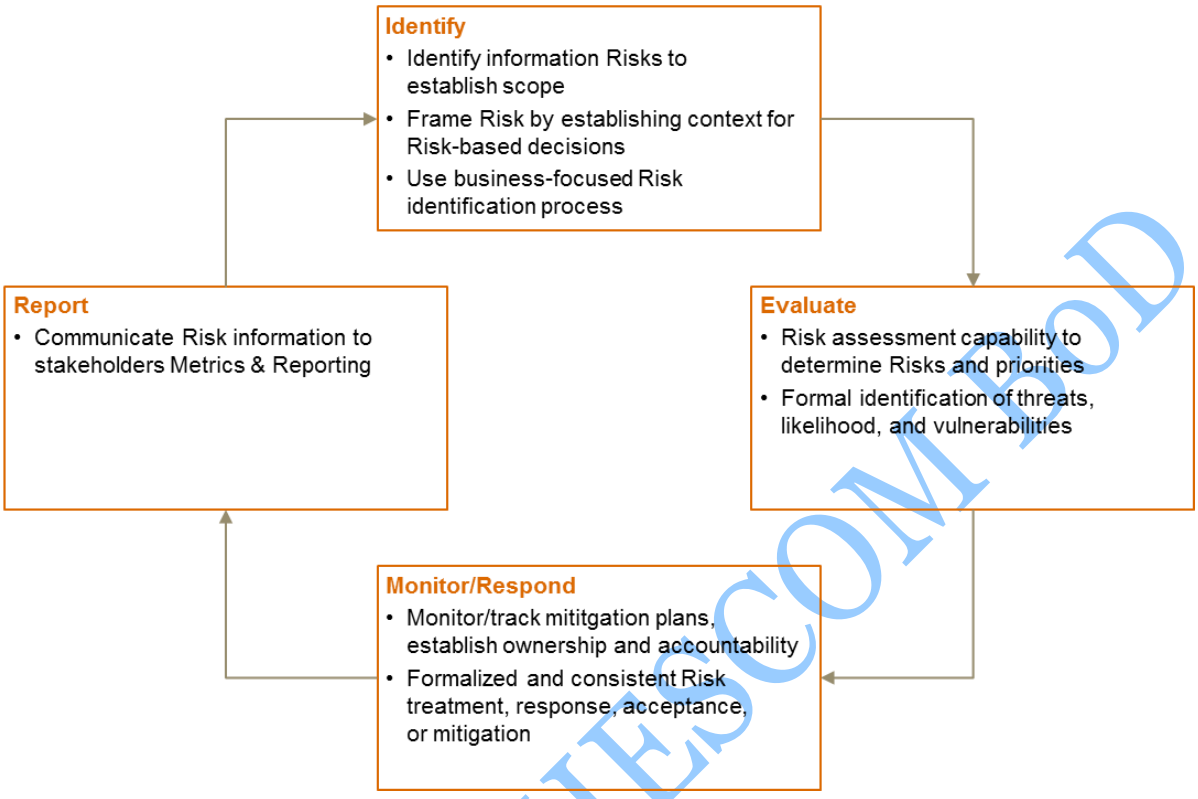
1. HESCOM must implement an Information Security Risk Management program to identify and review information security Risks and protect the confidentiality, integrity, and availability of its Information.

2. HESCOM must effectively manage information security Risk by:
   - Assigning Risk Management responsibilities to senior leaders/executives;
   - Ensuring senior leaders/executives ongoing recognition and understanding of information security Risks and their impact to HESCOM Assets;
   - Establishing an organizational tolerance for information security Risk and communicating this Risk Tolerance throughout the organization with guidance on how security Risk Tolerance impacts ongoing decision-making activities;
   - Ensuring accountability by senior leaders/executives for their Risk Management decisions and for the implementation of effective, system-wide Risk Management programs; and
   - Completing an enterprise Risk Assessment on an annual basis.

3. The Information Security Risk Management program must include capabilities and processes that:
   - Maintain traceability between business Risks, objectives, processes, and HESCOM Assets in its Risk Register. This will enable visibility into the value, Risks, decision-making, impact, and resulting outcomes of remediation activities;
   - Mitigate Risk to levels agreed upon with key stakeholders;
   - Identify Risk Tolerance for confidentiality, integrity, and availability of HESCOM Assets on an annual basis. The associated HESCOM Information will inherit the Risk Tolerance from the business process;
   - Formally identifies, tracks, remediates, and reports finding for HESCOM's Assets;
   - Maintain information security Risks in a central repository to enable reporting and monitoring of Risk identification, assessment, remediation activities, and exceptions;
   - Identify the likelihood that an identified Risk will occur and the resulting impact to the Asset; and
   - Prioritize information security activities based on agreed and documented Risk Tolerance.

B. Information Security Risk Management Lifecycle

Approved by HESCOM BoD



Approved by HESCOM BoD

- **Identify**
  - Information Security must establish a Risk framework to define how HESCOM intends to assess, treat, respond, and monitor HESCOM's Assets. The Risk framework should describe:
    - Business-focused Risk identification process to identify business priorities and associated confidentiality, integrity, and availability Risks;
    - Sources of Risk and representative scenarios (e.g., threat sources, vulnerabilities, impacts, and likelihood based on how information is used) that must be considered when evaluating Risk;
    - Threat hunting methodologies to understand threat sources and update the Risk Register for HESCOM's impacted Assets; all Residual Risk must be stored in a centralized repository;
    - Information Security Risk Tolerance, outlining a process by which the level of accepted Residual Risk must be determined (e.g., by providing a set of preventative scenarios and acceptable mitigation steps); and
    - Guidance for prioritization, making investments, and operational decisions regarding Risk Management.
  - Information Security must update and revise the Risk framework based on feedback and changes to the information security landscape (e.g., due to evolution of the threat landscape, advances in technology, changes in regulatory and compliance requirements).

