भारतीय अन्तर्देशीय जलमार्ग प्राधिकरण
(पत्तन, पोत परिवहन और जलमार्ग मंत्रालय, भारत सरकार)
मुख्यालय: जलमार्ग भवन, ए-13, सैक्टर-1, नौएडा-201 301 (उ0प्र0)

INLAND WATERWAYS AUTHORITY OF INDIA
(Ministry of Ports, Shipping and Waterways, Govt. of India)
Head Office : Jalmarg Bhawan, A-13, Sector-1, Noida-201 301 (U.P.)
Website: www.iwai.gov.in | www.iwai.nic.in

Tel. : +91-120-2544036, 2543972, 2527667, 2448101 Fax : +91-120-2544009, 2544041, 2543973, 2521764

File No.: IWAI/EDP/DLTREGISTER/2024 Date 09.05.2025

OFFICE MEMORANDUM

Subject: Information Security Policy of IWAI -reg

To ensure the protection of information assets of all the employees and secure & resilient operation of IWAI, Competent Authority has approved the Information Security Policy of IWAI.

2. Accordingly, the 'Information Security Policy' is hereby circulated for implementation with immediate effect. A copy of the Policy is enclosed herewith for compliance.

This issues with the approval of the Competent Authority.

Enclosed As Above:

09.05.2025

(Neeraj Singh)
Assistant Secretary (Admn. & Estt.)
Email Id : nsingh@iwai.gov.in
Phone : 0120-2474050

To

All Officials/Officers, IWAI.

Copy also to : (By e-mail)

i. CE (Tech)/CE (JMVP)/ CE (NER) & OW)/Hydrographic Chief/CAO/Deputy Secretary (P&C)/ Director (RE)/Direcro9t (JMVP)/ Director (Hydro.)/Assistant Secretary (L&H), IWAI, Noida.
ii. Director/Director (I/C), IWAI, Patna/Kolkata/Kochi/Bhubaneswar/Guwahati/ Varanasi.
iii. Officer-In-Charge, Sub Offices, Prayagraj, Sahibganj, Farakka, Swaroopganj, Vijayawada/
iv. PCSA (IT), IWAI, Noida- for uploading on IWAI website
v. Hindi Cell- for Hindi translation
vi. Section Office (Estt-I)/II/III
vii. Office Copy/Master Copy

Copy for kind information to: (By E.mail)

PPS/PS/PA to Chairman/Vice-Chairman/Member (Fin.)/ Member (Tech.)/ Member (Traffic)/Secretary, IWAI

Information Security Policy

Inland Waterways Authority of India

Version 1.0, 2025

Contents

Policy

1. Inland Waterways Authority of India

The Inland Waterways Authority of India (IWAI) was established on 27th October 1986 for the development and regulation of Inland waterways for shipping and navigation. The Authority primarily undertakes projects for development and maintenance of IWT infrastructure on national waterways through grant received from Ministry of Ports, Shipping and Waterways. The head office of the Authority is located at Noida. The Authority also has its regional offices at Patna, Kolkata, Guwahati, Varanasi, Bhubaneswar and Kochi and sub-offices at Prayagraj, Farakka, Sahibganj, Haldia, Swroopganj, Hemnagar, Dibrugarh, Dhubri, Silchar, Kollam and Vijayawada.

2. Purpose of the Policy

This policy establishes the mandatory minimum standards for information and data security within IWAI, aimed at ensuring the implementation of a sanitized and secure IT framework across the organization. The policy aims to maintain compliance with Digital Personal Data Protection Act, 2023[1] and adherence to the security guidelines of Ministry of Electronics and Information Technology (MeitY)[2], Government of India and CERT-In[3].

This policy serves as a foundational document for all other security policies and associated standards. This policy defines the responsibility to:

a. protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets
b. manage the risk of security exposure or compromise
c. assure a secure and stable information technology (IT) environment
d. identify and respond to events involving information asset misuse, loss or unauthorized disclosure
e. monitor systems for anomalies that might indicate compromise; and
f. promote and increase the awareness of information security.

This policy benefits IWAI by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

a) Responsible Officers

Chief Information Security Officer (CISO)- Overall In-charge of Cyber Security.

[1] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[2] https://www.meity.gov.in/documents/act-and-policies?page=1
[3] Guidelines on Information Security Practices for Government Entities

Deputy Information Security Officer (DISO)- Assisting the CISO.
One designated officer from the Electronic Data Processing Cell of the Authority- Assisting the DISO.
In the absence of CISO, DISO will discharge the duties of CISO. In the event of both CISO & DISO being unavailable, HoD (IT) will be in charge of CISO.

b) Infrastructure

The Authority's IT framework ensures secure and efficient operations through a protected internet and structured network management. Only licensed and free open-source software (FOSS) approved by MeitY[4], is authorized for use, with NIC email designated as the sole official email platform. Field offices are equipped with broadband connectivity and safeguarded by Firewall & licensed antivirus solutions, maintaining a consistent and secure IT environment.

c) Policy

I. This policy applies to all locations of IWAI, all personnel working on the IWAI network and applications.
II. This policy encompasses all systems, automated and manual, for which IWAI has administrative responsibility, including systems managed or hosted by third parties on behalf of IWAI. It addresses all information, regardless of the form or format, which is created or used in support of business activities.
III. The following core domains have been covered as a part of this document. These are listed below:
   a) Network and Infrastructure Security
   b) Identity, access and privilege management
   c) Physical Security
   d) Data Security and Handling
   e) Threat and vulnerability management
   f) Personnel Security
   g) Security and incident management
   h) IT Asset Management
   i) Mobility and Bring Your Own Device (BYOD)
   j) Virtualization
   k) Social Media
   l) Security Testing
   m) Security Auditing
   n) Operations Security
   o) Open-Source Technology
   p) Business Continuity Plan

d) Information Security Audit

The Information Security audit of the Authority is to be carried out internally on annual basis

[4] https://www.meity.gov.in/static/uploads/2024/03/Policy-Document.pdf

while an annual audit to be conducted by a CERT-In empaneled independent Agency.

e) Compliance Matrix

The Compliance matrix on Information with Cyber Security to be drawn up based on guidelines issued by MeitY, from time to time. Efforts are to be made to ensure compliance of all parameters listed in the compliance matrix.

f) Cyber Threats

Various natures of cyber threats are to be reported by CISO in line with the guidelines of CERT-In[5]. The individual employees identifying such suspicions / threats are to report to CISO to enable him to escalate the same to the appropriate level.

