सत्यमेव जयते

Safe & Trusted Internet

Guidelines on Information Security Practices for Government Entities

Issued by

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics and Information Technology

Government of India

Table of Contents

1. Introduction and Purpose

India is fast becoming one of the world's largest connected nations - with over 80 Crore Indians (Digital Nagriks) presently connected and using the Internet and cyberspace - and with this number is expected to touch 120 Crores in the coming few years. The Digital Nagriks of the country are using the Internet for business, education, finance and various applications and services including Digital Government services. Internet provides growth and innovation and at the same time it has seen rise in cybercrimes, user harm and other challenges to online safety.

The policies of the Government are aimed at ensuring an Open, Safe & Trusted and Accountable Internet for its users. Government is fully cognizant and aware of the growing cyber security threats and attacks.

It is the Government of India's objective to ensure that Digital Nagriks experience a Safe & Trusted Internet.

Along with ubiquitous applications of Information & Communication Technologies (ICT) in almost all facets of service delivery and operations, continuously evolving cyber threats have become a concern for the Government. Cyber-attacks can come in the form of malware, ransomware, phishing, data breach etc., that adversely affect an organisation's information and systems. Cyber threats leading to cyber-attacks or incidents can compromise the confidentiality, integrity, and availability of an organisation's information and systems and can have far reaching impact on essential services and national interests.

To protect against cyber threats, it is important for government entities to implement strong cybersecurity measures and follow best practices. As ICT infrastructure of the Government entities is one of the preferred targets of the malicious actors, responsibility of implementing good cyber security practices for protecting computers, servers, applications, electronic systems, networks, and data from digital attacks, also remain with the ICT assets' owner i.e. Government entity.

"Indian Computer Emergency Response Team (CERT-In)" has been established and appointed as national agency in respect of cyber incidents and cyber security incidents in terms of the provisions of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) to perform the following functions in the area of cyber security: -

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incidents response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

The Indian Computer Emergency Response Team(CERT-In) is satisfied that for the purposes of performing the aforesaid functions, it is necessary and expedient in the interest of cybersecurity that guidelines relating to information security practices, procedures, prevention and response be issued in exercise of the powers conferred by clause (e) of sub-section (4) of section 70B of the Information Technology Act, 2000 (21 of 2000) for all the Ministries, Departments, Secretariats and Offices specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, their attached and subordinate offices, and all government institutions, public sector enterprises and other government agencies under their administrative purview (hereinafter collectively referred to as "government entities"); and it is expected that the said guidelines be carried out by all government entities by doing necessary acts and things required in this regard;

The purpose of these guidelines is to establish a prioritized baseline for cyber security measures and controls within government organisations and their associated organisations. The guideline shall assist security teams to implement baseline and essential controls and procedures to protect their Cyber infrastructure from prominent threats. These guidelines shall also act as a baseline document for administration and audit teams (internal, external/ Third-party auditors) to evaluate an organisation's security posture against cyber security baseline requirements.

These guidelines cover best practices segregated in different security domains such as Network Security, Application Security, Data Security, Auditing, Third Party Outsourcing. Due to the ever-evolving threat landscape, this document is envisaged to be an organic document and would be updated as per changing threat landscape.

2. Applicability and Scope

The purpose of these guidelines is to establish a prioritized baseline of cyber security measures and controls within Central government organisations and their associated organisations. These guidelines relating to information security practices, procedures, prevention and response are issued by the Indian Computer Emergency Response Team (CERT-In) for all Ministries, Departments, Secretariats and Offices specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, their attached and subordinate offices, and all government institutions, public sector enterprises and other government agencies under their administrative purview (hereinafter collectively referred to as "government entities").

Government of India has already put in place various mechanisms which are aimed at preventing cyber-attacks and also to guide organisations in responding to cyber-related incidents such as comprehensive Cyber Crisis Management Plan (CCMP) document and maturity ladder. Government entities need to mature from baseline guidelines mentioned in this document to cyber resilient entity with implementation of comprehensive CCMP. In addition to this, Government of India has also issued a Cyber Security Guidelines for Central Government CISOs and Government Employees (**Ref. Annexure 1**), which shall be mandatorily complied with by Government departments.

3. Policy Measures

Senior management of the organisation should implement the following measures:

3.1. Nominate a Chief Information Security Officer (CISO) for IT Security and provide the details of this CISO (Point of Contact) to CERT-In as per Cyber Security Directions of 28 April 2022.

3.2. Formulate cyber security policy and assign roles and responsibilities for Chief Information Security Officer (CISO) and a dedicated cyber security functional team. Detailed Roles & Responsibilities of CISO are published on website of Meity at following URL:

https://www.meity.gov.in/content/key-roles-and-responsibilities-chief-information-security-officers-cisos

3.3. CISO should have a dedicated cybersecurity team, separate from IT operations and infrastructure team. The team would be responsible for:

i. monitoring network's security and responding to security alerts
ii. conducting incident response
iii. formulating, enforcing and reviewing IT security policies
iv. conducting cybersecurity awareness drills and campaigns within the organisation
v. liaising with CERT-In and other government and industry cybersecurity organisations

3.4. Organisations should conduct an internal and external audit of the entire ICT infrastructure and deploy appropriate security controls based on the audit outcome. Internal information security audit to be conducted at least once in 6 months. 3rd Party Security audits must be conducted at least once a year. Services of CERT-In empanelled auditors may be utilized for the purpose of external audits. List of empanelled auditors with details such as skills, competence, experience in audits, manpower, tools used etc., is available on website "https://www.cert-in.org.in".

3.5. Formulate security policies and procedures for building cyber resiliency. Prepare, test and implement Business Continuity Plan (BCP) and Disaster Recovery (DR) plan.

3.6. Maintain inventory of 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.

3.7. Prepare an organisation-wide Cyber Security Awareness Program and regularly educate end users about security practices to deal with cyber threats like phishing campaigns, social engineering and roles and responsibilities of users.

3.8. Maintain situational awareness of latest cyber security threats by following website of CERT-In and alerts and advisories thereof. Follow measures suggested by CERT-In for cyber hygiene including prevention of cyber threats. Alerts and advisories are available on the following websites:

Indian Computer Emergency Response Team (CERT-In)	https://सर्ट-इन.भारत https://www.cert-in.org.in
Cyber Swachhta Kendra (CSK):	https://www.सीएसके.सरकार.भारत https://www.csk.gov.in

4. Network and infrastructure security

4.1. Key principles and measures

4.1.1. Define an appropriate network architecture including the network perimeter, any internal networks, and links with other organisations such as service providers or partners. 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 which is required to support the business is being exchanged. Control and manage all inbound and outbound network connections and deploy technical controls to scan for malicious content.

4.1.2. Network should be properly segmented, with separate VLANs for different functional requirements. Communication between different VLANs should be denied by default and only be allowed specifically on basis of need with necessary restrictions on ports / applications / hosts.

4.1.3. Use firewalls to create a buffer zone between the Internet (and other untrusted networks) and the networks used by the business. The firewall rule set should deny traffic by default and a whitelist should be applied that only allows authorised protocols, ports and applications to exchange data across the boundary. This will reduce the exposure of systems to network based attacks. Employ effective processes for managing changes to avoid workarounds. An internal firewall for controlling connections within the LAN should also be deployed and properly maintained.

4.1.4. Network Intrusion detection / prevention and other appropriate security devices should be deployed and monitored for North-South (Internet to LAN) and East-West (Between Intranet for monitoring unauthorized lateral movements) by trained/certified personnel. Alerts generated from the devices should be thoroughly verified as most of them could be indicating an imminent attack.

4.1.5. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the mail gateway and hosts with a reputable antivirus solution.

4.1.6. Monitor/Block the communication to malicious IPs and Domains regularly shared by CERT-In and other security agencies

4.2. Identification and classification:

4.2.1. The organisation must ensure that classified information is mapped with the infrastructure elements through which it will be transmitted, processed or stored. All infrastructure devices should be categorized as per classification of information that they manage.

4.2.2. Each network should have a security classification so as to prevent any information breach. No data should be allowed to move between two different classification networks.

4.3. Network diagram:

4.3.1. The organisation shall develop an accurate mapping of the core components, connections and information of the network to build organisation'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 white listed systems/IP addresses, open/entry ports, subnet mask, administrative interface, zones, access control lists, network name etc. Organisation must store this document in confidential manner as this contains sensitive information.