- **Evaluate**
  a. HESCOM's Assets must undergo information security Risk Assessments to identify, estimate, and prioritize Risks at least annually or as deemed necessary based on changes in technology and processes. All information systems and components, including applications, servers, and networks, must be accessible for the purpose of conducting Risk Assessments. This includes Third Party systems and computer devices connected to HESCOM network.
     - A Risk Assessment must be conducted on Confidential Information Systems prior to the system being connected to HESCOM's network or being placed in a production environment.
     - Risk Assessments must be performed on Third Parties prior to HESCOM entering a contractual relationship with or providing access to/sharing HESCOM's Assets, and when required by the Third-Party Information Handling Policy during the contract period.
     - Risk Assessment must develop a process for prioritizing risks.
  b. An information security Risk Assessment must be performed whenever there is a(n):
     - New project that involves use of HESCOM's Information with potential to impact the confidentiality, integrity, or availability of HESCOM's Assets;
     - Exception to an Information Security policy or standard;
     - Audit issue pertaining to Information Security; or
     - Missing security control.
  c. Risk Assessments must use a Risk Assessment methodology to assess the value of HESCOM's Assets, identify threats and vulnerabilities, and identify level of Risk based on the likelihood and impact of compromise of Assets' confidentiality, integrity, or availability.

- **Monitor and Respond**
  a. Identified Risks must be monitored to:
     - Verify planned Risk response measures are implemented and applicable requirements are appropriately satisfied.
     - Use metrics to determine the ongoing effectiveness of information security Risk response measures following implementation.
  b. Information Security must maintain an inventory of identified Risks to HESCOM's Assets and the associated Risk response, and any required actions.
  c. A Risk Owner must be identified and assigned to each Risk identified in a Risk Assessment.
  d. Risk Owners must manage and/or execute the Risk response action items in accordance with the Risk Assessment.
  e. HESCOM must manage identified Risks appropriately based on the potential impact to HESCOM. Potential Risk responses include:

Approved by HESCOM BoD

- Mitigate the Risk – take steps to reduce the exposure to, probability of occurrence, and/or impact severity of a Risk;
- Transfer the Risk – shift ownership and/or management of a Risk, usually to a Third Party;
- Avoid the Risk – initiate changes to processes or systems to eliminate the potential Risk (e.g., shifting from using identifiable information to aggregated data); or
- Accept the Risk – no Risk mitigation occurs; Risk Owners and executive management (as applicable) are aware of all potential impacts.

C. Risk Reporting

1. Information Security, in coordination with Information Technology must generate quarterly Risk reports that reflect HESCOM's current Risk posture against emerging threats and vulnerabilities.
2. The report must be provided to the Chief Information Security Officer (CISO).

Approved by HESCOM BoD

9.12. Third Party Risk Management Policy

Purpose:

The purpose of this policy is to define the minimum requirements HESCOM Workforce Members must follow when identifying, assessing, monitoring, and responding to information security and privacy Risks associated with Third Parties and the products or services they provide to HESCOM

This Policy establishes principles for managing Third Parties across the lifecycle activities by:

- Identifying and defining the roles and responsibilities of key stakeholders
- Defining the Third-Party Risk Management framework as it relates to information security and privacy

Scope:

The policy applies to HESCOM and is intended for use by those who work with Third Parties that access, process, transmit, or store HESCOM workforce, affiliate, member, and/or customer data. Any individual involved with the use and/or management of a Third Party must be knowledgeable of this Policy and is responsible for compliance with it in their related business activities.

Roles and Responsibility:

Roles	Responsibilities
Business Owner	• Support HESCOM's business objectives by defining the business requirements and needs. • Assume responsibility of information security and privacy Risks associated with engaging Third Parties that may access HESCOM Assets • Accountable for all Third-Party relationships associated with their line of service
Business Unit Third Party Relationship Owner	• Oversee day-to-day operations of the Third-Party services • Ensure vendor compliance with TPRM program information security and privacy requirements • Communicate information security and privacy requirements outlined in applicable HESCOM polices, standards, and procedures • Complete IRQs for assigned services, with assistance from Subject Matter Experts • Participate in negotiating mitigation action plans for identified information security and privacy risks; monitor open Risks through remediation and closure • Perform ongoing monitoring of Third Parties to ensure compliance with contract terms and service-level agreements
Enterprise Architecture	• Support HESCOM's business objectives by establishing the architectural direction of HESCOM's information technology tools and resources • Provide consultation to the TPRM Program Office, Supply Chain Services, and the BUs to ensure the architectural needs as determined by HESCOM are met
Legal	• Provide legal guidance to BUs and Supply Chain Services on contractual and legal matters that may impact the Third-Party process • Define standard contractual terms and conditions • Review and negotiate non-standard terms within Third Party contracts • Support business with breaches, early contract termination, and/or Third-Party disputes
Subject Matter Experts	• Assist Business Owners and operational stakeholders to identify, evaluate, and manage Third Party Risks