3. User Awareness and Training

a) Awareness training program

i. The program should aim to increase user understanding and sensitivity to cyber threats and vulnerabilities.
ii. The awareness program should focus on the need to protect Authority's sensitive and classified information.
iii. Awareness training must be provided for new joiners as part of Induction training. Further, it should be provided to all employees annually.
iv. Information Security Awareness training including simulated phishing to be provided to all the employees for creating awareness about threats such as identity theft, adware, spear phishing, whaling, malware downloads etc.

b) Role Based Training

i. The Authority will ensure that role-based training is provided to all personnel within the Authority to familiarize them with their roles and responsibilities to support security requirements.
ii. The Authority will ensure that information security awareness and training include the following are as follows: -
    a. Purpose of the training or awareness program.
    b. Reporting any suspected compromises or anomalies
    c. Escalation matrix for reporting security incidents
    d. Fair usage policy for assets and systems
    e. Best practices for the security of accounts
    f. Authorization requirements for applications, databases and data
    g. Classifying, marking, controlling, storing and sanitizing media
    h. Best practices and regulations governing secure operation and authorized use of systems.

c) To maintain situational awareness of the latest cyber security threats by following the website of CERT-In and alerts and advisories of the same. To follow measures suggested by CERT-In for cyber hygiene including prevention of cyber threats.

[5] Guidelines on Information Security Practices for Government Entities

d) Alerts and advisories are available on the following websites:

i. Indian Computer Emergency Response Team (CERT-In): https://www.cert-in.org.in/

ii. Cyber Swachhta Kendra (CSK): https://www.csk.gov.in/

e) A comprehensive training calendar should be finalized and circulated, ensuring adherence to the planned schedule. Additionally, the CISO is authorized to make necessary amendments to the calendar during the financial year to address evolving requirements of the Authority.

4. Security Monitoring and Incident Management

All employees of IWAI are obligated to adhere to the confidentiality requirements and responsibilities outlined under the applicable laws governing sensitive information, including maintaining strict discretion in their professional duties. Any unauthorized possession/ divulgence of information will make the employees liable to be prosecuted under the afore mentioned Act.

The Authority face significant risks of information loss through inappropriate/ unauthorized access and other malicious activities that have implication such as sensitive information leakage resulting in misuse, financial loss and loss of reputation. Security monitoring and incident response management is a key component of the Authority's information security program as it helps build organizational capability to detect, analyze and respond appropriately to a cyber security incident/ cyber-attack which might emanate from external or internal sources.

a) Preparedness is the key for effectively handling/responding to a cyber security incident. Authority should identify a cyber security team under the leadership of CISO. The Authority should build appropriate cyber security capabilities for incident management. There are four key phases to Incident Response:

i. **Preparation:** An incident management plan must be in place to prevent and effectively respond to cyber security incidents.

ii. **Detection and analysis:** Second critical phase is to determine the occurrence of an incident, assess its severity, scope and the type of an incident.

iii. **Containment and eradication:** The purpose of this phase is to limit the effects of an incident for further damage. Affected hosts or systems are identified, isolated or mitigated, and when relevant stakeholders / affected parties are notified, and investigative process established. This phase also includes short- term containment, backup & restore, long-term containment, sub-procedures for seizure and evidence handling, escalation, and communication.

iv. **Recovery & lessons learned:** Recovery is the analysis of the incident for its

procedural and policy implications, the gathering of metrics, and the in incorporation of "lessons learned" into future response activities and training. A lesson learned meeting should be called after a major incident with the goal of improving security as a whole and incident handling.

b) The Authority will ensure that apart from addressing an incident, it is mandatory to report cyber incidents to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. Also, the information about its occurrence shall be shared with relevant stakeholders such as NIC-CERT, sectoral CSIRT, Regulators etc. as applicable.
c) Document procedures for reporting and handling a suspected incident, how NOT to tamper with potential evidence (i.e., NOT to attempt forensics when not authorized)
d) Document the incident analysis reports and include key aspects such as vulnerabilities exploited, gaps in security processes & security controls, impact of the incident, mitigation strategies etc.
e) The goal to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible. To lessen uncertainties, the focus is on authentication, authorization, and shrinking implicit trust zones while maintaining availability and minimizing delays in authentication. Access rules are made as granular as possible to enforce the least privileges needed to perform the action in the request.
f) The Cyber security team of the Authority shall possess system details, or reference to the location of information to be referred at the time of an incident i.e. information flow diagrams, network diagrams, system hardware inventory, logging information etc. A network diagram shall be updated as and when new security control or entity introduced in the network.
g) The Cyber security team shall maintain an updated list of points of contact (i.e. key persons within the Authority and the concerning SPOCs of the related organizations/ entities like NIC etc.) to be contacted at the time of incident response.
h) The EDP cell of the Authority shall actively monitor logs received at centralized location from various security mechanisms control devices implemented throughout the network of the Authority. Appropriate alerting mechanisms may be configured in a system for immediate alerting.
i) An effective defence-in-depth strategy may include (but not limited to) security best practices , tools, and policies including Network Segmentation, Firewalls, Intrusion Prevention or Detection Systems (IPS/IDS), The Principle of Least Privilege, Strong authentications, SIEM, Security orchestration, automation, and response (SOAR), User and entity behaviour analytics (UEBA), NDR, XDR, Data Leak Prevention (DLP), log repositories, online log retention, Antivirus and antispam solutions at gateways, Endpoint Detection and Response (EDR), Patch Management etc.
j) CISO to guide the Authority in responding to cyber-related incidents such as comprehensive Cyber Crisis Management Plan (CCMP).
k) Adhere to the Security Advisories published by NIC-CERT (https://nic-cert.nic.in/) and CERT-In (https://www.cert-in.org.in).

l) Report any cyber security incident, including suspicious mails and phishing mails to NIC- CERT (incident@nic-cert.nic.in) and CERT-In (incident@cert.org.in).