4.3.2. All amendments to network diagram should be documented with reason of change, nature of change and person responsible. All previous configuration diagrams must also be retained for reference. Proper change management procedure shall be followed with documentation.

4.4. Network configuration:

4.4.1. Network administration team of the organisation shall periodically review network configuration at least every 6 months or as and when new access controls are introduced in the network.

4.4.2. Configuration of networks shall be according to security policy of organisation.

4.5. Network security measures

4.5.1. For perimeter defence, organisation shall 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.

4.5.2. Deploy NextGen firewall (2 units) in High availability (HA) mode as a perimeter security device (external firewall). Another set of firewall from different OEM shall be used as internal firewall (in HA mode) for internal segmentation of network.

4.5.3. Organisation shall deploy their own local/internal DNS servers (primary & secondary) for all segments. This will help to monitor malicious DNS requests and blocking them by resolving to null (0.0.0.0) / localhost. Set default DNS pointing to organisation's DNS or DNS of National Informatics Centre (NIC) (IPv4 1.10.10.10 / IPv6 2409::1). In addition, organisation shall block access to all DNS requests for outside/public DNS services.

4.5.4. Organisation shall deploy proxy servers and allow access for internet for clients through proxy server only.

4.5.5. All devices placed within the network should have logging enabled. Logs of perimeter security devices and end points should be integrated with Security Information and Event Management (SIEM) and alerts from SIEM should be monitored and acted upon. Logs of perimeter security devices and SIEM should be stored for a rolling period of 180 days.

4.5.6. For protection against the distributed denial of service (DDoS) and denial of service (DoS) attacks, appropriate protection must be incorporated through DDoS mitigation devices and DDoS mitigation service through service providers. Clearly define the SLAs with service providers while planning for DDoS mitigation services.

4.5.7. Using secure protocols: Disable all non-IP-based access protocols such as TELNET, and use secure protocols such as SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router/switch/server.

4.5.8. Ensure that Virtual Private Network (VPN) is used for accessing Network Resources from Remote location. Enable Multi Factor Authentication (MFA) for VPN accounts. Enable VPN account logging and integrate VPN logs with Security Information and Event Management (SIEM) system.

4.5.9. Implement Media Access Control (MAC) address binding for all systems/IT devices. Disable DHCP and set IP configurations manually.

4.5.10. Change all default credentials & configurations at the time of first installation.

4.5.11. Ensure to block access to any remote desktop applications such as Anydesk, Teamviewer, Ammyy admin etc.

4.5.12. Organisation shall always deploy network infrastructure device in high-availability mode.

4.5.13. The organisation should conduct cyber security audit including vulnerability assessment to test network security measures.

4.5.14. The organisation should ensure that the devices procured are IPv6 compatible and enforce policy for IPv6 traffic.

4.6. Network Segmentation

4.6.1. Ensure segmentation of the network to create security zones for isolating sensitive traffic and secure critical IT systems.

4.6.2. Limit and segment user rights for access by implementing proper Access Control Lists (ACLs) in the network. Access control lists should be configured on devices such as routers and/or switches.

4.6.3. Network firewall should be used to restrict traffic movement outside the network segment. Only selected ports and protocols should be allowed for communication with selected IPs, as per the requirements of the official work.

4.6.4. Critical servers should be either made stand-alone or member of a dedicated secure zone and the servers need not communicate amongst themselves unless they are part of same application with dedicated ports and authenticated applications.

4.6.5. Applications / servers and systems in the Intranet should be separated from Internet facing networks/ systems.

4.7. Security zones:

4.7.1. Virtual LANs should be used by an organisation to logically separate zones. Communication between different VLANs should be disabled by default and only be allowed on need basis with per port / application basis.

4.8. Network traffic segregation

Organisation should enforce rule set to minimize exposure of information by:

4.8.1. Implementation of traffic flow filters, VLANs, network and host-based firewalls.

4.8.2. Implementation of application-level filtering, proxies, content-based filtering.

4.8.3. Wherever possible physical segregation must be preferred over logical segregation

4.9. Local Area Network (LAN) security

4.9.1. Traffic monitoring: Deploy traffic management capabilities which continuously monitors and controls IP network

4.9.2. 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. Preferably, wired 802.1x based network admission control, where only the systems / end points that meets the organisational security posture should be allowed in the network. Rest of the devices can be put in a quarantine VLAN till the remediation of patch / infection is cleared for the security posture. The quarantine VLAN can have patch servers and remediation servers such as Antivirus servers / platforms. Any new devices that are connected without posture checking can go to Guest/ Internet only / Quarantine VLANs.

4.9.3. Configure host firewall in all systems to restrict lateral traffic movement within the same network segments. The preferred approach should be such that the incoming and outgoing connections should be restricted only to needed services and its applications with default deny for rest of the traffic.

4.9.4. Ensure that remote-desktop software (like Anydesk, teamviewer, Ammyy Admin etc.) are not allowed in network.

4.9.5. 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.

4.9.6. Enable manual configuration of systems in network, disable DHCP, if not required. Rogue DHCP servers have to be detected and isolated immediately.

4.9.7. Bring Your Own Device (BYOD) should be restricted and no unknown devices should be allowed in the network without authorisation by the Network Administrator. For business purposes, Mobile Device Management (MDM) solution that provides security functions should be considered for security, prevention of data theft and for the remote management of the device as per the organisational policies.

4.10. Wireless LAN security

4.10.1. Limiting coverage of access points: Organisation must evaluate physical perimeter to define positioning of wireless device thereby limiting radio transmission and coverage, inside the physical premises or intended coverage area. Ensure that signal leaking out into insecure areas is minimized by setting appropriate power levels and the directions of the antennas.

4.10.2. Wireless encryption: Organisation 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.

4.10.3. Under no circumstances, should open APs be deployed in the network.

4.10.4. Ensure that there is a segmentation of Wi-Fi users and/or devices on the basis of SSID.

4.10.5. Ensure that customized access policies are applied per SSID as per the requirements.

4.10.6. Ensure to change default configuration & credentials of Wireless access point.

4.10.7. Using secure protocols: Organisation must 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.

4.10.8. Disable remote management (Telnet, SSH, HTTPS/HTTP) from WAN/internet.

4.10.9. Wireless security gateway: Organisation should place firewalls or application proxies between client and server subnets and before network.

4.10.10. Visitor access to WLAN: If the organisation sets up external WLANs primarily to provide Internet access to visitors, such WLANs should 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).

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

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

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

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

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

4.10.16. Wireless LAN should not be permitted in the sensitive organisations. Organisations 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.

4.11. Physical isolation

The Organisation should ensure that there is proper physical isolation of sensitive and wireless networks.

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

4.11.2. Disable SSID broadcasting to prevent the access points from broadcasting the SSID. Allow only authorized users with preconfigured SSID to access the Wireless network.

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

4.12. Disabling unused ports:

The organisation 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

4.13. Personal devices usage policy:

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

4.14. Restricting access to public network:

The organisation must disable unused network adapters in systems and restrict internet connection sharing and adhoc network creation.

4.15. Network access control:

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

4.16. Physical security:

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

4.17. Default device credentials:

The organisation 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.

4.18. Connecting devices:

The organisation 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 information resources

4.19. Extending connectivity to third parties

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

4.19.2. The organisation 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

4.19.3. The organisation 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.

4.19.4. All traffic to and from third party network/systems must be monitored

4.19.5. Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.

4.19.6. Disable the GPS, Bluetooth, NFC and other sensors on computers and mobile phones. They maybe enabled only when required and outside secure zones.

5. Identity and access management

All employees must be allotted a unique ID. User identity scheme must be defined and identity provisioning process should follow a workflow with proper checks and must be reviewed at least every six months and report in this regard to be submitted to the head of the department/organisation.

User access deactivation request must be submitted immediately upon termination of employment, instances of non-compliance, suspicious activity and in case required as part of disciplinary action etc.

5.1. Need to know access:

Access privileges to users must be based on operational role and requirements. Access security matrix must be prepared which contains the access rights mapped to different roles. This must be done to achieve the objective of role based access control (RBAC). Access to system must be granted based on access security matrix.

5.2. Review of user privileges:

All user accounts must be reviewed periodically by concerned authority by examining system activity logs, log-in attempts to access non-authorized resources, abuse of system privileges, frequent deletion of data by user etc.

5.3. Authentication mechanism for access:

The organisation must implement multi- factor authentication as much as possible.