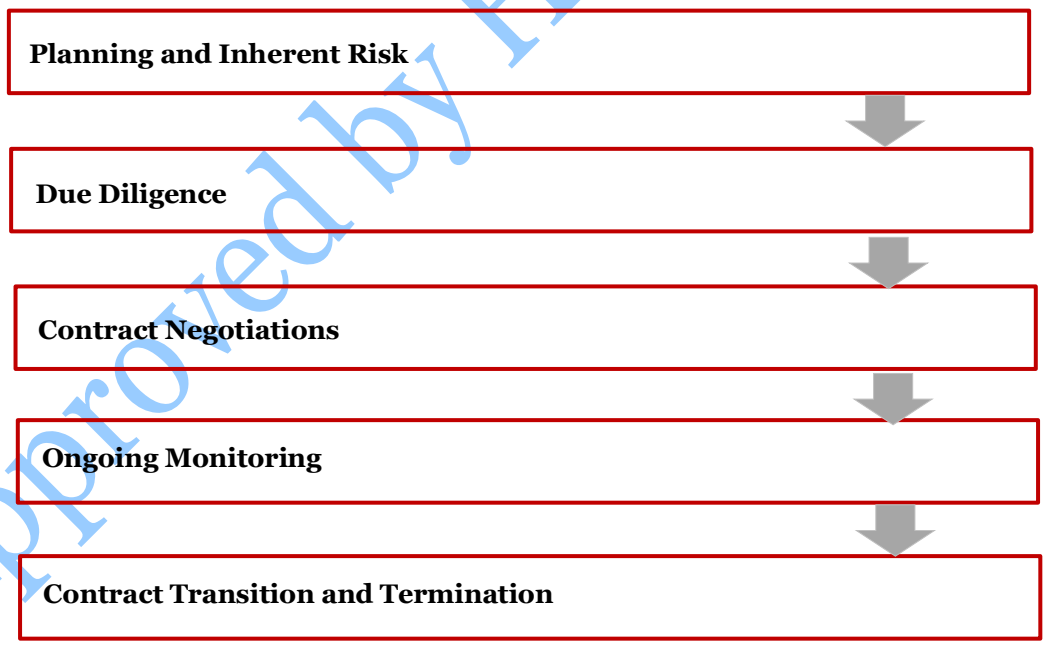
Approved by HESCOM BoD

	• Perform information security and privacy Third Party Assessments
Third Party Risk Management Program Office	• Develop, implement, manage, and monitor the TPRM Program • Oversee and assist the Business Units with the management Third Party information security and privacy Risks throughout the Third-Party lifecycle • Communicate this policy and associated Standards and Procedures to the necessary stakeholders • Report status of the TPRM Program to the appropriate Committee(s) • Review Third Party Information related policies annually

Policy:

A. Third-Party Risk Management Lifecycle

All Business Units (BUs) using Third Parties that access, process, transmit, or store HESCOM Information and/or Information Systems must continuously and consistently manage Third Party information security and privacy Risks throughout the lifecycle of the Third-Party relationship.



Approved by HESCOM BoD

B. Planning and Inherent Risk

1. BUs must be aware of and consider information security and privacy Risks when making decisions related to engaging Third Parties.

- BUs must engage with HESCOM Enterprise Architecture to ensure that the proposed Third-Party service and/or tool aligns with HESCOM's strategic architectural design.

2. HESCOM Third Party Risk Management (TPRM) Program Office will maintain a complete and comprehensive inventory of Third Parties that access, process, transmit, or store HESCOM Assets. The inventory must contain sufficient data elements about the Third Party, including, but not limited to:
    - A unique identifier;
    - A reference to the Business Unit(s) and Cost Centers (where applicable) that owns the relationship with the Third Party;
    - A description of the business process supported by the Third Party;
    - A clearly identifiable information security and privacy Risk rating and score for the Third Party and underlying services provided;
    - Summary of HESCOM Assets that may be accessed or handled by the Third Party;
    - Reference or links to any key supporting documentation relevant to the Risk profile of the Third Party.
3. BUs using Third Parties that access, process, transmit, or store HESCOM Assets, must ensure that the Third Parties go through a TPRM Inherent Risk Assessment. Inherent Risk Assessments must be conducted for:
    - Existing Third-Party relationships that have never undergone an Inherent Risk Assessment;
    - Existing Third-Party relationships where the scope of services or access to HESCOM Assets has significantly changed since the last Inherent Risk Assessment; and
    - New Third-Party relationships.
4. As part of the Inherent Risk Assessment, the BU Third Party Relationship Owner must complete an Inherent Risk Questionnaire (IRQ) and determine an Inherent Risk Rating.
    - The BU Third Party Relationship Owner must coordinate with the appropriate SME(s) to complete the IRQ. Completion of the IRQ may require input from the Supply Chain Services.
    - Results of the Inherent Risk Assessment and correlating Inherent Risk Rating will be used to inform the level of Due Diligence activities required.

C. Due Diligence

1. Pre-Contract Due Diligence
    - The level of Due Diligence Assessment, low, moderate, high, critical, is based on the IRQ results.
    - Prior to execution of a contract and completion of the IRQ, BU Third Party Relationship Owners, in coordination with the TPRM Program Office and SME(s), must perform Due Diligence Assessments, outlined in the procedures, on Third Parties' information security and privacy controls appropriate with the Risks identified.
    - For existing relationships with Third Parties that access, process, transmit, or store HESCOM Assets, BU Third Party Relationship Owners must partner with the TPRM Office and SME(s) to establish a timeframe for performing the Due Diligence Assessment.

Approved by HESCOM BoD

- BU Third Party Relationship Owners must inform the Business Owner of the results of the Inherent Risk Assessment and the Due Diligence Assessment.

2. Post-Contract Due Diligence
    - Throughout the lifetime of the Third-Party Contract, the BU Third Party Relationship Owner must perform assessments on an annual basis.
3. Third Party Residual Risk Determination and Mitigation
    - Level of Residual Risk must be determined by looking at the impact, threat, and potential for exploitation as it relates to the Third Party's Inherent Risk score.
    - Prior to execution of a contract, BUs must appropriately document, classify, and manage identified Third Party Residual Risk in accordance with HESCOM's Risk Management Policy.

