

CYBER SECURITY
STANDARD OPERATING PROCEDURE (SOP)



JIPMER PUDUCHERRY
Cyber Security Policy - 2025

Presented By

Er S.MURUGAIYAN DCE,B.Tech,M.Tech,MBA.,

Senior Information Engineer, JIPMER Puducherry

INDEX

S.NO	Subject	Page No
1.	Cyber Security Standard Operating Procedure	2
2.	Part-1: Endpoint Hardware and Software Security	6
3.	Part-2: Intra-Network Security	12
4.	Part-3: Internet Security	17
5.	Part-4: Asset Management and Data Handling	20
6.	Part-5: Physical and Environment Security	23
7.	Part-6: Audits and Incident Management	24
8.	General Guidelines	25

CYBER SECURITY: STANDARD OPERATING PROCEDURE

INTRODUCTION:

The increased dependence on the cyberspace warrants an understanding of the challenges and threats linked with the cyber domain. With proliferation of IT, associated cyber threats have also increased at all levels. To combat these existential threats, a comprehensive cyber security policy incorporating recent trends is a functional imperative.

The concept of cyber security develops upon **People, Process and Technology**. In order to ensure robust and resilient cyber security, we need to focus on people and process while leveraging available technology. This SOP security has been formulated in accordance with these tenets.

Policy implementation shall strengthen cyber defence and build strong resilience with risk assessment, awareness, education and training on information and cyber security.

Policy shall emphasize on information and operational security, IT and related secure asset handling, access control, backup solutions with extended utilities and environment controls.

The objective of this policy in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework at the national level. The National Cyber Security policy sets forth diverse objectives that range from enhancing the protection of India's critical infrastructure, to assisting the investigation and prosecution of cybercrime, to developing 500,000 skilled cyber security professionals over the next few years.

- a) Information Technology Act 2000 And Information Technology (Amendment) Act 2008
- b) Classification And Handling Of Classified Documents – 2001
- c) National Cyber Security Policy – 2013
- d) Army Cyber Security Policy -2023

AIM:

To lay down cyber security standard operating procedures (SOPs) for all IT products and stakeholders under IT-WING JIPMER.

VISION:

The information and cyber security policy of JIPMER for a secure and resilient information and cyber security framework at JIPMER.

PURPOSE:

The purpose of this document is to provide guidelines regarding secure network, resources and other IT assets owned by IT-Wing JIPMER from external intrusion to maintain the security and sanctity of internal data and information of the organization.

SCOPE

This policy applies to all computers and servers that are connected to the HIS-JIPMER network via standard network connection, wireless connection and virtual private network connection. It includes both HIS-JIPMER owned computers and personally-owned computers attached to the JIPMER network. The definition of computers includes desktop workstations, laptop computers and servers

RESPONSIBILITIES

Chief Information Security Officer (CISO), Network Administrator

OBJECTIVES:

The objectives of this documents are as under

- a) Generate trust and confidence in Information and Communication Technology (ICT) infrastructure that would facilitate exchange of operational and sensitive information, without compromising security.
- b) Refine overarching cyber security policies and procedures.
- c) Lay down inherent responsibility and accountability
- d) Safeguard digital information and ensure its availability, integrity and confidentiality during storage, processing, transit and handling.
- e) Create a culture and sense of cyber security and responsible user behaviour, through awareness, skill development, training and monitoring.

Inherent responsibility and accountability:

The details of responsibility of major IT-WING Products and Stakeholders have been outlined in the following paras

OIC: The Officer In-Charge of the IT-WING JIPMER will be responsible for implementation of Cyber Security policies at respective environment. Key areas of responsibility are highlighted as follows:

Daily Tasks:

- i. Ensuring timely maintenance, upkeep and logging of IT asset and service utilization.
- ii. Ensuring timely syncing of data with the main server.
- iii. Ensuring timely switching on/off of the computers, securing of data, and updation of Antivirus security suites.
- iv. Ensuring proper QoS for the Network connections.
- v. Ensuring serviceability of all IT assets, Client PCs, Servers, Network devices, peripherals, connectors, cables, repair tools etc.

Weekly Tasks:

- i. Ensuring updation of OS, firmware and software security updates/patches to the latest versions.
- ii. Ensuring timely maintenance, upkeep and logging of IT asset and service utilization and timely syncing of data with main server by PC's
- iii. Ensuring the maintenance and upkeep of server room including the wiring discipline in the Network and Server Racks.
- iv. Ensuring timely switching on/off of the computers, securing of data, and updation of Antivirus security suites.
- v. Ensuring proper QoS for the Network connections.
- vi. Ensuring serviceability of all IT assets viz, Client PCs, Servers, Network devices, peripherals, connectors, cables, repair tools etc.