5.4. Single Sign On (SSO) –

For Government/PSU/Statutory/Autonomous body users, ensure that Websites and Applications are integrated with any of three National SSO i.e. e-Pramaan by C-DAC Mumbai; Parichay/Janparichay by NIC; DigiLocker by NeGD: for login purpose.

5.5. Acceptable usage of Information assets & systems:

5.5.1. The organisation must ensure that users are made aware of their responsibility to use their account privileges only for mandated use.

5.5.2. The organisation must clearly state that it provides computer devices, networks, and other electronic information systems to meet its mission, goals, and initiatives and users must manage them responsibly to maintain the confidentiality, integrity, and availability of the organisation's information.

5.5.3. Acceptable Usage Policy needs to be elaborated across areas such as email, internet, desktops, information, clear desk policy, password policy etc.

5.5.4. The organisation must obtain user sign-off on Acceptable Usage Policy.

5.6. Password policy:

5.6.1. All active sessions of a user must be terminated post 15 minutes of inactivity and must be activated only post re-authentication by specified mechanism such as re-entering password etc.

5.6.2. Passwords must be encrypted when transmitting over an un-trusted communication network

5.6.3. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.

5.6.4. Change passwords at least once in 120 days.

5.6.5. Use and implement Multi Factor Authentication (MFA).

5.7. Default device credentials:

The organisation must ensure that default login credentials of devices such as routers, firewall, storage equipment etc., are changed prior to the deployment of such devices in the operational environment

5.8. Remote access:

Implement appropriate security technologies to protect information or information systems being accessed via remote access, such as using VPN based on SSL/TLS, SSTP or IPSec with MFA.

5.8.1. Avoid using Open Proxies, Tor, Free 3rd party VPN services for remote access.

5.8.2. Mandate Multi-Factor Authentication for Remote access.

5.8.3. Implement Geo-fencing for restricting remote access from unauthorized geo-locations.

5.9. Segregation of duties:

5.9.1. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

5.9.2. Documents duties of staff and privileges of different roles.

5.9.3. Create different administrator accounts for different roles assigning only the needed security attributes and privileges which are just needed for those roles alone.

6. Application security

6.1. Application security

6.1.1. The organisation 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.

6.1.2. Ensure privacy protection of citizen data at each stage of application life cycle.

6.1.3. The organisation must maintain an updated document 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.

6.1.4. 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.

6.1.5. The organisation must identify ports, protocols and least privileged services required to carry out daily operations of applications / platforms and restrict or block all others.

6.1.6. Organisation should ensure that applications validate the data on the server-side.

6.1.7. Ensure that all Websites and Applications are “https” enabled with a valid SSL/TLS Certificate.

6.1.8. Ensure applications execute proper error handling and should not provide detailed system information, deny service, impair security mechanisms, or crash the system.

6.1.9. Application security testing, vulnerability assessment and penetration testing, should be performed at a frequency determined by sensitivity of the information handled by applications (at least once in a year or whenever there is change in application).

6.1.10. Implement measures for securing Application Program Interfaces (APIs). Include API security in Vulnerability Assessment and Penetration Testing and mitigate vulnerabilities in APIs.

6.1.11. Log monitoring on a continuous basis to be carried out with the ability to alert the operations team when a security anomaly is suspected

6.1.12. Implement Integrity checks and disallow the binary from executing that does not confirm to the application / system security

6.2. Mobile Application Security:

6.2.1. Organisations should ensure that their mobile applications address the Open Web Application Security Project (OWASP) Mobile Top 10 vulnerabilities.

6.2.2. The mobile application must implement SSL Pinning to prevent man-in-the-middle attacks.

6.2.3. No secret keys used by the application should be stored unencrypted in the application storage.

6.2.4. User data should not be stored in unencrypted/plain-text form on the device.

6.2.5. 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.

6.2.6. Only permissions required for essential functionality of the application should be sought from the user.

6.2.7. Sensitive data should be shared over secure SSL/TLS connection only.

7. Data security

7.1. Identify and classify sensitive/personal data and apply measures for encrypting such data in transit and at rest. Deploy data loss prevention (DLP) solutions / processes.

7.2. Review and change any default/ weak/ misconfigured settings with appropriate authentication & authorization controls for all database applications

7.3. Deploy detection and alerting tools and create process to prevent, contain and respond to a data breach/ data leak.

7.4. Evolve and implement a Data Backup policy. All the business-critical data should be backed up regularly to prevent data loss and to ensure faster recovery in case of an incident.

7.5. 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.

7.6. Develop and maintain policies enforcing strong passwords (password management) and the use of multi-factor authentication (MFA).

7.7. Conduct third party risk assessment on regular basis and monitor for any data breach /leak cases from supply chains to take necessary protective & remedial measures.

7.8. Implement Micro-segmentation for controlled granular access to database applications

7.9. Personal external storage media devices should not be allowed to be connected with official information systems or assets and vice-versa.

7.10. Data Backup policy:

7.10.1. Back-up procedures should be documented, scheduled and monitored.

7.10.2. 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:

- Data files
- Utilities programmes
- Databases
- Operating system software
- Applications system software
- Encryption keys
- Pre-printed forms
- Device configurations

7.10.3. 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.

7.10.4. Backups of the system, application and data should be performed on a regular basis as per the DR and BCP policy of the organisations. Backups should also be made for application under development and data conversion efforts.

7.10.5. Data backup is required for all systems which are deemed critical for the organisation including personal computers, servers and distributed systems, databases, network, security equipment.

7.10.6. 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.

7.10.7. 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 organisation.

7.10.8. 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.

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

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

8. Third party access and Outsourcing

8.1. Organisation should ensure that third party access to information should be restricted and should only be shared after signing Non-Disclosure-Agreement.

8.2. 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.

8.3. 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.

8.4. Information security audit report of the vendor to be made available to Procuring entity on periodic basis or when required.

8.5. 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. Vendor is also responsible for informing any identified vulnerabilities in the system to the organisation within reasonable time period.

8.6. 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.

8.7. External party personnel should comply with the information security policies, processes and procedures of the organisation.

8.8. 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.

9. Secure Cloud Services

9.1. 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

9.2. Check public accessibility of all cloud instances in use. Make sure that no server/storage is inadvertently leaking data due to inappropriate configurations.

9.3. Implement least privilege principle for access control with granular permission to cloud resources

9.4. Enable cloud native security controls along with logging for critical cloud resources and ensure continuous monitoring

9.5. 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 an organisation.

9.6. Detailed cloud security best practices are published on website of MeitY. at following URL:

https://www.meity.gov.in/writereaddata/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

10. Hardening Procedures

10.1. Desktop

10.1.1. 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.

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

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

10.1.4. 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.

10.1.5. 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.

10.1.6. Do not allow peer-to-peer file sharing application to be installed on office systems or to communicate with outside internet.

10.1.7. 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.

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

10.1.9. Enable system level firewall.

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

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

10.1.12. Configure organisation DNS of all office systems

10.1.13. 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

10.1.14. Disable Remote Desktop (RDP), SMB, PowerShell and any other services, if not required by organisation

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

10.1.16. Offline backups with encryption for critical systems should be maintained. Online backup systems should be properly hardened and access to its network should be strictly restricted. Sensitive information or data should be stored in encrypted format.

10.1.17. An inventory of all devices and systems connected to the network should be maintained with a focus on keeping track of versions of operating system and other software running on these devices and systems.

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

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

10.1.20. Endpoint security solutions should be deployed for continuously monitoring end user devices to detect and respond to cyber threats like ransomware, malware and unauthorized accesses. 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.

Security measures for Printers, commonly used & shared devices in network

10.1.21. Disable default credentials on printers

10.1.22. 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

10.1.23. Restrict internet access for all printers, cloud-printing etc., enable Stricter User Access Controls

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

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

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

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

10.1.28. 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.

10.2. Email server

10.2.1. Deploy a dedicated mail server.

10.2.2. Encryption: Make sure to use secure connections.

10.2.3. Implement Sender Policy Framework (SPF), Domain-Based Message Authentication Reporting & Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for email security

10.2.4. To avoid DoS attacks, limit the number of connection and authentication errors that system will accept.

10.2.5. Remove unneeded server functionality by disabling any unnecessary default settings.

10.2.6. Keep total, maximum connections to SMTP server limited.

10.2.7. Access Control: To protect server from unauthorized access, implement authentication and access control. Make sure access to servers is on a need-to-have basis and is shared with as few people as possible.