D. Contract Negotiations

1. New Contracts or existing Contracts (at the time of renewal) with Third Parties that access, process, transmit, or store HESCOM Assets, must include a requirement to comply with HESCOM's information security and privacy requirements.
2. BUs must consult with Legal for guidance on specific Contract terms and provisions that must be included in Third Party Contracts.
3. Third Party Contracts must outline applicable information security and privacy controls in accordance with HESCOM's Third Party Information Handling Policy. At a minimum Third-Party Contracts must:
    - Consider the outcome of the Inherent Risk Assessment and any other issues identified during the Due Diligence phase;
    - Include a "Right to Audit" Clause to ensure the protection of HESCOM's Assets;
    - Include a Business Associate Agreement (BAA), as applicable, prior to the Third Party accessing or receiving any HESCOM Asset; and
    - Upon occurrence of material risk of significant authorized disclosure, include a right to terminate the contract immediately upon HESCOM's determination of significant Risk or problem.
4. BU Third Party Relationship Owners must review contracts periodically and document the determination of the continuation of the contract based on the risk assessment.

E. Ongoing Monitoring

1. BU Third Party Relationship Owners must review the performance of Third Parties on an on-going basis to determine if Third Parties are meeting and can continue to meet the terms and conditions of their Contracts. All performance reviews must be documented and stored in a centralized location as specified by the TPRM Program Office.

Approved by HESCOM BoD

2. BUs must immediately notify the TPRM Program Office if they observe or are made aware of any information security and privacy Risk or discrepancy that is in violation of any Third Party's agreement or any applicable HESCOM information security and privacy requirements.
3. Certain events or changes to the scope or nature of services require a re-assessment of the Third Party's information security and privacy controls. Examples include, but are not limited to:
    - An additional service line added to the contract;
    - Contract renewal or renegotiations;
    - Failure by the Third Party to remediate any open action items from previous assessments or failure to comply with information security and privacy requirements outlined in the contract;
    - The occurrence of an information security or privacy incident at the Third Party;
    - Changes in a Third Party's organizational structure (e.g., mergers, acquisitions), operations, or financial stability;
    - Material changes to the amount of HESCOM Information and/or Information Systems the Third Party will access, process, transmit, or store; and/or
    - New or redefined state or federal requirements.
4. BU Third Party Relationship Owners must ensure Risks that arise from the completion of a re-assessment are documented, classified, and tracked through resolution. When necessary, Risks must be escalated to the appropriate stakeholders for further mitigation.

F. Contract Transition or Termination

1. The TPRM Office must establish and maintain a termination process that outlines information security and privacy controls and requirements that must be followed when a Third-Party Relationship must end.
2. BUs must provide Third Parties with written termination instructions, detailing specific requirements for how Third Parties should handle, return, and/or destroy HESCOM Information and/or Information Systems in their possession or control.

Approved by HESCOM BoD

9.13. Cyber Crisis Management Plan

Introduction

The Cyber Crisis Management Plan helps lay down a strategic framework to prepare for, respond to, and begin to manage recovery from a cyber-attack. The plan covers various forms of cyber crisis, possible targets and its associated impacts, stakeholder responsibilities, and cyber incident response coordination within an enterprise to deal with cyber crisis situations. This section and the sub-sections below discuss the cyber crisis management in brief. HESCOM may choose to develop a separate Cyber Crisis Management Plan broadly covering the below mentioned points –

a. The crisis situations should be identified and defined in detail

b. Various system and network anomalies/symptoms causing cyber crisis shall be defined

c. Mechanisms for identification and reporting the anomalous behaviour of IT Infrastructure

d. Mechanism needs to be defined for declaring a cyber crisis and frameworks & matrices developed for declaring a cyber crisis based on severity and impact.

e. Stakeholders need to be identified and roles and responsibilities need to be fixed for crisis wise response

f. Preventive and detective controls need to be defined for every crisis situation

g. Cyber incidents pertaining to the attack on critical information infrastructure shall be reported to institutions like NCIIPC

h. The cyber security management plan (CCMP) shall be reviewed once a year or as and when required

i. Mock drills shall be carried out for testing the organization CCMP

Nature of Cyber Crisis and Contingencies

Cyber-attacks can be triggered on:

- Individual Systems
- Multiple Systems and Networks in a single organization
- Multiple Organizations within a State or the Nation

An attack can be categorized into several formats such as:

- Probing and Reconnaissance of networks and IT Infrastructure

- Large scale defacement of websites
- Malicious code attacks [virus/worms/trojans/botnets]
- Large scale SPAM attacks
- Identity theft attacks
- Denial of service attacks and Distributed denial of service attacks
- Domain Name Server attacks
- Application Level attacks
- Cyber Espionage and Advanced Persistent Threats

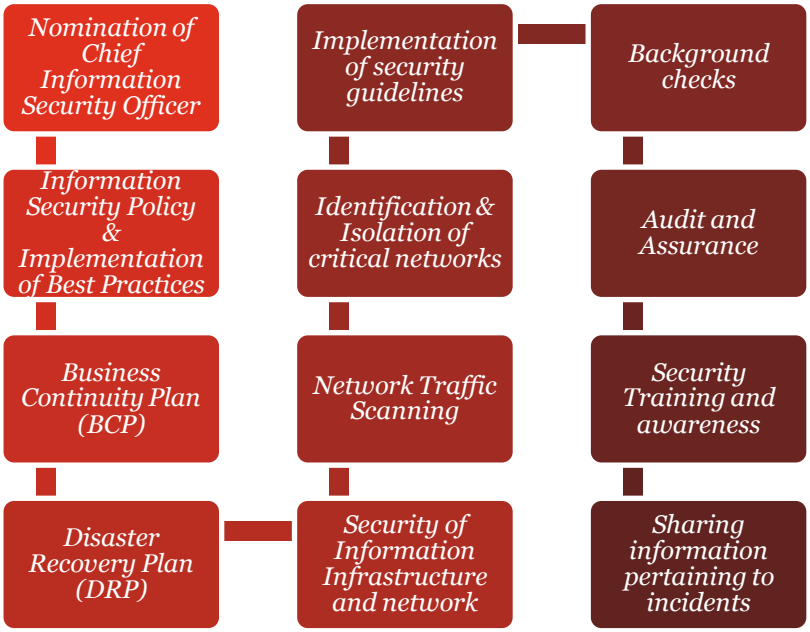
Building Cyber Resilience

Cyber Resilience is the ability of an enterprise to:

1. **Anticipate:** Being prepared to foresee compromises of business functions from cyber-attacks.
2. **Withstand:** Continue major business functions irrespective of a successful cyber-attack by an adversary.
3. **Contain:** Isolate trusted systems from threat prone systems and localize the containment of crisis to continue major business functions during cyber-attacks.
4. **Recover:** Restore the failed business operations to the maximum extent possible post the cyber-attack.
5. **Evolve:** To improve the cyber security capabilities to minimize further attacks.

Prevention and Precautionary Measures

The below mentioned roles, processes, etc. need to be in place to ensure proactiveness in handling of situation, in the event of occurrence, prevention and precautionary measures of the same.



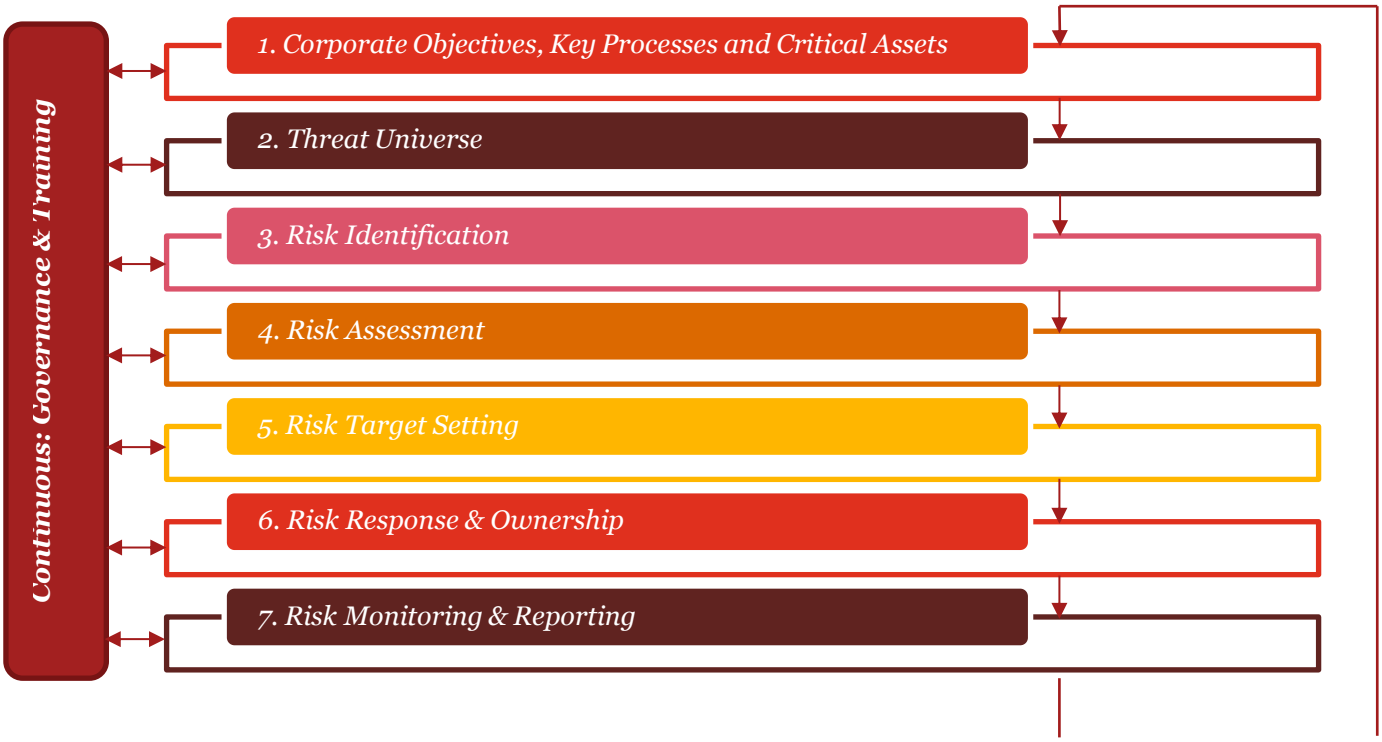
Crisis Management and Emergency Response

Crisis Management and Emergency Response are a set of actions focusing on quick response and remedial measures and restoration to normal state in the emergence of a crisis. The set of actions are as follows:

- Containment of crisis and communication to all stakeholders
- Coordinate and facilitate swift response in a timely manner
- Ensure Business Continuity in accordance with the Business Continuity Plan
- Analyse the crisis event, implement appropriate disaster recovery measures and return to normal state at the earliest
- Learn from the crisis, improve and always be prepared

Cyber Risk Management

The below indicated framework is for addressing and management of the cyber risks that may arise. The below mentioned components must be addressed to proactively assess and mitigate any risks that may exist or may occur in future.



Identification of Digital Assets

Identification of key digital assets of HESCOM is very critical to mitigate challenges, if any, being faced. It is also advisable to categorise the digital assets into two categories, viz. Information Technology (IT) and Operational Technology (OT) assets.