Monthly Tasks:

- i. Monthly checks to ensure functional availability and preventive maintenance of IT Network and Support peripherals.
- ii. Monthly checks to ensure major security updates/upgrades of OS, firmware and software.
- iii. Providing weekly feedback to Head of the department about the operational and security concerns regarding the IT assets and services.
- iv. Ensuring the maintenance and upkeep of server room including the wiring discipline in the Network and Server Racks.
- v. Ensuring proper QoS for the Network connections.

Quarterly Tasks:

- i. Ensuring successful conduct of Quarterly internal and annual External cyber security audits of PC's, Switches, WAP along with timely liquidation of observations.
- ii. Nomination of suitable members to constitute internal and external audit teams for HIS under their IT-wing Jipmer

PART 1: ENDPOINT HARDWARE AND SOFTWARE SECURITY

Hardware Security Management

Hardware management:

a) **Inventory management of IT Assets:**

Inventory of IT hardware and devices will be maintained by Cyber Security Officers/ Network Administrators, duly nominated by Office In-charge of IT-Wing JIPMER. To ensure accountability and maintainability of IT assets, Logbooks for each IT asset will be maintained centrally by each unit establishment.

b) **Secure Disposal of Data:**

System logs, Printouts, used Printer ribbons, Printer cartridges, damaged optical media, Tapes and Hard disks should be disposed off in a secure manner. Records of disposal will be maintained for equipment by respective IT-Wing Officers.

c) **Backup and Storage of Data:**

To prevent loss of data, system backup of data system settings should be taken periodically.

Authentication and Access Control:

- a. Password based authentication and access control to be implemented.
- b. Passwords will be minimum 10 characters in the length and should have a mix of alphanumeric and special characters.
- c. To protect against unauthorized physical access, user will lock system using screensaver, login and BIOS password
- d. All users should shut down the system when leaving office premises.
- e. No unauthorizes user should be permitted to access open hardware devices.

- f. Features like camera, Wi-Fi, Voice recording, Bluetooth, GPS and Geo-tagging will be disabled on official devices like Computers, Laptops and Tablets, etc
- g. Enabling bit-locker policy at end user devices like Computers and Laptops

Software Security Management:

Software Security:

i. Operating System (OS):

Only licensed versions of OS will be used. Installation of dual boot virtualized OS at user level within official computers is strictly prohibited.

ii. Application Software:

User will Only use licensed version of application software duly examined and obtained from authorized sources.

iii. Software Updating:

User system administrators will ensure that software is regularly updated with genuine patches. Responsibility for monitoring updation of latest patches updates will be monitored by System admin.

iv. Pirated software:

Since pirated software is prone to be embedded with malicious codes and cannot be updated, use of pirated, unlicensed, cracked software is prohibited for use within official system.

v. System Hardening:

Commercially available software carries inherent vulnerabilities that need to be plugged by hardening of the system.

Actions necessary for ensuring system hardening are as follows:

- BIOS software installed in all computers servers to be hardened to ensure that only authorized peripherals are configured. Inbuilt onboard devices like internal card readers, wireless network adapters, multiple network interfaces etc. must be disabled.

- Network administrators must manually re-configure all systems to enable only essential services. All non-essential services of an OS will be disabled for enhanced cyber security. Measures for hardening of Windows based OS are available in JIPMER

Anti-Malware Software:

Malware refers to any malicious software like virus, Trojan, etc. that carries out malicious activity on a computer system or network. To protect against such malicious activities, user must install, a comprehensive anti-malware security suite that provide features like anti- virus, anti-spam, anti-root kits.

Personal Firewall:

Firewall prevents potential intruders in a network from gaining access to a system. All users must have software firewall running on their personal computers. By default, Windows OS comes with an inbuilt firewall which must be enabled.

Encryption Software:

Encryption provides another layer of security to a user handling classified information data. Users should install file and folder encryptions software like vera crypt for ensuring security of information data.

User Access Control:

Access control policy ensures “Role Based Access”, network administrators at all levels will ensure implementation of the following measures.

✓ **Privilege management:**

A user must always log in with user rights and not with administrative rights. Administrator accounts should always be managed by network administrator.

✓ **Password Management:**

Users will implement multilevel password based authentication and access. Multi-level passwords refer to BIOS password user account login and screensaver password.