10.2.8. Ensure email server software is updated with latest patches.

10.2.9. Enable logs of web interfaces of email server and review the same on continuous basis to detect any anomalies and devise mitigation measures for any attacks detected.

10.3. Database server

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

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

10.3.3. 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.

10.3.4. Limit user privileges and access.

10.3.5. Restrict administrative privileges.

10.3.6. Maintain regular software updates for the database and DBMS

10.3.7. 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.

10.3.8. Lock database accounts with suspicious login activity

10.3.9. Disable unnecessary services

10.3.10. Encrypt sensitive database information.

10.3.11. 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.

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

10.4. Software security

10.4.1. Use authorized and licensed software only.

10.4.2. Allow installation of software only from trusted application repositories.

10.4.3. Automate patching of standard and third-party applications.

10.4.4. Use Software-based data encryption

10.4.5. Uninstall software that is no longer in use.

11. User awareness and Training

11.1. Awareness training program

11.1.1. The program should aim to increase user understanding and sensitivity to cyber threats, vulnerabilities.

11.1.2. The awareness program should focus on the need to protect organisation's information.

11.1.3. Awareness training must be provided to new joiners as part of Induction training. Further, it should be provided to all employees every 6 months. Attendance to such training should be recorded in the Annual Performance reports.

11.1.4. 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.

11.2. Role based Training

11.2.1. The organisation must ensure that role-based training is provided to all personnel within the organisation to familiarize them with their roles and responsibilities in order to support security requirements.

11.2.2. The organisation must ensure that information security awareness and training include the following:

- Purpose of the training or awareness program
- Reporting any suspected compromises or anomalies
- Escalation matrix for reporting security incidents
- Fair usage policy for organisations assets and systems
- Best practices for the security of accounts
- Authorization requirements for applications, databases and data
- Classifying, marking, controlling, storing and sanitizing media
- Best practices and regulations governing the secure operation and authorized use of systems

12. Social media security

12.1. Official social media platform accounts access should be restricted and limited to the designated officials and systems only.

12.2. 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 organisation.

12.3. Do NOT use personal email account for operating official social media account.

12.4. Multi factor authentication should be enabled for all social media accounts wherever possible.

12.5. Content to be posted on social media handles should be approved by appropriate authority within the organisation.

12.6. Official Social media platform accounts should be operated by designated officials only and on trusted devices only. Ensure to log out from official social media platform account immediately after usage.

12.7. Do not use official social media platform accounts on public devices / unauthorized devices.

12.8. Disable Geolocation (GPS) access feature for official social media platforms.

12.9. 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.

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

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

12.12. Revoke access to official social media accounts if employee role changes or employee leaves the organisation.

12.13. 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.

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

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

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

13. Vulnerability and patch management

13.1. Standard operating environment:

13.1.1. The organisation 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.

13.1.2. The organisation must ensure standardization of operating environment like Operating systems, Servers, application platforms etc. across the organisation.

13.2. Threat assessment:

13.2.1. The organisation must identify the possible threat vectors, exploitation points, tools and techniques, which can compromise the security of the organisation.

13.2.2. The organisation 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

13.3. Threat intelligence:

13.3.1. The organisation must establish a formal relationship with external entities such as CERT-In, Sectoral CSIRTs and other stakeholders for receiving relevant threat intelligence feeds / information about emerging threats, vulnerabilities, bugs and exploits.

13.3.2. Set up processes to examine threat intelligence and ingest the same in automated manner through standard processes such as STIX / TAXII implementation.

13.4. Vulnerabilities knowledge management:

13.4.1. The organisation must 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.

13.4.2. The organisation must 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.

13.4.3. The organisation must ensure that all third-party vendors, agencies, partners with access to the organisation's information implement controls and processes to counter emerging threats and address vulnerabilities.

13.5. Patch management:

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

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

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

13.5.4. Organisations should conduct risk assessment activities to identify and replace any software and hardware that are not capable of automatic updates. If the organisation chooses to keep such devices, they should have a business process to ensure regular manual updates.

13.6. Perimeter threat protection:

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

13.7. Configuration of endpoints:

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

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

14. Security monitoring and incident management

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

14.1. Preparedness is the key for effectively handling/responding to a cyber security incident. Organisation should create a dedicated cyber security team under the leadership of dedicated CISO. This cyber security team shall directly report to the senior management of the organisation. The organisation should build appropriate cyber security capabilities for incident management.

There are four key phases to Incident Response:

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

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

- **Containment and eradication:** The purpose of this phase is to limit the effects of an incident for further damages. 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.

- **Recovery & lessons learned:** Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the 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 in particular.

14.2. The organisation must ensure that apart from addressing an incident, the organisation shall mandatorily 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.

14.3. 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)

14.4. 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.

14.5. While analysing the incidents such as Ransomware, advanced persistent threat (APT) incidents, identify and document the Tactics Techniques and Procedures (TTPs) of the attackers as per MITRE ATT&CK framework. The Adversarial Tactics, Techniques, and Common Knowledge or MITRE ATT&CK is a guideline for classifying and describing cyber attacks and intrusions. Devise defences to mitigate attack techniques and test the same through red teaming and blue teaming exercises.

14.6. Consider Defence-in-Depth (D-i-D) approach along with zero trust approach wherever applicable as it is important for an organisation to implement series of security mechanisms and controls throughout a computer network to protect the confidentiality, integrity, and availability of the network and the data within.

Zero Trust is a shift in cybersecurity approach for the protection of data and services and assets of an enterprise (devices, applications, IT infrastructure devices, virtual & cloud infra components etc.). Zero Trust considers that there is no traditional network edge i.e. networks may be local, in cloud, or a combination or hybrid with IT resources anywhere & everywhere as well as employee/users at any location. Zero trust involve minimizing access to the resources (data and compute resources and applications/services) to only those end users/systems and assets identified as needing access as well as continually authenticating and authorizing the identity and security posture of each access request. Zero Trust approach includes eight pillars i.e. User, Device, Network, Infrastructure, Application, Data, Visibility and Analytics, and Orchestration and Automation.

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 least privileges needed to perform the action in the request.

A Zero-Trust Architecture (ZTA) is an enterprise cybersecurity architecture that is based on zero trust principles. ZTA requires all users and devices to be authenticated and authorized before they are granted access to resources. This helps to protect against a variety of cyberattacks limiting internal lateral movement. ZTA can be implemented in a variety of ways, but it typically involves the use of a combination of technologies, such as identity and access management (IAM), micro-segmentation, cloud security, continuous monitoring, and advanced authentication mechanisms.

14.7. Cyber security team of an organisation 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.

14.8. Cyber security team shall maintain an updated list of point of contact (i.e. key persons within organisation and authorities/entities) to be contacted at the time of incident response.

14.9. A dedicated cyber security team of the organisation shall actively monitor logs received at centralized location (i.e. Syslog server, SIEM etc.) from various security mechanisms & control devices implemented throughout the network of an organisation. Appropriate alerting mechanisms may be configured in system for immediate alerting.

14.10. 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.

15. Security auditing guidelines

15.1. Audit management function

A dedicated management function must be formulated by organisation to conduct security audits and associated tasks such as the following:

15.1.1. Compiling audit requirements

15.1.2. Defining audit types

15.1.3. Identifying audit engagements

15.1.4. Planning and arranging audits

15.1.5. Overseeing audit execution

15.1.6. Managing engagement performance

15.1.7. Actions on audit results

15.1.8. Follow-up audits

15.1.9. Reporting to the management

15.2. Risk Assessment and security auditing requirements:

15.2.1. The organisation must hold meetings with all stakeholders and heads of the department to chalk out the requirements for security audits such as the following:

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

15.3. Periodicity and nature of audits

15.3.1. The scope of audit should be comprehensive so as to cover entire ICT infrastructure of the organisation

15.3.2. Internal information security audit to be performed at least once in 6 months.

15.3.3. 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.

15.3.4. Security audit should be performed prior to and after implementation or installation or major enhancements in the organisation

15.3.5. Follow-up audits should be conducted to ensure compliance and closure of vulnerabilities

15.4. 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 organisation for remediation. The results of all security audits must be shared with the senior management.