5. Audit

a) To facilitate conducting internal and external audits of the entire ICT infrastructure and ensure deployment of appropriate security controls based on the audit outcome.

b) Internal information security annual audit will be carried out. The audit reports submitted by the Internal information security Auditors will be shared with the authorities from time to time on need basis. The internal auditors will assist in preparation, testing and implementation of the Business Continuity Plan (BCP) and Disaster Recovery (DR) plan.

c) The Authority will compulsorily maintain inventory of only authorised hardware and software (including versions, patch level, validity of support etc) along with mechanism for automated scanning to detect presence of unauthorized device and software. The audit of the above will also be within the ambit of the terms of reference of the Internal Auditors.

d) The 3rd Party Security audits would be conducted annually by the CERT-In[6] empaneled auditors.

e) Functional Audit: Functional Audit will examine whether the company's IT systems operate according to predefined business logic and identify areas which do not comply with either efficiency or business requirements. Specifically, the subject audit is carried out mandatorily, prior to the software delivery/production to verify that all requirements specified in the Software Requirements Specification have been met.

f) Security auditing guidelines

i. **Audit management function:** A dedicated management function is formulated by the Authority to conduct security audits and associated tasks such as the following:

1. Compiling audit requirements
2. Defining audit types.
3. Identifying audit engagements.
4. Planning and arranging audits.
5. Overseeing audit execution.
6. Managing engagement performance.
7. Actions on audit results.
8. Follow-up audits.
9. Reporting to the management.

g) Risk Assessment and security auditing requirements

The Authority must hold meetings with all stakeholders and head of the departments to chalk out the requirements for security audits such as the following:

[6] https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

I. Scope of the audit.
II. Risk based asset classification.
III. Audit benchmarks, standards and compliance requirements.
IV. Remediation plan on audit findings.
V. Audit report format along with requirements of evidence and artifacts.
VI. Follow-up audits.
VII. Examine the effectiveness of the existing policy, standards, guidelines and procedures.

h) Periodicity and nature of audits
   i. The scope of audit should be comprehensive to cover the entire ICT infrastructure of the Authority.
   ii. Internal information security audits be carried out at least once a year.
   iii. 3rd Party Security audits must be conducted periodically at least once a year to ensure compliance with security policy, guidelines, and procedures, and to determine the minimum set of controls required to address an organisation's security.
   iv. Security audit should be conducted prior to and after implementation or installation or major enhancements.
   v. Follow-up audits should be conducted to ensure compliance and closure of vulnerabilities. Management reporting and actions personnel associated with security audit should analyse auditing results to reflect current security status, severity level of the vulnerabilities or anomalies present after removing false- positives and report it to the concerned departments of the Authority for remediation. The results of all security audits must be shared with the Competent Authority of IWAI.
   vi. For detailed guidelines for Auditee entity, Auditors and Baseline requirements refer to Cyber Security Assurance section on website of CERT-In:
      i. https://www.cert-in.org.in/PDF/Auditor_Guidelines.pdf
      ii. https://www.cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf

6. Desktop/Laptop and Printer Security at Office

a) Only Standard User (non-administrator) account to be used for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.
b) BIOS Password to be set for booting.
c) Ensure that the Operating System and BIOS firmware are updated with the latest updates / patches.
d) Set Operating System updates to auto-updated from a trusted source.
e) Ensure that the inbuilt/ Cert-In or NIC approved Antivirus software on the systems is kept "On" and in auto update mode.
f) Only applications / software, which are part of the list authorized by CISO, shall be used.
g) Always log off the desktop/ laptop when not in use.
h) Desktop/Laptop/ Printers to be shut down before leaving office.

i) Keep printer's software updated with the latest updates/patches.
j) Setup unique pass codes for shared printers.
k) Printer to be configured to disallow storing of print history.
l) Enable Desktop Firewall for controlling information access.
m) Keep the GPS, Bluetooth, NFC, Wi-Fi adapter and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.
n) Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.
o) Do not write passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-itnotes, plain paper pinned or posted on users table etc.).
p) Do not use any external mobile App based scanner services (ex: Cam scanner) for scanning sensitive government documents.
q) Use of all pirated Operating systems and other software/applications that are not part of the authorized list of software's (as per MeitY/ NIC) should be immediately deleted.
r) In the event of requirement of replacement of hard disk for non-functioning, the discarded hard disk not to be handed over to the service engineer or parted with.
s) Data recovery of faulty HDD/SSD is mandatory for vendor/Service provider.
t) In case of replacement of faulty HDD/SSD by the vendor, faulty HDD/SSD will be retained by the Authority.
u) Desktop/Laptop/Printer procured by the Authority is to mandatorily be assigned to the user strictly following the laid down handover process.
v) Before disposing of any ICT device of the Authority it is mandatory to check that all data has been completely erased which will be certified by the user.
w) If the OS is corrupt due to any software, then user access regarding internet & LAN will be restricted. Decision in this regard will be taken by CISO.
x) The document pertaining to handover process will be verified by the EDP cell and a final report to be submitted to CISO.

7. Application Security

a) The Authority must incorporate security at each level of software development lifecycle such as during development, deployment and maintenance of application etc. to reduce vulnerabilities. During development secure coding practices should be followed. Testing should be conducted during development, deployment and maintenance of application.
b) Ensure privacy protection of citizen data at each stage of application life cycle.
c) The Authority must maintain an updated documents containing the list of authorized applications, their usage, custodian(s) assigned to each application, level of criticality, version implemented, number of installed instances, application license details etc.
d) Authorization and access to resources should be based on role, affiliation and membership of group rather than individual basis. Periodic review of authorization should be performed.
e) The Authority must identify ports, protocols and least privileged services required to carry out daily operations of applications / platforms and restrict or block all other less

important services.

f) The Authority should ensure that applications validate the data on the server- side.
g) Ensure that all Websites and Applications of the Authority are "https" enabled with a valid SSL/TLS Certificate.
h) Ensure applications execute proper error handling and should not provide detailed system information, deny service, impair security mechanisms, or crash the system.
i) Application security testing, functional testing, vulnerability assessment and penetration testing, should be performed at a frequency determined by the sensitivity of the information handled by applications (at least once in a year or whenever there is change in application or before production/ going live).
j) Implement measures for securing Application Program Interfaces (APIs). Include API security in Vulnerability Assessment and Penetration Testing and mitigate vulnerabilities in APIs.