✓ **Management of USB Ports:**

To prevent information theft and intrusion related malicious activities, USB ports will be disabled on all computers to prevent access to mass storage media.

✓ **Data ownership of End point terminal:**

User remains sole owner/custodian of data on computer and is responsible for terminal end user level violations like use of USB device, air-gap violation, unauthorised formatting, violations related to security classification of data etc.

✓ **Unauthorised data:**

Unauthorised data like personal documents, presentations, multimedia files, pornographic content etc. will not be stored within official systems.

Security of System documentation:

System documents and files (such as logs, configuration files of IT devices, photocopiers, etc) should be stored on designated computers in a secure manner to prevent unauthorised access, modification or deletion.

Desktop/Laptop and Printer Security:

- 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.
- Set Operating System updates to auto-updated from a trusted source
- 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.
- Always lock/log off from the desktop when not in use.
- Shutdown the desktop before leaving the office.
- Keep printer's software updated with the latest updates/patches.
- Setup unique pass codes for shared printers.
- Internet access to the printer should not be allowed.
- Printer to be configured to disallow storing of print history.
- Enable Desktop Firewall for controlling information access.

- Keep the GPS, Bluetooth, NFC and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.
- Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.
- 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.).
- Do not use any external mobile App based scanner services (ex: Cam scanner) for scanning internal government documents.
- Remove pirated /unsupported Operating systems and other software/applications that are not part of the authorized list of software.

Password Management:

- ✓ Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters
- ✓ Change passwords at least once in 120 days.
- ✓ Use Multi-Factor Authentication, wherever available.
- ✓ Don't use the same password in multiple services/websites/apps.
- ✓ Don't save passwords in the browser or in any unprotected documents.
- ✓ 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).
- ✓ Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons

Internet Browsing Security:

- ✓ 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.
- ✓ 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.

- ✓ Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
- ✓ Don't store any usernames and passwords on the internet browser.
- ✓ Don't store any payment related information on the internet browser.
- ✓ Don't use any 3rd party anonymization services (3rd party VPN, Tor, Proxies etc).
- ✓ Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.
- ✓ Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software).
- ✓ Don't use your official systems for installing or playing any Games

Email Security:

- ✓ Ensure that Multi-Factor Authentication is configured on the JIPMER Email Account.
- ✓ Download app from valid mobile app stores only. Do not download from any website.
- ✓ Do not share the email password or OTP with any unauthorized persons.
- ✓ Don't use any unauthorized/external email services for official communication.
- ✓ Don't click/open any link or attachment contained in mails sent by unknown sender.
- ✓ Regularly review the past login activities on JIPMER 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 IT-WING Team.

Removable Media Security:

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

PART 2: INTRA-NETWORK SECURITY

Network Management.

Responsibility Of Network Management

Networks will be managed and controlled to protect them from cyber threats. Appropriate security solutions will be incorporated at physical, network, transport and application layers.

Network And Application Access control.

Access to both internal and external network service resources will be as,

- **Remote Access Software:** third party application software used for remote access to a system over a network, like Team Viewer and Any Desk is prohibited from use on official computers.
- **Access Control:** Access to software and related information will be restricted to authorized users only.
- **Security of Application Software:** the classification of an application software will be explicitly defined and documented. All applications will be duly examined by cyber security point of view.
- **Network Administrator shall implement the following:**
 - ✓ Review the router services and configurations and disable all unwanted services
 - ✓ Disable the services finger
 - ✓ Disable source routing
 - ✓ Disable directed broadcasts on appropriate interfaces
 - ✓ Disable IP Redirects on untrusted interfaces. To disable IP Redirect messages, issue the following command on desired interfaces: 'no IP redirects'
 - ✓ Disable root admin
 - ✓ Disable Auto-Loading thereby requiring that the router configuration be loaded from local memory and not the network

- ✓ Router should be physically placed in a shelf or rack mount with locking facility

Network Segmentation:

- ✓ Ensure segmentation of the network to create security zones for isolating sensitive traffic and secure critical IT systems.
- ✓ 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.
- ✓ 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.
- ✓ 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.
- ✓ Applications / servers and systems in the Intranet should be separated from Internet facing networks/ systems.

Security Zones:

Virtual LANs should be used by JIPMER Campus to logically separate zones. Communication between different VLANs and allowed on need basis with per port / application basis.