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/guideline_auditee.pdf

ii. https://www.cert-in.org.in/PDF/Auditor_Guidelines.pdf

iii. https://www.cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf

****

Annexure 1:

Guidelines for Central Government CISOs and Employees

Issued by National Informatics Centre

TABLE OF CONTENTS

Appendix 1 – Security Compliance Checklist

1. LOCAL AREA NETWORK SECURITY COMPLIANCE CHECKLIST
2. WIRELESS LAN SECURITY COMPLIANCE CHECKLIST
3. DESKTOP/LAPTOP/PRINTER SECURITY COMPLIANCE CHECKLIST
4. LOGGING COMPLIANCE CHECKLIST
5. SERVER SECURITY COMPLIANCE CHECK LIST

Appendix 2 – NETWORK ARCHITECTURE

INTRODUCTION

Information Communication Technology (ICT) has become ubiquitous amongst government ministries and departments across the country. The adoption and use of ICT has increased the attack surface and threat perception to government, due to lack of harmonisation, standardisation and proper cyber security practices followed on the ground.

These guidelines for CISO have been compiled by National Informatics centre with the objective to ensure security framework in the Government of India (GoI) Ministries/Departments. CISO is also required to sensitize the government employees, contractual/outsourced manpower and build awareness from a cyber security perspective as per the Cyber security guidelines for Government Employees.

The ownership of Compliance of this guideline rests with the CISO of each Ministry/Department.

This Guideline has been divided into 2 parts as given below:

1.	Guidelines for CISOs of Central government Ministries/ Departments	Part-1	Part-1 of this guideline is for adherence of CISOs and DCISOs.
2.	Cyber security Guidelines for Government Employees	Part-2	Part-2 of this guideline is for adherence by all government employees, including outsourced/contractual/temporary employees who work for government.

S. No	**Instructions to CISO**
1.	The contact details of CISO and Deputy CISO should be shared with all employees.
2.	Compliance matrix enclosed as **Appendix 1** to be sent to **security-compliance@nic.in** latest by last Friday of every quarter. This process will be made online in due course.
3.	CISO and Deputy CISO will only use the designation-based email addresses for communication. Process of handing over of E-mail addresses and updating of corresponding mobile number of successors to be ensured by CISO and Deputy CISO respectively.
4.	CCMP plan of the Ministry/Department to be prepared and shared with CERT-In. CISO has to ensure that CCMP is implemented for the Ministry/Department.
5.	**Appendix 2** provides basic Network Architecture. It may be referred to review the existing network or while planning a network.

Part- 1

Guidelines

for

Chief Information Security Officers (CISOs)

of

Central Government Ministries/Departments

1. SCOPE

The following guideline issued by National Informatics centre on Secure Local Area Network, Secure Wireless LAN, Desktop/Laptop Security and Server Security, shall be adhered to by the respective IT/Network teams of each Ministry/Department. The CISO of the Ministry/Department shall ensure the compliance of these guidelines.

2. SECURE LOCAL AREA NETWORK

2.1. Ensure that timely action is taken on the alerts and advisories issued by CERT-In and NIC-CERT.

2.2. All ICT devices should be connected via the Internet gateway of NIC's network (i.e. NICNET) and any other direct internet connection i.e., broadband, 3G/4G/5G etc., should be withdrawn with immediate effect. No hotspots to be used in the network

2.3. Ensure that an inventory of authorized hardware and software in the network is maintained.

2.4. Ensure that default credentials of network devices are changed.

2.5. Media Access Control (MAC) address binding or IEEE 802.1x is mandatory for all systems/IT devices connected in the Ministries/Department.

2.6. Unmanaged network devices should be replaced with managed devices on an immediate basis.

2.7. Ensure that organisation's or NIC DNS (IPv4: 1.10.10.10 / IPv6: 2409::1) server is configured for DNS.

2.8. Ensure that DNS queries for public DNS servers are not allowed in the network.

2.9. Ensure that NIC NTP (samay1.nic.in, samay2.nic.in) server is configured as NTP in the network.

2.10. Configure host firewall in all systems to restrict lateral traffic movement within the same network segments.

2.11. Internet connectivity to be withdrawn and Only NICNET connectivity to be provided to users who do not adhere to the guidelines mentioned under the head "*desktop/laptop and printer security*". Internet connectivity is to be restored with the approval of CISO of the ministry.

2.12. Network firewall shall be used to restrict traffic movement outside the network segment. Only selected ports and protocols shall be allowed for communication with selected IPs, as per the requirements of the official work.

2.13. Systems and equipment which are obsolete/unsupported/unpatched operating systems, to be removed from the network.

2.14. Ensure that Kavach Multi-Factor Authentication is configured on all the NIC Email Accounts in the Ministry.

2.15. It is recommended to have mechanism to identify unauthorized device and unauthorized software usage in the Network.

2.16. Implementation of Network Access control (NAC) is recommended to restrict the network access of the noncompliant devices.
2.17. Deployment of UEM (Unified Endpoint Management) for centralized endpoint management, updating and patching of operating system, antivirus and other applications is recommended.
2.18. Deployment of tools like DLP (Data Loss Prevention), NBAD (Network Behaviour Anomaly detection) are recommended.
2.19. It is recommended to deploy Unified Threat Management (UTM) device for policy-based access control of internet traffic.
2.20. Ensure that remote-desktop software (like Anydesk, teamviewer etc.) are not allowed in network
2.21. Ensure that RDP (Remote desktop) is restricted, if not required
2.22. Ensure that manual configuration of systems in network is done and DHCP is disabled, if not required.
2.23. Ensure that Virtual Private Network (VPN) is used for accessing Network Resources from Remote location.
2.24. Ensure that segmentation of LAN is done to ensure separation of zones like division-wise LAN segmentation.
2.25. Ensure that internet access is allowed only to systems as per the directives of CISO/Deputy CISO.
2.26. It is recommended to have at least 2 WAN links of Minimum 1 Gb for redundancy.
2.27. It is recommended that the Router for termination of WAN Links has minimum 4 ports of 1Gb for dynamic failover.
2.28. Ensure that the Layer 2 switches support security features like 802.1x MAC binding, Simple Network Management Protocol (SNMPv3) and operational features like Virtual LAN(VLAN) segregation, 802.1q, Quality of Service (QoS), Dynamic Host Configuration Protocol (DHCP) etc.
2.29. Ensure that L3 switch support Access control List to control East-West and North-South traffic.

3. SECURE WIRELESS LAN

3.1. Ensure that the there is a segmentation of Wi-Fi users and/or devices on the basis of SSID.
3.2. Ensure that customized access policies are applied per SSID as per the requirements.
3.3. Ensure that there is a separate Wi-Fi for the guest user with restricted network access.
3.4. Ensure to change default configuration and credentials of Wireless access point.
3.5. Enable encryption protocol Wi-Fi Protected Access version 2 or 3(WPA2/WPA3) on wireless access point
3.6. Ensure that WAN management is disabled for the wireless access point.
3.7. Ensure that MAC filtering is enabled on the wireless network.

3.8. Ensure that organisation's or NIC DNS server (IPv4: 1.10.10.10 / IPv6: 2409::1) is configured for DNS.
3.9. Ensure that DNS queries for public DNS Servers are not allowed.
3.10. Ensure that NIC NTP server (samay1.nic.in, samay2.nic.in) is configured for NTP.
3.11. Ensure that there are tools in the WLAN platform to identify rogue Access Point or those potentially spoofing corporate SSIDs.
3.12. Ensure that signal leaking out into insecure areas is minimized by setting appropriate power levels.
3.13. It is recommended to use 802.1x for authentication in the Wi-Fi.

4. DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE

4.1. Standard User (non-administrator) account to be set for all users for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.
4.2. Ensure that Guest user is disabled on the devices.
4.3. Set BIOS Password for booting.
4.4. BIOS firmware to be updated with the latest updates/patches.
4.5. It is recommended to enable device encryption in laptop/desktop.
4.6. Ensure all user systems are installed with genuine operating system (OS)
4.7. Set OS updates to auto-update from a trusted source and ensure they are updated on all devices. Install enterprise Antivirus/ EDR client offered/recommended by Government on official desktops/laptops. Ensure that the Antivirus client is updated with the latest virus definitions, signatures and patches.
4.8. CISOs shall maintain a whitelist of authorized Applications/software's, which can be used by the employees/users. Applications/Software's which are not part of the authorized list shall not be allowed.
4.9. Ensure to allow only authorized USB storage devices. External storage devices (outside department) should NOT be allowed on the system.
4.10. Ensure Change of passwords at least once in 120 days.
4.11. Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in the system's DNS Settings for all users.
4.12. Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in all the user's system NTP Settings for time synchronization.
4.13. Ensure that Remote Desktop (RDP) is disabled, if not required.
4.14. Removal of all pirated/unsupported Operating systems and deletion of other software/applications that are not part of the white-listed software should be done immediately.
4.15. Ensure to change default credentials and services like FTP, HTTP, SSH, SMB, Telnet etc. on printers.