8. Password Management

a) Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
b) It is recommended to change the passwords at least once in 120 days
c) Use Multi-Factor Authentication, wherever available.
d) Don't use the same password in multiple services/websites/apps.
e) Don't save passwords in the browser or in any unprotected documents.
f) Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table).
g) Don't share system passwords or printer pass code or Wi-Fi passwords with anybody.

9. Mobile Security

a) Ensure that the mobile operating system is updated with the latest available updates/patches.
b) Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.
c) Download Apps from official app stores of Google (for android) and apple (for iOS).
d) Before downloading an App, check the popularity of the app and read the user reviews.
e) Observe caution before downloading any apps which has a bad reputation or less user base etc.
f) While participating in any sensitive discussions, switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.
g) Don't accept any unknown request for Bluetooth pairing or file sharing.
h) Before installing an App, to carefully read and understand the device permissions required by the App along with the purpose of each permission.
i) In case of any disparity between the permissions requested and the functionality provided by an app, users to be advised not to install the App (Ex: A calculator app requesting GPS and Bluetooth permission).

j) Note down the unique 15-digit IMEI number of the mobile device and keep it offline. It can be useful for reporting in case of physical loss of mobile device.
k) Use auto lock to automatically lock the phone or keypad lock protected by pass code/ security patterns to restrict access to your mobile phone.
l) Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen.
m) Take regular offline backup of your phone and external/internal memory card.
n) Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates
o) Observe caution while opening any links shared through SMS or social media etc., where the links are preceded by exciting offers/discounts etc., or may claim to provide details about any latest news. Such links may lead to a phishing/malware webpage, which could compromise your device.
p) Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.
q) Always keep an updated antivirus security solution installed.
r) In the event of the mobile getting stolen, credentials for logging in the mobile to be changed immediately.
s) If the mobile has the facility of logging in to the official mail, the same to be securely used with high security procedure like two-factor authentication.
t) Memory card of the mobile not to share with any unknow source, for whatever reason.

10. Mobile Application Security

a) The Authority should ensure that their mobile applications address the Open Web Application Security Project (OWASP) Mobile Top 10 vulnerabilities.
b) The mobile application must implement SSL Pinning to prevent man-in-the-middle attacks.
c) No secret keys used by the application should be stored unencrypted in the application storage.
d) User data should not be stored in unencrypted/plain-text form on the device.
e) The final build of the application must not contain any test code and all debug logs must be disabled. Obfuscation of the code by packers, encryptors and related tools could be considered for preventing reversing the applications.
    I. Only permissions required for essential functionality of the application should be sought from the user.
    II. Sensitive data should be shared over secure SSL/TLS connection only.

11. Data Security

a) Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and rest. Deploy data loss prevention (DLP) solutions / processes.
b) Review and change any default/ weak/ misconfigured settings with appropriate authentication & authorization controls for all database applications.
c) Deploy detection and alerting tools and create processes to prevent, contain and respond to a data breach/ data leak.
d) Evolve and implement a Data Backup policy. All the critical data should be backed up regularly to prevent data loss and to ensure faster recovery in case of an incident.
e) Audit and remediate vulnerabilities in applications on priority, which could cause data breaches/leaks that include Insecure Direct Object Reference (IDOR), SQL injection, Insecure API endpoints, Directory listing etc.
f) Develop and maintain policies enforcing strong passwords (password management) and the use of multi-factor authentication (MFA).
g) Conduct third party risk assessments on regular basis and monitor for any data breach/ leak cases from supply chains to take necessary protective & remedial measures.
h) Implement micro-segmentation for controlled granular access to database applications.
i) Personal external storage media devices should not be allowed to be connected with critical systems or assets and vice-versa.
j) Data Backup policy:
    I. Back-up procedures should be documented, scheduled and monitored.
    II. Up-to-date backups of all critical items should be maintained to ensure the continued provision of the minimum essential level of service. These items include:
        i. Data Files
        ii. Utilities programmes
        iii. Databases
        iv. Operating system software
        v. Applications system software
        vi. Encryption keys
        vii. Pre-printed forms
        viii. Device configurations
    III. One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
    IV. Backups of the system, application and data should be performed on a regular basis as per the DR and BCP policy of the Authority. Backups should also be made for application under development and data conversion efforts.
    V. Data backup is required for all systems which are deemed critical for the Authority including personal computers, servers and distributed systems, databases, network, security equipment.
    VI. The backups must be kept in an area physically separate from the server. If critical

system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.

VII. Critical system data and file server software must have incremental backups taken daily. Based on the criticality of the applications hourly / lesser interval backup also can be considered based on the BCP policy of the Authority.

VIII. Systems that are completely static may not require periodic backup beyond the initial backup but shall be backed up after changes or updates in the information.

IX. Each LAN/system should have a primary and backup / secondary system to ensure continuity of business operations.

X. The business continuity and disaster recovery plans should be prepared and tested at least on an annual basis

k) Database server

I. Keep database server in a secure environment with access controls in place to prevent unauthorized access.

II. Keep the database on a separate physical machine, separate from the machines running applications or web servers.

III. Database server should be protected by a firewall, which denies access to traffic by default. Traffic may be allowed from specific applications or web servers that need to access the data.

IV. Limit user privileges and access.

V. Restrict administrative privileges.

VI. Maintain regular software updates for the database and DBMS

VII. Use complex passwords for database accounts, with a minimum length of 15 characters, using a combination of capital letters, small letters, numbers and special characters.

VIII. Lock database accounts with suspicious login activity.

IX. Disable unnecessary services.

X. Encrypt sensitive database information.

XI. Maintain file system integrity for incident response and regulatory compliance and monitor critical files that should be tracked for changes and accidental deletion or corruption.

a. Monitor for unusual database queries / traffic that exceeds thresholds for DLP.

12. Software Security

a) Use authorized and licensed software only.

b) Allow installation of software only from trusted application repositories.

c) Automate patching of standard and third-party applications

d) Use Software-based data encryption.

e) Uninstall software that is no longer in use.