The term Information Technology (IT) refers to anything related to computing technology. The term 'operational technology' (OT) refers to the hardware and software used to control industrial processes. With time, OT systems are becoming increasingly interconnected and integrated with the IT systems. Keeping this in view, it become only imperative, to mitigate the risks that may exist for the OT systems and have convergence of policy measures for both IT and OT system

IT and OT systems should be both categorised for any risks and necessary measures may be taken as indicated in this policy document and existing industry standards. Below diagram presents a risk rating matrix for both IT and OT systems

Risk Name	IT Risk Rating	OT Risk Rating
Sensitive Data Leakage	Medium	-
Network breach	Medium	High
Data destruction	Medium	
Application/system malfunction	-	High

INDICATIVE

Failure of Utility infrastructure	-	High
Unauthorized personnel entry	Medium	High

Critical Information Infrastructure

As per IT Act 2000 (amended 2008), Critical Information Infrastructure means "Computer Resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety" [3]. National Critical Information Infrastructure Protection Centre (NCIIPC), a Government of India organization has published Guidelines for Identification of Critical Information Infrastructure [4] and Framework for Evaluating Cyber Security in Critical Information Infrastructure [5]. HESCOM may use the same identify its critical information infrastructure and evaluation of the same.

[3] https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf
[4] https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf
[5] https://nciipc.gov.in/documents/Evaluating_Cyber_Security_Framework.pdf

Definitions

Term	Definitions
User ID	A unique sequence of characters used to identify a single account and facilitate access to HESCOM's Information Systems and/or network.
Asset	Information System and Information. Please see corresponding definitions.
Asset Owner	Designated HESCOM officer/employee or Business Unit who has authority over the business process/data that the Asset supports or enables. The Asset Owner is accountable for the production, development, maintenance, use, and security of an Asset. Asset ownership may be allocated to: A business process A defined set of activities An application A defined set of data
Application Owner	A type of Asset Owner with the responsibility to ensure that the program or programs, which make up the application, accomplish the specified objective or set of user requirements established for that application, including appropriate security safeguards.
Authorization	Process ensuring that correctly authenticated Users can access only those resources for which approval has been given.
Authentication	Process of verifying identity of an individual, device, or process
Baseline Build Configuration	Standardized software and settings, including security, which are applied to a computing device when the device is being prepared for use.
Birthright Access	The minimum base access granted to an individual, upon joining the HESCOM Workforce, which is shared by a group of peers with common organizational attributes such as similarities in job title, department, or location.
Business Partner (BP)	An entity with which HESCOM has some form of alliance, such as a supplier or vendor. The BP employees and other persons under their control are considered Non-HESCOM workforce

Term	Definitions
Business Owner	key stakeholder within HESCOM who has a need to support HESCOM's business objectives, defines the business requirements, and is accountable for the access approvals.
Bring Your Own Device (BYOD)	The practice of allowing officers/employees of an organization to use their personally-owned computers, smartphones, or other devices for work purposes.
Business Impact Analysis (BIA)	An on-going process performed by The Service Continuance Team to determine the criticality of clinical and business departments, processes, and computer applications relative to the continued operation of the organization in the event of an unplanned disruption.
Business Tools	Refers to telephones, desks, file cabinets, copy machines, and other job-specific equipment and tools that process, transmit, or store HESCOM information and assets. It also includes electronic tools including computers, mobile devices (e.g., smartphones tablets, etc.), printers, internet, intranet, electronic mail, voice mail, and fax machines.
Business Unit (BU)	Sections and departments of HESCOM's organization that represents a specific business function or collective of related functions.
Cardholder Data (CHD)	Data used to process payment card transactions, including the primary account number (PAN), cardholder name, expiration date, and service code (i.e., three- or four-digit security code).
Categorization	The process of characterizing an object (e.g., Information, Information System) based on the potential impact to HESCOM should certain events occur which jeopardize confidentiality, integrity, or availability of the Information and/or Information System
Confidential	Data that is protected by law, contract, or policy. Data is available to certain authorized individuals and is only released as permitted by applicable policies and procedures with approval of the Data Owner(s), the Legal Department, or Risk Management.
Contract	Binding written agreement (e.g., service agreements, purchase orders (POs)) between HESCOM and a Third Party which sets forth the terms and conditions of a business relationship. This does not include Non-Disclosure Agreement (NDA).

Term	Definitions
Cryptography	Method of converting an original message of regular text into encoded text. Examples of cryptographic functions include, but are not limited to: ▪ Encryption and decryption ▪ Digital signatures ▪ Authentication techniques ▪ Random number generation
Data Classification	The process of categorizing both HESCOM electronically-stored Information (ESI) as well as electronic Information, based on its sensitivity, business value, context, and regulatory and legal requirements. Data Classification determines the level of safeguards that are applied to the Information and to the Information System it is stored on.
Data Owner	Type of Asset Owner that can authorize or deny access to certain data and is responsible for its accuracy and integrity.
Demilitarized Zone (DMZ)	Physical or logical sub-network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.
Development Environment	Environment where developers configure, customize, and use source control to build an application to be promoted to the Test Environment.
Distribution	Handing out written materials (such as brochures, literature, and other documents) or items (such as books, promotional products like pens and other office supplies, water bottles, coffee mugs, etc.) in support of a cause or organization. Distribution includes giving literature/items to another, whether they are provided for free or for a charge.
Due Diligence	The process of gathering information and documentation about a Third Party for the purpose of evaluating the Risks associated with that relationship and the need and degree of ongoing oversight.
Due Diligence Assessment	Evaluation process used to determine whether a potential Third Party maintains appropriate controls to mitigate identified Risks that may arise from the fulfilment of the service.