4.16. Restrict internet access for all printers, cloud-printing etc. and enable stricter User Access Controls.
4.17. Ensure remote administration of printer with secure connection (HTTPS) only with strong admin credentials
4.18. Ensure printer firmware are updated with latest available from OEM.
4.19. Ensure requirement of user passcodes in case of shared printers and disable feature which store print history.
4.20. Ensure that NTP is configured on printer and logs are enabled.

5. SERVER SECURITY

5.1. Ensure that the Applications/websites/services are hosted only at the designated data centres of Government or Cloud Service providers empanelled by MeitY. No application/website shall be hosted within the LAN segment of a Ministry/Department/Office.
5.2. Ensure that all applications and websites are audited by CERT-In empanelled auditing organisation prior to hosting, at-least once annually and also after any major changes.
5.3. Ensure practice of 'Implement secure by design' and 'secure coding' is made mandatory for all applications. Ensure privacy protection of citizen data.
5.4. Ensure that the access to the server is restricted and appropriate security solutions as recommended by NIC /CERT-IN are deployed. Server level firewall may be configured along with network firewall.
5.5. Ensure that servers are accessed through VPN for purpose of administration and/or configuration.
5.6. Ensure that groups and users are configured as per their role and responsibilities.
5.7. Ensure that default user accounts are disabled.
5.8. Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in the server DNS Settings.
5.9. Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in the server NTP settings for time synchronization.
5.10. Ensure that the logs of servers are reviewed on daily basis. Any suspicious activity related to user access, privilege escalation, authentications should be shared with the CISO/Dy CISO
5.11. Ensure that all server logs are retained on a separate server.
5.12. Ensure that unwanted or unused OS components, services, ports, applications are uninstalled or disabled.
5.13. It is recommended to create a staging environment for testing feature releases or testing update/patch of OS, BIOS firmware, application to ensure that the functionality of the server is not impacted by the changes/updates. Any constraint on part of applying an update/patch needs to be bought into the notice of CISO / Dy. CISO

5.14. Install enterprise Antivirus/ EDR client recommended by NIC /CERT-In on all servers.
5.15. It is recommended to have IPS (Intrusion Prevention System) for preventing signature-based attacks and DDOS (Distributed Denial of Service) mitigation tools for the Servers.
5.16. It is recommended to deploy application firewall for preventing application Layer attacks.
5.17. It is recommended to configure multiple servers to ensure availability of services and use load balancer to balance the load across the servers.
5.18. Ensure that the Antivirus client and Server are updated with the latest patches/updates.
5.19. Ensure that Websites and Applications are deployed/hosted only after a security audit clearance from an accredited CERT-In empanelled audit agency.
5.20. Ensure that audit of server/application is carried out once a year/or every time the application is upgraded/customized. The audit report and its compliance should be duly shared with the CISO/Dy CISO.
5.21. Ensure that all Websites and Applications are "https" enabled with a valid SSL/TLS Certificate.
5.22. For government users, ensure that Websites and Applications are integrated with NIC SSO (parichay.nic.in) for login purpose.
5.23. For general public, ensure that Websites and Applications have MFA/2FA enabled for login purpose.
5.24. Ensure that the websites follow 'Guidelines for Indian Government Websites' (GIGW) guidelines issued by MEITY.

6. LOGGING

6.1. Ensure that logging is enabled on all ICT systems – which includes but not limited to websites/applications, databases, operating systems, ICT devices.

6.2. The logs of ICT Systems shall be retained for minimum 180 days unless specified otherwise by the CISO.

Central Ministries and Departments shall contact NIC and onboard their ICT systems to PRATIMAAN (Security Events Management System) and IPAM (asset management). State Government Departments/Entities may contact the respective state NIC centres for on boarding their ICT systems to PRATIMAAN and IPAM.

7. COMPLIANCE

The CISOs of the respective Ministry/Department shall ensure compliance of the guidelines mentioned in the Part-I: Guidelines For Chief Information Security Officers (CISOs) of Central Government Ministries/Departments.

Part- 2

Cyber Security Guidelines

For

Government Employees

1. SCOPE AND TARGET AUDIENCE

The following guidelines issued by National Informatics centre are to be adhered to by all government employees, including outsourced/contractual/temporary employees, who work for government Ministry/Department.

2. DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE

2.1. Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.
2.2. Set BIOS Password for booting.
2.3. Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.
2.4. Set Operating System updates to auto-updated from a trusted source.
2.5. Ensure that the Antivirus clients installed on your systems are updated with the latest virus definitions, signatures and patches.
2.6. Only Applications/software's, which are part of the allowed list authorized by CISO, shall be used; any application/software which is not part of the authorized list approved by CISO, shall not be used.
2.7. Always lock/log off from the desktop when not in use.
2.8. Shutdown the desktop before leaving the office.
2.9. Keep printer's software updated with the latest updates/patches.
2.10. Setup unique pass codes for shared printers.
2.11. Internet access to the printer should not be allowed.
2.12. Printer to be configured to disallow storing of print history.
2.13. Enable Desktop Firewall for controlling information access.
2.14. Keep the GPS, Bluetooth, NFC and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.
2.15. Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.
2.16. Do not write passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on users table etc.).
2.17. Do not use any external mobile App based scanner services (ex: Cam scanner) for scanning internal government documents.
2.18. Remove pirated /unsupported Operating systems and other software/applications that are not part of the authorized list of software.

3. PASSWORD MANAGEMENT

3.1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.

3.2. Change passwords at least once in 120 days.
3.3. Use Multi-Factor Authentication, wherever available.
3.4. Don't use the same password in multiple services/websites/apps.
3.5. Don't save passwords in the browser or in any unprotected documents.
3.6. 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).
3.7. Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons

4. INTERNET BROWSING SECURITY

4.1. While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/Incognito Mode in your browser.
4.2. While accessing sites where user login is required, always type the site's domain name/URL, manually on the browser's address bar, rather than clicking on any link.
4.3. Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
4.4. Don't store any usernames and passwords on the internet browser.
4.5. Don't store any payment related information on the internet browser.
4.6. Don't use any 3rd party anonymization services (3rd party VPN, Tor, Proxies etc).
4.7. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.
4.8. Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software).
4.9. Don't use your official systems for installing or playing any Games.
4.10. Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services. Such links may lead to a phishing/malware webpage, which could compromise the device.

5. MOBILE SECURITY

5.1. Ensure that the mobile operating system is updated with the latest available updates/patches.
5.2. Don't root or jailbreak your mobile device. Rooting or Jail breaking process disables many in-built security protections and could leave your device vulnerable to security threats.
5.3. Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.
5.4. Download Apps from official app stores of Google (for android) and apple (for iOS).
5.5. Before downloading an App, check the popularity of the app and read the user reviews.

5.6. Observe caution before downloading any apps which has a bad reputation or less user base etc.
5.7. While participating in any sensitive discussions switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.
5.8. Don't accept any unknown request for Bluetooth pairing or file sharing.
5.9. Before installing an App, carefully read and understand the device permissions required by the App along with the purpose of each permission.
5.10. 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).
5.11. 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.
5.12. Use auto lock to automatically lock the phone or keypad lock protected by pass code/ security patterns to restrict access to your mobile phone.
5.13. 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.
5.14. Take regular offline backup of your phone and external/internal memory card.
5.15. Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.
5.16. 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.
5.17. Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.
5.18. Disable automatic downloads in your phone.
5.19. Always keep an updated antivirus security solution installed.

6. EMAIL SECURITY

6.1. Ensure that Kavach Multi-Factor Authentication is configured on the NIC Email Account.
6.2. Download Kavach app from valid mobile app stores only. Do not download from any website.
6.3. Do not share the email password or Kavach OTP with any unauthorized persons.
6.4. Don't use any unauthorized/external email services for official communication.
6.5. Don't click/open any link or attachment contained in mails sent by unknown sender.
6.6. Regularly review the past login activities on NIC's Email service by clicking on the "login history" tab. If any discrepancy is observed in the login history, then the same should be immediately reported to CERT-In and NIC-CERT.
6.7. Use PGP or digital certificate to encrypt e-mails that contains important information.

6.8. Observe caution with documents containing macros while downloading attachments, always select the "disable macros" option and ensure that protected mode is enabled on your office productivity applications like MS Office.