13. Removable Media Security

a) Perform a low format of the removable media before the first-time usage.
b) Perform a secure wipe to delete the contents of the removable media.
c) Scan the removable media with Antivirus software before accessing it
d) Encrypt the files /folders on the removable media.
e) Always protect your documents with strong password.
f) Don't plug-in the removable media on any unauthorized devices.
g) No removable media shall be used without the approval of the concerned authority

14. Third Party Access and Outsourcing

a) The Authority should ensure that third party access to information should be restricted and should only be shared after signing Non-Disclosure-Agreement.
b) Wherever any activity is outsourced or awarded as work contract to any 3rd party / vendor, it shall be ensured that the contract specifies the information security requirements, and the same are complied with, in addition to the regular contractual details.
c) The following information security requirements should be documented as part of the contract:
    i. General policy on information security.
    ii. Procedures to protect organisational assets.
    iii. Restrictions on copying / disclosure.
    iv. Controls to ensure return of information/assets in their possession at the end of the contract.
    v. The right to monitor and the right to terminate services in the event of a security incident or a security breach.
    vi. Right to audit contractual responsibilities or to have the audits carried out by third parties.
    vii. Arrangements for reporting, notification and investigation of security incidents and breaches.
d) Information security audit report of the vendor to be made available to Procuring entity on periodic basis or when required.
e) Detailed list of all components of the software (including open source) / solution in the form of Software Bill of Material (SBOM) shall be provided by the vendor.
f) Vendor is also responsible for informing any identified vulnerabilities in the system to the Authority within a reasonable time period.
g) Data collected and processed by the vendor should be protected appropriately (cannot be shared with any others without explicit consent / agreement) and made available to the procuring entity as and when required.
h) External party personnel should comply with the information security policies, processes and procedures of the Authority.

i) Any external party found in violation to this policy shall be subjected to termination of contract and/or will be handled as per applicable laws, rules & regulations.

15. Secure Cloud Services

Cloud services follow a shared responsibility model for security and compliance. It is advised to thoroughly examine these models and implement appropriate security policies and measures for testing, staging and backup environments hosted on cloud services.

a) Any external party found in violation to this policy shall be subjected to termination of contract and/ or will be handled as per applicable laws, rules & regulations.
b) Check public accessibility of all cloud instances in use.
c) Make sure that no server/storage is inadvertently leaking data due to inappropriate configurations.
d) Implement the least privilege principle for access control with granular permission to cloud resources.
e) Enable cloud native security controls along with logging for critical cloud resources and ensure continuous monitoring.
f) Ensure User Accounts have Multi Factor Authentication (MFA) with strong password policy along with a procedure / standard for disabling of the account when an administrator / user leaves the Authority.
g) Detailed cloud security best practices are published on website of MeitY- https://www.ambud.meity.gov.in/

16. Internet Browsing Security

a) When accessing government applications, email services, banking/payment platforms, or other critical services, it is advisable to use Private Browsing or Incognito Mode for enhanced security and privacy.
b) For secure access to websites requiring user login, manually entering the domain name or URL in the browser's address bar is strongly recommended. Avoid clicking on external, unverified links to mitigate phishing risks and ensure compliance with CERT-In [7]security guidelines.
c) Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
d) It is strongly recommended to Not store any usernames and passwords or any payment related information on the internet browser.
e) Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc).
f) Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me toolbar etc.) in your internet browser.
g) Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software's).
h) Don't use your official systems for installing or playing any Games.
i) Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many

[7] https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

malwares and phishing sites abuse URL shortener services. Such links may lead to a phishing/malware webpage, which could compromise your device.

17. Hardening Procedures

a) Desktop

I. Ensure that all office systems are installed with genuine copy of operating system and other application software solutions. Pirated or unsupported OS/software shall NOT be installed on official systems.

II. Ensure installation of reputed Antivirus/EDR software on all the systems with regular signature updates.

III. Set/enable BIOS Password at system boot. Enable disk encryption policy on laptop/mobile devices, if possible

IV. Enable standard user (non-administrator) accounts for all users on all office systems used for regular work. Admin access shall be given to limited users on requirement with approval of competent authority. For day-to-day work / operations use standard user account / privileges and use the admin privilege only for specific tasks wherever applicable. Disable Guest user on all office systems.

V. It is recommended to install only whitelisted software on office systems based on the roles of the users. Do not allow installation of Tor browsers or such anonymizer plug-ins for standard web-browsers.

VI. Allow peer-to-peer file sharing applications to be installed on office systems or to communicate with outside internet.

VII. External USB storage devices (i.e., pen drive, memory cards, hard disk, mobile phone storage etc.) shall NOT be allowed, only authorized USB storage devices (approved by department) shall be allowed on official systems based on the roles & requirements of the user.

VIII. Ensure email client security, if used in office network.

IX. Enable system level firewall.

X. Enable system level user password policy (password complexity & password expiry)

XI. Windows Active Directory server (AD) or Lightweight Directory Access Protocol (LDAP) servers and applications should be hardened as per standard guidelines.

XII. Configure organisation DNS of all office systems

XIII. Configure NTP services of NIC in all office systems (i.e. samay1.nic.in or samay2.nic.in) or NPL (time.nplindia.org) or any other standard time source

XIV. Disable Remote Desktop (RDP), SMB, PowerShell and any other services, if not required by the Authority.

XV. Maintain centralized patch management and centralized Antivirus server managing antivirus on all office systems with up-to-date patches and signatures.

XVI. Offline backups with encryption for critical systems should be maintained.

XVII. Online backup systems should be properly hardened and access to its network should be strictly restricted. Sensitive information or data should be stored in an encrypted format.

XVIII. An inventory of all devices and systems connected to the network should be

maintained with a focus on keeping track of versions of operating systems and other software running on these devices and systems.

XIX. A policy regarding the timely update of firmware, operating systems and other software should be formed and strictly enforced. Products which have reached end of the support should NOT be used in office network.

XX. It is recommended to keep all the systems which contain sensitive data/information disconnected from the untrusted internet/ untrusted networks

XXI. Endpoint security solutions should be deployed for continuously monitoring end user devices to detect and respond to cyber threats like ransomware, malware and unauthorized access. It should record all activities and security events taking place on all office end points, which should be continuously monitored by the IT Infra/expert team.