Term	Definitions
End of Life	The final stage of an Asset's existence, where the Asset is discontinued from vendor production and support perspective
Electronic Communication	Transfer of HESCOM data transmitted via electronic mail, text messaging, instant messenger, or online meeting platform.
Incident	An occurrence or event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Information System or the Information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of HESCOM policies, procedures, or acceptable use policies.
Incident Response Playbook	Step-by-step guidance outlining the proper information security response activities after the classification and criticality of the Incident have been determined.
Information	Any information collected, processed, maintained or stored by HESCOM, or on behalf of HESCOM; including, but not limited to, workforce, affiliate, member and/or customer data.
Information Systems	Information technology systems, devices, and media (HESCOM and personally-owned), where HESCOM data is electronically stored, transmitted, or processed.
Inherent Risk (IR)	The innate Risk associated with a particular activity, product, service, or process without consideration of controls or the potential Third Party providing the product or service.
Inherent Risk Questionnaire (IRQ)	The form completed to capture project and background information, as well as identify potential Risks associated with a particular engagement
Internal	Data that is available for use within HESCOM and may be shared outside the organization only if there is a legitimate business need to know and is approved by the Data Owner(s).
Internal Risk	The innate risk associated with a particular activity, product, service, or process without consideration of controls or the potential Third Party providing the product or service.
IT Owner	Person(s) who have primary responsibility for system administration, maintenance, and ensure that the system is available to end-users.
Manager	A HESCOM Workforce Member with direct reports

Term	Definitions
Media Device	Any device capable of recording, reproducing, distributing, or playing audio and video signals. Such devices include, but are not limited to: computers, media servers (interactive TV), DVD players, VCRs, iPods, iPads, mp3 players, tablets and mobile devices.
Multi-Factor Authentication	Method of authenticating a User whereby two or more factors are verified. These factors include: • Hardware or software tokens (something the User has) • Password, passphrase, or PIN (something the User knows) • Fingerprint, retinal scan, or other forms of biometrics (something the User is or does)
Non-Public	Data that is classified as Confidential, Restricted, or Internal data. Please see corresponding definitions.
Non-Production Environment	Development, Test, QA Environments; refer to corresponding definitions for each data type.
Non-HESCOM Workforce	Individuals (including vendors, Business Partners, students, affiliated physicians, joint ventures, volunteers, etc.) who are not under the direct control of HESCOM and/or who access HESCOM Information Systems or data.
Payment Card Information (PCI) System	Technologies deemed to be in scope for compliance with the Payment Card Industry Data Security Standards (PCI DSS) requirements. PCI Systems includes, but are not limited to, any machine, terminal, system, or application that stores, processes, or transmits cardholder data, including network (i.e., firewalls, routers) and system (i.e., desktop/laptop computers, servers, applications) components that are connected to the cardholder data environment (CDE). This also includes, by reference, any person, business process, workflow, or tool that supports storing, processing, or transmitting (CHD).
Production Environment	Environment where real-time staging of programs that run an organization are executed.
Personally-Owned Devices	A device that was purchased, owned, and used by an individual to access HESCOM's corporate network. Examples of personally-owned devices include personal computers, smartphones, tablets, pagers, and other devices.
Personally Identifiable	Any oral, written or electronic individually identifiable personal information

Term	Definitions
Information (PII)	collected or stored by a facility. Examples of PII include the following data elements. i. Bank/Credit Union account numbers ii. Biometrics (finger/face print) iii. Birth certificate iv. Citizenship v. Credit card expiration date vi. Credit card number vii. Criminal records viii. Date of birth ix. Date of death x. Death certificate number xi. Dependent information xii. Disability information xiii. Driver's license number xiv. Financial data xv. Home address xvi. Home phone number xvii. IP address xviii. Mother's maiden name xix. Name xx. Other identity verification or authentication data xxi. Passport number xxii. Personal phone number xxiii. Personal e-mail address xxiv. Photo xxv. Race or Ethnicity xxvi. Salary and bonus xxvii. Aadhaar Number xxviii. Vehicle registration plate number xxix. Work eligibility
Provisioning	The act of assigning and providing a User(s) access to a secured resource; provisioning can be performed for User accounts or service accounts

Term	Definitions
Principle of Least Privilege	Principle that holds that entities (people, processes, devices) should be assigned the fewest necessary data access privileges consistent with their assigned duties and functions.
Privileged Account	An account with elevated access rights and/or permissions to key HESCOM assets, including but not limited to: operating systems, database servers, User directories, network devices, and enterprise resource planning applications
Quality Assurance (QA) Environment	Environment where developers test upgrade procedure against controlled data and perform controlled testing of the resulting application.
Recovery Point Objective [RPO]	The maximum tolerated period to recover from in the event of a disaster.
Recovery Time Objective [RTO]	The goal for how soon each business process must be restored to operation after a disruption
Remote Access	The ability for HESCOM Workforce, Non-HESCOM Workforce, and Medical Staff Members to access HESCOM's internal networks, computing devices, or data from external locations (i.e., internet) other than HESCOM's facilities
Residual Risk	The risk of a particular activity, product, service, or process after taking into account the ability to mitigate the Inherent Risk through the use of controls.
Restricted	Data that is available for internal or external use only with prior approval by the Data Owner(s).
Restricted Services	Prohibited use of HESCOM Information and/or Information Systems for any other business or profit-making activity, commercial venture, solicitation of non-company business, advancement of outside organizations, personal views, religious or political causes, or for personal gain.
Risk	A measure of the extent to which HESCOM is threatened by a potential circumstance or event, and typically a function of: • The adverse impacts that would arise if the circumstance or event occurs • The likelihood of occurrence
Risk Assessment	Process that identifies Risks to organizational operations, Assets, and individuals resulting from the operation on an Information System.

Term	Definitions
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), Assets, and individuals.
Risk Owner	An individual with understanding of the Risk and associated Risk outcomes/implications. The Risk Owner has the accountability, authority, and resources to manage the information security Risk and related mitigation activities.
Risk Register	Record of information about identified risks.
Risk Tolerance	Level of Risk or degree of uncertainty that is acceptable to HESCOM.
Safeguards	Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, Information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
Service Account	Computer account used by systems, applications, batch processes, or other non-interactive purposes for internal, system-related tasks
System Account	Accounts(s) provided with a product or operating system for the purpose of providing access; these accounts typically provide administrative access.
Sensitive Personally Identifiable Information (PII)	Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. PII that is sensitive includes: **Stand Alone:** • Aadhaar Number • Driver's license or state ID number • Passport number • Alien Registration number • Bank/Credit Union account number • Biometrics (finger/face print) **If Paired with Another Identifier:** • Citizenship or immigration status

Term	Definitions
	• Medical information • Ethnic or religious affiliation • Sexual orientation • Account passwords • Last 4 digits of Aadhaar Number • Date of birth • Criminal history • Mother's maiden name
Solicitation	Asking a person to support a cause or organization, either financially (such as by asking a person to purchase an item or membership) or by making a personal commitment (such as by asking a person to attend a meeting of an organization or to join an organization). Some examples of Solicitation include the following activities, but this list is not exhaustive: 1. Asking officers/employees or visitors to support an organization; 2. Asking officers/employees or visitors to donate to a charity; 3. Asking officers/employees via email to click on a link or go to a website in support of a cause or organization; 4. Selling candy to raise money for a child's extracurricular activity; 5. Selling personal items such as cars, boats, exercise equipment; or 6. Asking officers, employees, patients or visitors to join a club.
Third Party	Companies and/or firms accessing, processing, transmitting, storing, or collecting Information, products, services, technology, capability, communication, capacity, or data that enables it to perform operations and service customers, patients, and Workforce Members.
Third Party Risk Management Program (TPRM)	Comprehensive framework for ensuring information security and privacy Risks are identified, considered, and managed during the Third-Party selection and contracting process and there is ongoing program oversight (e.g., testing and review) commensurate with the identified Risk.
Third Party Risk Management (TPRM) Program Office	HESCOM's organizational body that facilitates, coordinates, creates, evaluates, and monitors Third Party relationships, including establishing a Third-Party Risk Management information security and privacy requirements and controls
Unsolicited Bulk Electronic Mail	Electronic mail, used for non-business purposes, sent to a large numbers of electronic mail accounts.

Term	Definitions
User	Any individual with access to HESCOM Information, including, but not limited to, HESCOM Workforce, Non-HESCOM Workforce, Medical Staff Members, Business Partners, consultants, contractors, and temporary workers.
Workforce Member	Officers, Employees, volunteers, trainees, students, physicians, contracted staff, consultants, or other persons who perform work for and on behalf of HESCOM.
Zero Trust Network	Network that treats all traffic as untrusted, restricting access to secure business data and sensitive resources as much as possible to reduce the risk and mitigate the damage of breaches.
Insufficient Authentication Controls	An attacker could use a brute-force attack to determine the password of one account; if other accounts are connected to it through a single-sign-on arrangement, the attacker would then have administrative access to a number of systems.
Cross Site Scripting (XSS)	Cross site scripting is a type of attack in which the victim's web browser is induced to execute malicious code. Depending on the type of attack, the malicious code may steal the victim's personal information, enabling the attacker to impersonate the victim, or cause the victim's computer to launch an attack against a third party without either the victim's or the third party's knowledge
Cross Site Request Forgery (CSRF)	Cross site request forgery is an attack which causes an end user's web browser to execute actions of the attacker's choosing without the user's knowledge. By embedding a malicious link in a web page or sending a link via email or chat, an attacker may cause the users of a web application to perform unwanted actions. More specifically, the attacker causes the user's browser to make requests to a web site to which it has been authenticated, without the user's or the web site's knowledge. These actions may result in compromised end user data and operations, or even an entire server or network.
Phishing	Many people view social media sites on cell phones or other mobile devices. This makes it harder to distinguish real and fake web sites. Additionally, social media enables attackers to send phishing messages that appear to come from someone that the victim knows. Having obtained login information for a few accounts, scammers will then send out messages to everyone connected to the compromised accounts, often with an enticing subject line that suggests familiarity with the victims.
Information Leakage	Social media sites like Facebook and Twitter create the illusion of familiarity and intimacy on the Internet. The result is that people may be inclined to share

Term	Definitions
	information on the Internet that their employer would have preferred to keep private. Individuals may not be divulging trade secrets, but the cumulative effect of small, seemingly innocuous details can enable a business's competitors to gain valuable intelligence about that company's business situation and future plans.
Injection Flaws	The technologies that social media uses make it vulnerable to injection attacks such as XML injection. Additionally, social media applications often rely on client-side code, so they rely heavily on client-side input validation which an attacker can bypass.
Information Integrity	Data integrity is one of the foundations of information security. Malware introduced on a platform or network can modify user information and databases. Users who do not diligently update their antivirus software can make their systems vulnerable. An attacker could deliberately modify data in transit or storage through malware or direct manipulation, but legitimate users also make honest mistakes. Unintentional misinformation is frequently posted on the Internet, which is then taken as fact by many viewers. In social media, data is stored in many places where many different users can access it. Having data accessible to many users increases the chance that a malicious or mistaken user could post inaccurate information, which compromises data integrity.

10. Policy Compliance:

11.1 **Compliance Measurement:** The Security Management team will verify compliance to this policy through various methods including business tool reports, internal and external audits, periodic walk through etc.

11.2 **Non-Compliance:** Any violations to this policy would be governed as per IT Act, 2000 and its subsequent amendments and rules & regulations of HESCOM, Government of Karnataka and Government of India.