7. REMOVABLE MEDIA SECURITY

7.1. Perform a low format of the removable media before the first-time usage.
7.2. Perform a secure wipe to delete the contents of the removable media.
7.3. Scan the removable media with Antivirus software before accessing it.
7.4. Encrypt the files /folders on the removable media.
7.5. Always protect your documents with strong password.
7.6. Don't plug-in the removable media on any unauthorized devices.

8. SOCIAL MEDIA SECURITY

8.1. Limit and control the use/exposure of personal information while accessing social media and networking sites.
8.2. Always check the authenticity of the person before accepting a request as friend/contact.
8.3. Use Multi-Factor authentication to secure the social media accounts.
8.4. Do not click on the links or files sent by any unknown contact/user.
8.5. Do not publish or post or share any internal government documents or information on social media.
8.6. Do not publish or post or share any unverified information through social media.
8.7. Do not share the @gov.in/@nic.in email address on any social media platform.
8.8. It is recommended to use NIC's Sandes App instead of any 3rd party messaging app, for official communication.

9. SECURITY ADVISORY AND INCIDENT REPORTING

9.1. Adhere to the Security Advisories published by CERT-In (https://www.cert-in.org.in) and NIC-CERT (https://niccert.nic.in).
9.2. Report any cyber security incident, including suspicious mails and phishing mails to CERT-In (incident@cert-in.org.in) and NIC-CERT (incident@nic-cert.nic.in).

10. CYBER SECURITY RESOURCES

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

S. No	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in	Security Tools & Best Practices
5	https://infosecawareness.in/	Security Awareness materials
6	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips
7.	https://security.nic.in/docs/Security_Policies_for_GOI/Password%20Management%20Guidelines.pdf	NIC Password Policy
8.	https://guidelines.india.gov.in/	Guidelines for Indian Government Websites

11. COMPLIANCE

All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines mentioned in this document. Any non-compliance may be acted upon by the respective CISOs/Ministry/Department heads.

Appendix 1

Security Compliance Checklist

1. LOCAL AREA NETWORK SECURITY COMPLIANCE CHECKLIST

S.no	Guidelines	Compliance	Remarks
1	Is a Cyber Crisis Management Plan (CCMP) prepared and implemented for the Ministry/Department?	☐ Yes ☐ No	
2	Whether required process is put in place to ensure that timely action is taken on the alerts and advisories shared by CERT-In and NIC-CERT?	☐ Yes ☐ No	
3	Whether all ICT devices are connected via the internet gateway of NIC's network (i.e. NICNET) and any other direct internet connection i.e., broadband, 3G/4G/5G…etc., withdrawn from office premises?	☐ Yes ☐ No	
4	Whether inventory of authorized hardware and & software is maintained.	☐ Yes ☐ No	
5	Whether default credentials of network devices are changed.	☐ Yes ☐ No	
6	Is Media Access Control (MAC) address binding or IEEE 802.1x done for all systems/IT devices connected in the Ministries/Department?	☐ Yes ☐ No	
7	Do all Un-managed network devices replaced with managed devices?	☐ Yes ☐ No	
8	Whether organisation's or NIC DNS server is configured for DNS.	☐ Yes ☐ No	
9	Whether DNS queries for public DNS Servers is not allowed in the network.	☐ Yes ☐ No	
10	Whether host firewall is configured in all systems to restrict lateral movement within the same network segment?	☐ Yes ☐ No	
11	Whether required process is put in place to implement the policy to restrict Internet connectivity and allow only NICNET connectivity for users who do not adhere to guidelines mentioned under the head "desktop/laptop and printer security "?	☐ Yes ☐ No	
12	Is Network firewall configured for the ministry/department and network access is configured as per the requirements of the official work?	☐ Yes ☐ No	
13	Whether Systems and equipment's which are obsolete and/or using obsolete/ unpatched operating systems, are removed from the network of the Ministry/Department?	☐ Yes ☐ No	

14	Whether Kavach Multi-Factor Authentication is configured or enabled on all the NIC Email Accounts in the Ministry/Department?	☐ **Yes** ☐ **No**	
15	Whether Network Access control (NAC) is implemented in the Ministry/Department?	☐ **Yes** ☐ **No**	
16	Whether UEM (Unified Endpoint Management) is deployed for the Ministry/Department?	☐ **Yes** ☐ **No**	
17	Whether DLP (Data Loss Prevention) is deployed for the Ministry/Department?	☐ **Yes** ☐ **No**	
18	Whether NBAD (Network Behaviour Anomaly detection) is deployed for the Ministry/Department?	☐ **Yes** ☐ **No**	
19	Whether Unified Threat Management (UTM) device for policy-based access control of internet traffic is deployed?	☐ **Yes** ☐ **No**	
20	Whether list of authorized applications/software that can be installed for the system made for the Ministry/Department?	☐ **Yes** ☐ **No**	
21	Whether remote-desktop software (like Anydesk) are blocked to access Network resources from remote?	☐ **Yes** ☐ **No**	
22	Whether use of VPN is made mandatory for accessing Network Resources from Remote location?	☐ **Yes** ☐ **No**	
23	Whether segmentation of LAN is done to ensure separation of zones?	☐ **Yes** ☐ **No**	
24	Whether internet access is allowed only to systems as per the directives of CISO/Deputy CISO/	☐ **Yes** ☐ **No**	
25	Whether NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) is configured as DNS for all systems/servers in the Ministry/Department?	☐ **Yes** ☐ **No**	
26	Whether NIC's NTP Service (samay1.nic.in, samay2.nic.in) is configured as NTP for in all systems/servers in the Ministry/Department?	☐ **Yes** ☐ **No**	
27	Whether network devices like routers, switches meet specifications as per the guidelines?	☐ **Yes** ☐ **No**	

2. WIRELESS LAN SECURITY COMPLIANCE CHECKLIST

S.no	Guidelines	Compliance	Remarks
1	Whether segmentation of Wi-Fi users and/or devices on the basis of SSID is done?	☐ **Yes** ☐ **No**	
2	Whether customized access policies are applied per SSID as per the requirements?	☐ **Yes** ☐ **No**	
3	Whether default configuration and credentials of Wireless access point are changed?	☐ **Yes** ☐ **No**	
4	Whether encryption protocol and features are configured for wireless access point as per the guidelines?	☐ **Yes** ☐ **No**	
5	Whether DNS and NTP server are configured as per the guidelines?	☐ **Yes** ☐ **No**	
6	Whether there are tools in the WLAN platform to identify rogue Access Point or those potentially spoofing corporate SSIDs?	☐ **Yes** ☐ **No**	
7	Whether signal leaking out into insecure areas is minimized by setting appropriate power levels?	☐ **Yes** ☐ **No**	
8	Whether 802.1x is used for authentication in the Wi-Fi?	☐ **Yes** ☐ **No**	

3. DESKTOP/LAPTOP/PRINTER SECURITY COMPLIANCE CHECKLIST

S.no	Guidelines	Compliance	Remarks
1	Whether Standard User (non-administrator) account is set for the user for accessing the computer/laptops for regular work?	☐ Yes ☐ No	
2	Whether BIOS Password is configured for booting?	☐ Yes ☐ No	
3	Whether OS update is set to auto-update from a trusted source.	☐ Yes ☐ No	
4	Whether Government offered enterprise Antivirus/ EDR client is Installed on official desktops/laptops and configured for auto-update?	☐ Yes ☐ No	
5	Whether it has been ensured that Applications/software's used are part of authorized list?	☐ Yes ☐ No	
6	Whether it has been ensured that pirated or software that are not part of authorized list of applications/software are uninstalled?	☐ Yes ☐ No	
7	Whether security of password enforced as per the guidelines?	☐ Yes ☐ No	
8	Whether it is ensured to allow only authorized USB storage devices, external storage devices?	☐ Yes ☐ No	
9	Whether printers are configured as per the guidelines?	☐ Yes ☐ No	

4. LOGGING COMPLIANCE CHECKLIST

S.no	Guidelines	Compliance	Remarks
1	Whether logging is enabled on all ICT systems as per the guidelines?	☐ Yes ☐ No	
2	Whether it has been ensured that the logs of ICT Systems are retained for minimum 180 days unless specified otherwise by the CISO?	☐ Yes ☐ No	
3	Whether on-boarding of ICT systems to PRATIMAAN and IPAM done?	☐ Yes ☐ No	