XXII. Security measures for printers, commonly used & shared devices in network

i. Disable default credentials on printers

ii. Disable default services (i.e. FTP, HTTP, SSH, SMB, Telnet etc.) on printers, if not in use. Enable security if using any of these services for managing printer remotely

iii. Restrict internet access for all printers, cloud-printing etc., enable strict user access controls

iv. Ensure remote administration of printer with secure connection (HTTPS) only with strong admin credentials. Printer administration shall only be allowed from local network only.

v. Ensure printer firmware is updated to the latest available from OEM. Firmware update/upgrade/patch shall only be downloaded from OEM website

vi. Ensure requirement of user passcodes in case of shared printers. Don't Allow printer to store print history

vii. Configure NTP on office printer, enable logs and monitor.

viii. If dedicated VLAN / ethernet port is allocated for printers and other devices the policy should not allow other devices to use the same port for bypassing MAC address / 802.1x based authentication.

18. Email Security

a) Do not share the email password/ OTP/ TOTP with any unauthorized persons.
b) Employees must not use unauthorized or external email services to transmit sensitive or confidential official communications.
c) Don't click/open any link or attachment contained in mails sent by unknown sender.
d) Regularly review the past login activities. If any discrepancy is observed in the login history, then the same should be immediately reported to CISO.
e) Use PGP or digital certificate to encrypt e-mails that contains important information.
f) Observe caution with documents containing macros while downloading attachments, always select the "disable macros".

20. Network And Infrastructure Security

a) Key principles and measures

I. To manage the network perimeter by controlled access to ports, protocols and applications by filtering and inspecting all traffic at the network perimeter to ensure that only traffic essential to the Authority's official operations are permitted.

II. To define an appropriate network architecture including the network perimeter, all internal networks, and links with other organisations such as service providers or partners

III. To control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content.

IV. To ensure that the network is properly segmented, with separate VLANs for different functional requirements.

V. To ensure that communications between different VLANs are strictly denied by default. The same to be allowed in specific cases with consent of CISO on recommendation of DISO, on need basis with necessary precautions regarding restrictions on ports / applications / hosts.

VI. To ensure the use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the for the Authority's official activities.

VII. To make sure that the 'firewall rule set' strictly provides for denial of traffic by default and firming up a whitelist to ensure allowance of only authorized protocols, ports and applications to exchange data across the boundary.

VIII. An internal firewall for controlling connections within the LAN to be deployed and properly maintained.

IX. Detection and prevention of network intrusion to be monitored for North-South (Internet to LAN) and East-West (Between Intranet for monitoring unauthorized lateral movements) by trained/certified personnel to be engaged by the Authority. Other appropriate security devices for the said purpose to be deployed on the recommendation of the afore mentioned certified personnel.

X. Any alert generated from the devices to be seriously looked into thoroughly verified as most of them could be indicating an imminent attack.

XI. To ensure the following measures for further strengthening of the email, filtering, and web-filtering:

i. Deploying web and email filters on the network.

ii. Configuring the above devices to scan for known bad domains, sources, and addresses.

iii. Blocking the above before receiving and downloading messages.

iv. Scanning all emails, attachments, and downloads both on the mail gateway and hosts with a reputable antivirus solution.

b) Identification and classification:

I. It is to be ensured that classified information is mapped with the infrastructure elements through which the same will be transmitted, processed, or stored.
I. All infrastructure devices to be categorized as per classification of information that they manage.
II. Each network to have a security classification in order to prevent any information breach.
III. No data to be allowed to move between two different classification networks.

c) Network diagram

I. An accurate mapping of the core components, connections and information of the network to build organization's network diagram including network components such as routers, switches, firewall and other Perimeter Security devices, computer systems, IP addresses, data flow routes, blacklisted or whitelisted systems/IP addresses, open/entry ports, subnet mask, administrative interface, zones, access control lists, network name etc. to be developed.
II. The above document to be store in confidential manner as the same contains sensitive information.
III. All amendments to network diagram to be documented with reason for change.
IV. All amendments to network diagram to be documented with nature of change and person responsible.
V. All previous configuration diagrams to be mandatorily retained for reference.
VI. Proper change management procedure to be followed with documentation.

d) Network configuration

I. The Network administration team to periodically review network configuration at least every 6 months or as and when new access controls are introduced in the network.
II. The configuration of networks to be done according to the security policy of the Authority.

e) Network security measures

I. For perimeter defense, the Authority may deploy Intrusion Detection System (IDS), Intrusion Prevention System (IPS), NDR (Network Detection and Response), Extended detection and response (XDR) and Firewalls as appropriate, to monitor network or system activities, to detect and mitigate malicious activities or policy violations.
II. Deploy NextGen firewall (2 units) in High availability (HA) mode as a perimeter security device (external firewall). Another set of firewalls from different OEM shall be used as internal firewall (HA) for internal segmentation of network.
III. The Authority may deploy its own local/internal DNS servers (primary & secondary) for all segments. This will help in monitoring malicious DNS requests and blocking them by resolving to null (0.0.0.0) / localhost. Set default DNS pointing to Authority's DNS or DNS of National Informatics Centre (NIC) (IPv4 1.10.10.10/ IPv6 2409::1). In addition, Authority will block access to all DNS requests for outside /public DNS services.

IV. The Authority may deploy proxy servers and allow access for internet for clients through proxy servers only or, must follow the NIC-CERT instructions as NIC ensures a secure and resilient network environment, safeguarding government digital assets and information.
V. All devices placed within the network to have logging enabled.
VI. Logs of perimeter security devices and end points to be integrated with Security Information and Event Management (SIEM) and alerts from SIEM to be monitored and acted upon.
VII. Logs of perimeter security devices and SIEM to be stored for a rolling period of 180 days.
VIII. Using secure protocols: The Authority to ensure disabling all non-IP-based access protocols such as TELNET, and using secure protocols such as SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router/switch/server.
IX. The Authority to ensure that Virtual Private Network (VPN) is used for accessing Network Resources from Remote locations.
X. To enable Multi Factor Authentication (MFA) for VPN accounts.
XI. To enable VPN account logging and integrate VPN logs with Security Information and Event Management (SIEM) system.
XII. To Implement Media Access Control (MAC) address binding for all systems/IT devices. To Disable DHCP and set IP configurations manually.
XIII. To change all default credentials & configurations at the time of first installation.
XIV. To ensure blocking access to unauthorized remote desktop applications.
XV. The Authority to ensure that the devices procured are IPv6 compatible and enforce policy for IPv6 traffic.