Network Traffic Segregation:

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

- ✓ Implementation of traffic flow filters, VLANs, network and host-based firewalls.
- ✓ Implementation of application-level filtering, proxies, content-based filtering.
- ✓ Wherever possible physical segregation must be preferred over logical segregation

Physical Isolation:

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

- ✓ All the terminals or computers dealing with sensitive/classified information should not have any wireless equipment including Internet and Bluetooth.
- ✓ Disable SSID broadcasting to prevent the access points from broadcasting the SSID. Allow only authorized users with preconfigured SSID to access the Wireless network.
- ✓ Disable DHCP and assign static IP addresses to all wireless users.

Disabling Unused Ports:

The JIPMER Campus 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

Personal Devices Usage Policy:

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

Restricting Access To Public Network:

The JIPMER Campus must disable unused network adapters in systems and restrict internet connection sharing and Adhoc network creation.

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.

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.

Default Device Credentials:

The JIPMER Campus 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.

Connecting Devices:

The IT-Wing 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.

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/JIPMER Campus

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.

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.

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.

Authentication mechanism for access:

The JIPMER campus must implement multi- factor authentication as much as possible.

Segregation Of Duties:

- Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
- Documents duties of staff and privileges of different roles.
- Create different administrator accounts for different roles assigning only the needed security attributes and privileges which are just needed for those roles alone.

PART 3: INTERNET SECURITY

Extension Of Internet

The hiring of internet connectivity will be ensured primarily from Govt affiliated Internet Service Provider (ISP) only. The extension and securing of internet connectivity will be as under:

- All internet connected computers deployed in JIPMER premises of various department must be installed with standardized genuine OS and office software along with requisite cyber security controls.
- Adapters providing Wi-Fi connectivity should not be installed within the official devices. Devices with in-built Wi-Fi adaptors should be disabled.
- A list of users authorized internet connectivity within the office premises must be maintained within the Campus.

Internet computer will not be connected to following devices

- Mobile phones
- Plug and surf type of GSM/CDMA USB MODEMS
- Wi-Fi, Bluetooth, Near Field Communication (NFC) adaptors, dongles, etc.

SECURE WIRELESS LAN:

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

WI-FI GUIDELINES

The following are the baseline controls to be implemented on all wireless networks in JIPMER -

- ✓ Before using your wireless router, turn on security
- ✓ Use WPA security and not WEP
- ✓ Change the default password
- ✓ Change the default SSID
- ✓ Place the router in a physically secure place
- ✓ Upgrade to the latest software
- ✓ In addition to the above, following controls can be optionally implemented to enhance security level on wireless devices:
- ✓ Use MAC filtering for access control
- ✓ Wi-Fi configuration will be defined on the firewall to bind user login with MAC address of user
- ✓ Disable remote administration
- ✓ Enable firewall on the access point

Web Filtering Provides Protection

These categories allow you provide protection to business users by:

- 1 Blocking access to categories including malware, phishing, malicious sites and spam sites.
2. Adhere to corporate usage policy by blocking access to categories such as adult, pornography, gambling, hate speech and nudity.
3. Create usage policies to ensure resource protection, controlling or limiting access to social media, social sites, video or streaming sites.

1. **Criminal Skills/Hacking**: Activities that violate human rights including murder, sabotage, bomb building etc. Information about illegal manipulation of electronic devices, encryption, misuse, and fraud. Warez and other illegal software distribution.
2. **Dating**: Web pages that promote relationships such as dating sites and marriage sites.

3. **Chat/Instant Messaging:** Communication through chat or Instant Messaging services as well as sites with information about Instant Messaging communication or chatrooms. A particularly popular category with the increased popularity of Facebook messenger.
4. **Gambling:** Web pages which promote gambling, betting, lotteries, casinos and betting agencies involving chance
5. **Games:** Web pages consisting of computer games, game producers and online gaming
6. **Hate Speech:** Web pages that promote extreme right/left wing groups, sexism, racism, religious hate and other discrimination
7. **Illegal Drugs:** Web pages that promote the use or information of common illegal drugs and the misuse of prescription drugs and compounds
8. **Nudity:** Web pages that display full or partial nudity with no sexual references or intent
9. **Online Ads:** Web pages strictly devoted to advertising graphics, banners, or pop-up ad content
10. **Pornography/Sex:** Explicit sexual content unsuitable for persons under the JIPMER campus.
11. **Tobacco:** Web pages promoting the use of tobacco related products (cigarettes, cigars, pipes)
12. **Weapons:** Web pages that include guns and weapons

Zero Tolerance For Use Of Pen Drives And Air Gap Violations:

The use pen drives is strictly prohibited and incident of air gap violations shall invite strict admin proceedings. No personal data will be processed or stored on internet PC.