5. SERVER SECURITY COMPLIANCE CHECK LIST

S.no	Guidelines	Compliance	Remarks
1	Whether applications/websites/services are hosted only at the designated data centers of Government or Cloud Service Providers empaneled by MeitY and No application/website is hosted within the LAN segment of a Ministry/Department/Office?	☐ **Yes** ☐ **No**	
2	Whether access to the server is restricted and appropriate security solutions as recommended by CERT-In and NIC-CERT are deployed?	☐ **Yes** ☐ **No**	
3	Whether provision is made to access servers only through VPN for purpose of administration and/or configuration?	☐ **Yes** ☐ **No**	
4	Whether user groups are configured as per their role and responsibilities?	☐ **Yes** ☐ **No**	
5	Whether default user accounts are disabled?	☐ **Yes** ☐ **No**	
6	Whether a provision is made to review logs of servers on daily basis and guidelines to report any suspicious activity related to user access, privilege escalation, authentications with the CISO/Dy CISO are shared?	☐ **Yes** ☐ **No**	
7	Whether server logs are maintained on a separate server and there is a provision to store the logs for minimum of 180 days unless specified otherwise by the CISO?	☐ **Yes** ☐ **No**	
8	Whether unwanted or unused OS components, services, ports, applications are uninstalled or disabled?	☐ **Yes** ☐ **No**	
9	Whether there is a staging environment for testing feature releases or to try out update/patch of OS, BIOS firmware, application?	☐ **Yes** ☐ **No**	
10	Whether enterprise level Antivirus/ EDR client recommended by CERT-In and NIC-CERT is installed on all servers?	☐ **Yes** ☐ **No**	
11	Whether provision is made to update Antivirus client and Server with the latest patches/updates?	☐ **Yes** ☐ **No**	
12	Whether IPS (Intrusion Prevention System) and DDOS (Distributed Denial of Service) mitigation tools are deployed for the servers?	☐ **Yes** ☐ **No**	
13	Whether application firewall is deployed for servers?	☐ **Yes** ☐ **No**	

14	Whether multiple servers are configured to ensure availability of services and load balancer is used to balance the load across the servers?	☐ **Yes** ☐ **No**	
15	Whether security audit of server/application is carried out before deployment with a provision to audit once a year/or every time the application is upgraded/customized?	☐ **Yes** ☐ **No**	
16	Whether all Websites and Applications are "https" enabled with a valid SSL/TLS Certificate?	☐ **Yes** ☐ **No**	
17	Whether Websites and Applications of Ministry/Department/Office are integrated with NIC SSO (parichay.nic.in) for authentication/login purposes for Government Employees?	☐ **Yes** ☐ **No**	
18	Whether Websites and Applications of Ministry/Department/Office have MFA/2FA enabled for login purpose for general public?	☐ **Yes** ☐ **No**	
19	Whether the websites of the Ministry/department follow 'Guidelines for Indian Government Websites' (GIGW) issued by MEITY?	☐ **Yes** ☐ **No**	
20	Whether it is ensured that all applications and websites will be audited by CERT-In empaneled auditing organisation prior to hosting and at-least once annually and also after any major changes?	☐ **Yes** ☐ **No**	

Name of the Ministry/Department:
Communication Address

CISO

Name:

Designation:

Email ID:

Deputy CISO:

Name:

Designation:

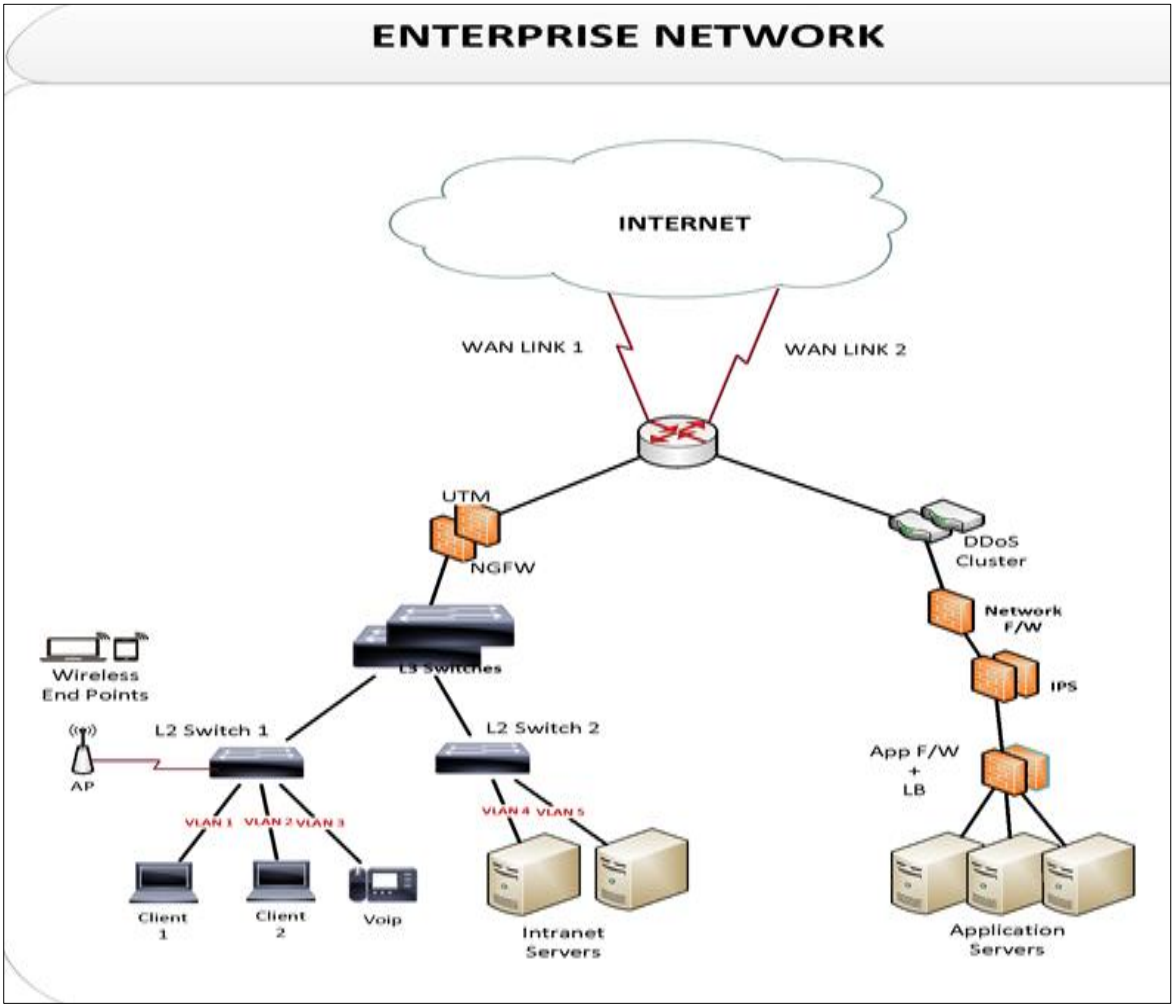
Email ID:

Appendix 2

Network Architecture for Reference

1. NETWORK ARCHITECTURE

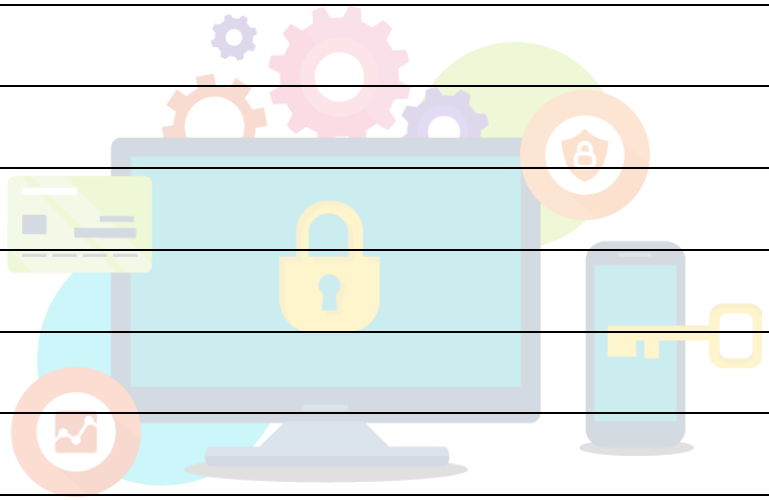
This section shows sample network architecture for Ministry/Department for reference



END

***

Notes:



Issued by

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics and Information Technology

Government of India