f) Network Segmentation

I. To Ensure segmentation of network for creating security zones for isolating sensitive traffic and secure critical IT systems.
II. To Limit and segment user rights for access by implementing proper Access Control Lists (ACLs) in the network. Access control lists to be configured on devices such as routers and/or switches.
III. Network firewall to be used for restricting traffic movement outside the network segment.
IV. Only selected ports and protocols to be allowed for communication with selected IPs, as per requirements during the course of official work.
V. Critical servers to be either made stand-alone or member of a dedicated secure zone. The servers need not communicate amongst themselves unless they are part of same application with dedicated ports and authenticated applications.
VI. The Applications / servers and systems in the Intranet to be separated from Internet facing networks/ systems.

g) Security zones

I. To ensure use of Virtual LANs for separating the zones, logically. Communication between different VLANs to be disabled by default and to be allowed only on need basis with per port / application basis.

h) Network traffic segregation

The Authority to enforce rule set to minimize exposure of information by:

I. Implementation of traffic flow filters, the VLANs, network and host-based firewalls
II. Implementation of application-level filtering, proxies, content-based filtering.
III. Wherever possible physical segregation to be preferred over logical segregation.

i) Local Area Network (LAN) security

I. Traffic monitoring: To deploy traffic management capabilities to continuously monitor and control IP network.
II. Allocating IP address: Ensure that IP addresses allocated to each network appliance/system/server is associated with their respective MAC address and is not user modifiable.
III. For preferably, wired 802.1x based network admission control, where only the systems / end points that meets the organisational security posture to be allowed in the network.
IV. The rest of the devices to be put in a quarantine VLAN till the remediation of patch / infection is cleared for security posture.
V. The quarantine VLAN to have patch servers and remediation servers such as Antivirus servers / platforms. New devices that are connected without posture checking can go to Guest/ Internet only / Quarantine VLANs.
VI. Configure host firewall in all systems to restrict lateral traffic movement within the same network segments.
VII. The preferred approach to be such that the incoming and outgoing connections to be restricted only to needed services and its applications with default denial for rest of the traffic.
VIII. To ensure that remote-desktop softwares (like Anydesk, teamviewer, Ammyy Admin etc.) are not allowed in network.
IX. Restrict RDP (Remote desktop), if not required. If RDP is used, limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration. Allowing of RDP can be restricted only from certain hosts / VLANS / Network segments.
X. To enable manual configuration of systems in network, disable DHCP, if not required.
XI. Rogue DHCP servers have to be detected and isolated immediately.
XII. Bring Your Own Device (BYOD) to be restricted and no unknown devices to be allowed in the network without authorisation by the Network Administrator.
XIII. For official purposes, Mobile Device Management (MDM) solution that provides security functions to be considered for security, prevention of data theft and for the remote management of the device as per the Authority's policies.

j) Wireless LAN security

I. Limiting coverage of access points:
II. The Authority must evaluate physical perimeter to define positioning of wireless device thereby limiting radio transmission and coverage, inside the physical premises or intended coverage area.
III. To ensure that signal leaking out into insecure areas is minimized by setting

appropriate power levels and the directions of the antennas.

IV. Wireless encryption: The Authority must ensure that communication between user system and wireless Access Point (AP) is secured using highest graded encryption (WPA-2 or higher) for data confidentiality and integrity.

V. Under no circumstances, to open APs be deployed in the network.

VI. To ensure that there is a segmentation of Wi-Fi users and/or devices on the basis of SSID.

VII. To ensure that customized access policies are applied per SSID as per the requirements.

VIII. To ensure to change default configuration & credentials of Wireless access point

k) Using secure protocols:

I. The Authority to ensure that all available measures are applied on Access Points (APs) or WLAN switches to secure them from unauthorized access. Do not use plaintext protocols such as SNMP, Telnet or HTTP for access management services. Restrict systems from which management access is permitted.

II. To disable remote management (Telnet, SSH, HTTPS/HTTP) from WAN/internet.

l) Wireless security gateway:

I. The Authority take place firewalls or application proxies between client and server subnets and before network.

II. Visitor access to WLAN: If the Authority sets up external WLANs primarily to provide Internet access to visitors, such WLANs to be designed so that their traffic does not traverse the organisation's internal trusted networks. Configure a guest WLAN with a "separate" SSID and limit guest access to Internet only. Ensure that guest accounts require login (guest authentication).

III. Prevent simultaneous connections: The Authority must implement appropriate technical security controls to separate Wi-Fi network and wired network. Devices used for connecting the Wi-Fi network do not be allowed to connect simultaneously to the wired network to protect against bridging of networks.

IV. Enable firewall, MAC filtering, RADIUS and MFA etc.

V. To Set default DNS pointing to organisation's DNS, disable all DNS requests for public DNS servers.

VI. To ensure that there are tools in the WLAN platform to identify rogue Access Point or those potentially spoofing corporate SSIDs.

VII. It is recommended to use 802.1x for authentication in the Wi-Fi.

VIII. The Authority should watch out for unauthorized mobile / smart watch with networking capabilities being connected to the USB ports of the compute devices. This allows bridging of networks and will pave a way for attacker to reach the Internet without the security restrictions.

m) Physical isolation

I. All the terminals or ICT devices dealing with sensitive/classified information should not have any wireless equipment including Internet and Bluetooth.

II. Disable SSID broadcasting to prevent the access points from broadcasting the SSID.

III. Allow only authorized users with preconfigured SSID to access the Wireless network.

IV. Disable DHCP and assign static IP addresses to all wireless users.

n) Disabling unused ports

I. The Authority must identify ports, protocols and services required to carry out daily operations and block all others, including all non-IP based and unencrypted protocols, by establishing policies in routers and wireless access points.

o) Personal devices usage policy:

I. Use of personal devices must be authorized by concerned Network Administrator and in accordance with cyber security policy. Security checks of the systems like open ports, installed firewall, antivirus, latest system patches must be done.

p) Restricting access to public network:

I. The Authority must disable unused network adapters in systems and restrict internet connection sharing and ad hoc network creation.

q) Network access control:

I. Verify identity of device upon request to connect to the network. Conduct health scan on the device prior granting access to the network.

r) Physical security:

I. Unauthorized access, physical damage and tampering to IT systems should be prevented by implementing physical security and continuous monitoring. Important / sensitive zones should be monitored through CCTV cameras and footage should be retained for at least 180 days.

s) Default device credentials:

I. The Authority must ensure that default credentials of network devices and information systems such as usernames, passwords, and tokens are changed prior to their deployment or first use. All devices at User level should use USER account and use of Administrator account should be restricted to Network/System Administrators only.

t) Connecting devices:

I. The Authority must identify active hosts connected to its network using tools and techniques such as IP scanners, network security scanners etc. Deploy client-side digital certificates for devices to authorize access to network or sensitive information resources.