PREVENTION OF DATA LEAKAGE:

Data leakage may take place inadvertently or by use of unauthorised software on official computers. Details of the same are given as under:

- Name of computer or user account configured on internet computers, should not reveal appointment, identify of the person, unit using computer.
- Unauthorised software (normally obtained as free software) will not be installed on official computers. Some examples of such software are as under:

❖ Messenger and Chat Software:

Software like Skype, Yahoo Messenger, Google Talk, WhatsApp, WeChat, etc provide facilities of free chatting and instant messaging. The Messenger, chat software

maintains a list of all contacts and related information on its servers. Hackers can exploit such information and also spread malware to all contacts.

❖ **File Sharing Software:**

The Software including Torrent Clients, eMule, etc that facilitate peer-to-peer file or folder sharing. Such software, besides facilitating download also enable simultaneous upload of data amongst its users hence are inherently insecure and disposed to compromise by hackers

❖ **Remote Access software:**

Software providing remote access to users, agencies over internet will not be installed on official computers. Software like Team viewer, Any Desk etc allow remote access of machine, data rendering it vulnerable to compromise.

PART 4: ASSET MANAGEMENT AND DATA HANDLING

INVENTORY OF ASSETS:

Inventory of cyber/ IT assets and infrastructure must be prepared and updated periodically. Updated inventory list of all cyber assets will be checked during cyber security audits.

Ownership And Accountability Of Assets:

All cyber and IT assets like servers, computers, Laptops, Routers, Switches, Unified Threat Management (UTM) devices, Firewall, Mobile computing Devices, Multi-function Devices (MFDs), Digital Cameras, Removeable Optical Media(CD/DVD/Pen drive), Printers, Scanners and Smart TVs will be held on charge of designated holder or user.

The holder will be responsible for accounting, handling, administering and secure disposal of these assets. It will be ensured that these devices are accounted for at all times and any theft, loss must be reported promptly through the intelligence channel. Proper record of handling taking over of digital assets, duly countersigned by superior officer, will be maintained and produced during cyber security audits.

Accounting Of Secondary Mass Storage Devices:

Strict control is required to be exercised in use of secondary mass storage devices such as CD/DVD writers, USB Storage, External HDD and Ethernet based hard drives, Network Attached Storage (NAS) Drives. Cyber security audits must ensure a comprehensive check of all related security aspects.

Disposal Of Storage Media and Printer Cartridges:

Storage media and user printer cartridge will be disposed off in a secure manner when it fulfils its desired task completes its functional lifecycle.

The suggested method for disposal of such media is by secure destruction of the optical and magnetic platter or adopting physical destruction methods like disintegration, incineration, melting and shredding.

A record of all such destruction by Board of Officers must be maintained and produced for audit.

Handling of Removable Storage Media:

Ban On Universal Serial Bus (USB) Based Storage Media:

Use of removable USB based storage devices is banned. All types of memory sticks including external USB based hard disks, Secure Digital (SD), Mini-SD, Multi Media Card(MMC cards), Personal Digital Assistant (PDAs) and mobile phones come under preview of this ban. Such devices will neither be procured nor be held by any office.

Unauthorised Possession Of Information/Data:

Handing / Taking Over By All Ranks:

All ranks and personals will ensure that no official data is retained on their personal IT assets. Unauthorised possession of information and data in soft form needs to be prevented at all levels.

The under mentioned certificate will be added in the Handing and Taking over certificate of all key appointments handling IT assets, on being posted out:

- I am not carrying Soft and Hard copy of any classified and unauthorised

information data.

- I am aware that violation of above declaration will render me liable to disciplinary action.

Change Management:

All changes in hardware, software and their configuration will be duly analysed and carried out in a controlled manner under supervision. The following need to be ensured in this regard.

➤ **System Formatting, Recovery, Repair and Restore:**

Permission from appropriate authority will be obtained prior to formatting, recovery, repair or restoration of information system assets, including computers, laptops, external storage disks etc.

➤ **Maintenance Repair:**

Records of system formatting, recovery, repair or restoration, carried out will be maintained in designated registers specifically maintained for the purpose. All such registers will be produced during the internal and external cyber security audits.

Change of Appointment:

On change of appointment, de-facto formatting of computers will not be resorted to. The handing and taking over of IT assets will be undertaken as follows:

- An internal audit should be conducted by the new incumbent during the change of appointment and all digital information assets taken on charge.
- Access rights to particular information and information processing facilities for any appointment, user will be revoked immediately on transfer or relinquishing of the appointment.
- The network administrator will issue fresh user credentials with role based access rights to the new user on assumption of appointment.
- The handing and taking over of information regarding access rights must be undertaken directly between appointments and not through clerks

PART 5: PHYSICAL AND ENVIRONMENT SECURITY

PHYSICAL AND ENVIRONMENT SECURITY:

Secure Areas:

Information processing facilities will be housed in secure areas. Entry to these secure areas will be controlled, regulated and monitored to ensure that only authorised persons are allowed access.

IT assets deployed in common un attended areas should be secured against unauthorised access.

Access Security:

Security parameters such as access cards, biometric access devices, controlled entry points or manned reception desks will be used to establish entry to areas that contain information and information processing facilities.

Network Cabling:

All network cabling and test points will be protected from unauthorised interception and damage. All network cables should be uniquely marked to indicate type of connectivity handled, unused network sockets should be blocked and their status formally documented.

Medium Access Control (MAC) binding must be ensured in all network switches. Structured cabling should be ensured within all centralized communication and IT premises.

Internal cyber security checks should entail periodic physical inspection of cables to detect tampering at all levels

PART 6: AUDITS AND INCIDENT MANAGEMENT

AUDITS:

The Head of Department IT-Wing JIPMER shall nominate suitable members to constitute audit teams for the IT-Wing. The records of the audits are to be maintained and furnished during Annual Inspections:

a) Internal Audits:

Internal audit to be undertaken on Quarterly basis by nominated Team.

b) External Audits:

External audit to be undertaken on annual basis by nominated agencies.

INCIDENT REPORTING AND HANDLING:

Cyber Incidents:

Cyber incident is an adverse event on computer and information system, network or threat of occurrence of such an incident. examples of cyber incidents could be loss of information from computer, computer resource, compromise of access controls or malware infection etc.

Incident Reporting:

All cyber security incidents will be reported to IT-WING Engineers through respective IT-Wing staffs at various levels like Office In-Charge, Head of the Department, Computer Programmer. format for reporting the incident to make available on JIPMER IT-wing portal as “Incident Reporting Form”.

GENERAL GUIDELINES:

- Router configuration files shall be secured by providing access rights given by Network Administrator only to authorized users.
- Personal use of computer and network resources shall be allowed with approval from IT-WING after sending request by the concerned Nodal Officer.
- Network architecture shall be such that each application and database server of production environment shall be in clustering mode and proper backup shall be scheduled periodically.
- Network components used for network security shall be configured properly and quarterly tested by Network Administrator. The backup of these configurations shall be taken quarterly or when any changes made to the system
- Documentation related to Network devices, configuration and architecture shall be properly maintained and updated when required.
- Appropriate tools shall be deployed to manage and monitor network health on daily basis. Proper log shall also be maintained which specify type of network, bandwidth limits, inbound & outbound traffic etc. and can archived for future reference.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself. Wherever technically feasible, single points of failure in network shall be minimized.
- The Network Administrator shall evaluate each new release of the network component to determine whether any upgrade is required or not.
- Password, Firewall, Antivirus, Remote Access and logical access control Policy shall be followed strictly to access the network devices / services.
- IT-Admin shall be configured to ensure detection and prevention of any malicious network traffic entering the network. The number of entry points to IT-JIPMER network shall be restricted and secured through firewall, web content filtering and Intrusion Detection System.
- Network devices shall be configured to display logon banners which provide adequate warning against unauthorized logon attempts. These banners shall give least information about the network and system to the user.

The following logon banner shall be displayed to the users:

L E G A L W A R N I N G

- This system is owned by IT-JIPMER. If you are not authorized to access this system, exit immediately. Unauthorized access to this system is forbidden by IT-WING policy

Unauthorized users are subject to criminal and civil penalties as well as IT-WING initiated disciplinary proceedings. By entry into this system you acknowledge that you have authorized access and the level of privilege you subsequently execute on this system. You further acknowledge that by entry into this system you expect no privacy violation from monitoring.”

- Configure “session timeouts” (2minutes) for the interface using the exec-timeout command.
- Remote maintenance of the network shall be restricted to authorized individuals, confined to individual secured sessions from internal network, and subject to review to prevent unauthorized access to the network through the misuse of remote maintenance facilities.
- The Network Administrator shall store any kind of password in a secure form.