II. Extending connectivity to third parties:

a. The Authority must restrict the use of ports, services, protocols etc. used for extending access of organisation's network to third parties.

b. The Authority must limit the access granted to third parties according to the purpose of granting such access and for the time duration specified for completion of defined tasks.

c. The Authority must ensure that network documentation provided to a third

party, such as to a commercial provider, must only contain information necessary for them to undertake their contractual services and functions. Detailed network configuration information should not be included in such documentation. Such information should be treated as Confidential and appropriate non-disclosure agreement (NDA) should be signed by the third party.

d. All traffic to and from third party network/systems must be monitored.
e. Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centers.
f. Disable the GPS, Bluetooth, NFC and other sensors on computers and mobile phones.
g. They may be enabled only when required and outside secure zones.

21. Social Media Security

a) Limit and control the use/exposure of personal information while accessing social media and networking sites.
b) Always check the authenticity of the person before accepting a request as friend/contact.
c) Use multi-factor authentication to secure social media accounts.
d) Do not click on the links or files sent by any unknown contact user.
e) Do not publish or post or share any sensitive/ confidential government documents or information on social media.
f) Do not publish or post or share any unverified information through social media.
g) Do not share the official email address on any social media platform without the consent of the appropriate authority.
h) Official social media platform accounts access should be restricted and limited to the designated officials and systems only.
i) Always use a dedicated/separate email account for operating official social media platform accounts. Always use a different set of credentials for official email account and official social media platform account. Social media platform account credentials should be in accordance with the password policy of the Authority.
j) Do NOT use personal email account for operating official social media account
k) Multi factor authentication should be enabled for all social media accounts wherever possible.
l) Content to be posted on social media handles should be approved by appropriate authority.
m) Do not use official social media platform accounts on public/ unauthorized

devices.

n) Disable Geo location (GPS) access feature for official social media platforms.

o) Ensure that social media platform software/application is updated to the latest available version and devices from which official social media accounts are operated are updated to the latest available security patches.

p) Keep eye on latest updates by social media companies regarding security and privacy settings and implement appropriately.

q) Enable role-based accounts with appropriate privilege for social media management platform and official social accounts.

r) Revoke access to official social media accounts if employee role changes or employee leaves the Authority.

s) Enable account security logs and monitor periodically to identify log-in attempts from untrusted devices or log-in attempts from geographical regions other than the usual.

t) Enable alerts for unrecognized login attempts under login & security settings of social media platform/application.

u) Exercise caution while using third party applications for managing social media platform accounts.

v) Regularly monitor email account associated with official social media accounts for any alerts received related to account activities.

22. Vulnerability And Patch Management

a) Standard operating environment:

I. The Authority must do replacement of ICT assets with newer/upgraded version keeping in view their backward and forward compatibility with existing infrastructure devices. Addition of ICT infrastructure components is to be done post compatibility / interoperability analysis.

II. The Authority must ensure standardization of operating environment like Operating systems, Servers, application platforms.

b) Threat assessment:

I. The Authority must identify the possible threat vectors, exploitation points, tools and techniques, which can compromise the security.

II. The Authority must perform vulnerability assessment to identify vulnerabilities and weaknesses in configuration devices and systems; vulnerabilities and threats associated with the use of specific ports, protocols and services and vulnerabilities introduced due to changes in ICT infrastructure.

c) Threat intelligence:

I. The Authority must establish a formal relationship with external entities such as

CERT-In, Sectoral CSIRTs[8] and other stakeholders for receiving relevant threat intelligence feeds / information about emerging threats, vulnerabilities, bugs and exploits.

II. Set up processes to examine threat intelligence and ingest the same in automated manner through standard processes.

d) Vulnerabilities knowledge management: The Authority must-

I. Ensure that ICT systems and devices are updated with the latest security patches and virus signature to reduce the chance of being affected by malicious code or vulnerabilities.

II. Perform security risk assessment regularly by using capabilities such as vulnerability scanning tools (host-based or network based) to identify patch inadequacy or potential system misconfiguration and prioritize the order of the vulnerabilities identified and remedial measures.

III. Ensure that all third-party vendors, agencies, partners with access to the organization's information implement controls and processes to counter emerging threats and address vulnerabilities.

e) Patch management:

I. The Authority must ensure that patch management is carried out at regular intervals or as soon as critical patches for ICT systems or software are available.

II. Keep operating systems, browsers and any other applications up to date and apply all security patches.

III. Enable automatic patching for all software and hardware or establish full vulnerability and patch management solutions.

IV. The Authority should conduct risk assessment activities to identify and replace any software and hardware that are not capable of automatic updates. If the Authority chooses to keep such devices, they should have a documented procedure to ensure regular manual updates.

f) Perimeter threat protection:

I. The Authority must ensure perimeter threat protection of its network infrastructure through implementation of capabilities such as a firewall, IPS etc.

g) Configuration of endpoints:

I. The Authority must block all unnecessary services and system level administrator privileges through methods such as active directory, group policies on endpoint devices and systems.

II. The Authority must ensure that each information system is protected by installation of antivirus software and application of regular updates.

[8] https://www.cert-in.org.in/CSIRT.jsp

23. Compliance Statement

a) This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

b) If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support official function, entities shall request an exception through the Chief Information Security Officer (CISO) exception process.

24. Definitions of Key Terms

Term	Definition
CISO	Chief Information Security Officer
PPI	Prepaid Payment Instruments
CERT-In	Indian Computer Emergency Response Team
OS	Operating System
PII	Personally Identifiable Information
ISO	International Organisation for Standardization
VPN	Virtual Private Network

25. Contact Information

Submit all requests for future enhancements to the policy owner at: iwainoi@nic.in

26. References

a) National Information Security Policy and Guidelines, Ministry of Home Affairs, Government of India Version 5.0

b) Guidelines on Information Security Practices for Government Entities by Cert-In

c) ISO/IEC 27001:2022 (ISO 27001) Standard

d) National Institute of Standards and Technology (NIST) - National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations