CYBER SECURITY SOP

CO ECHS

INDEX

CYBER SECURITY: STANDARD OPERATING PROCEDURE

Introduction.

1. 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.

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

3. All IT assets of stakeholders under **ECHS** and personnel handling these resources will be governed by this cyber security policy. It is imperative that all personnel are fully conversant with this SOP. Contravention of any clause of this policy will be construed as a cyber-violation and mandated for suitable disciplinary action. The SOP has been derived by referring following documents, which same may be referred for further clarification on the subject: -

(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.

4. To lay down Cyber Security Standard Operating Procedures (SOPs) for all stakeholders under ECHS.

Objectives.

5. The objectives of this document 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 behavior, through awareness, skill development, training and monitoring.

Inherent responsibility and accountability.

6. The details of responsibility of major stakeholders have been outlined in following paras:-

(a) **OIC PC**. The Officer in Charge of the Polyclinic (PC) will be responsible for implementation of cyber security policies at respective PC. 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 the maintenance and upkeep of server room including the wiring discipline in the Network and Server Racks.

(iv) Ensuring timely switching on/off of 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.

Weekly Tasks.

(i) Ensuring updation of OS, firmware and software security updates/patches to the latest versions.

(ii) Providing weekly feedback to Dir RC about the operational and security concerns regarding the IT assets and services.

(iii) Fortnightly checks of the IT assets in accordance with latest official cyber security audit check-list.

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) Ensure liquidation of observations raised during external cyber security audit.

Quarterly Tasks.

(i) Ensuring successful conduct of Quarterly Internal and annual External cyber security audits at the PC along with timely liquidation of observations.

(b) **OIC ECHS Cell (Station HQ)**. Officer in Charge at ECHS Cell (Stn HQ) will ensure implementation of cyber security policies at respective PC associated with Stn HQ. Key areas of responsibility are highlighted as follows:-

Weekly tasks.

(i) Ensuring timely maintenance, upkeep and logging of IT asset, service utilization and timely syncing of data with main server by PC's.

(ii) Ensuring maintenance and upkeep of server room including the wiring discipline in the Network and Server Racks by PC's.

(iii) Ensuring timely switching on/off of computers, securing of data, and updation of Antivirus security suites by PC's.

(iv) Ensuring proper QoS for the Network connections at PC's.

(v) Ensuring serviceability of all IT assets viz. Client PCs, Servers, Network devices, peripherals, connectors, cables, repair tools etc. at PC's.

(vi) Ensuring updation of OS, firmware and software security updates/patches to the latest versions at PC's.

Monthly Tasks.

(i) Monthly checks to ensure functional availability and preventive maintenance of IT Network and Support peripherals at PC's.

(ii) Monthly checks to ensure major security updates/upgrades of OS, firmware and software at PC's.

Quarterly Tasks.

(i) Ensuring successful conduct of Quarterly Internal and the annual External cyber security audits of PC along with timely liquidation of observations of PC's.

(ii) Nomination of suitable members to constitute internal and external audit teams for PCs under their AORs.

(c) **Director RC.** Dir RC will be overall responsible for implementation of cyber security policies at respective RC and all PCs under AOR. He will also be

responsible for resolving key concerns as projected by PCs under AOR. Key areas of responsibility are highlighted as follows:-

Weekly Tasks.

(i) Ensuring updation of OS, firmware and software security updates/patches to the latest versions at RC/PC's.

(ii) Fortnightly checks of IT assets in accordance with latest official cyber security audit check-list at RC/PC's.

(iii) Ensuring maintenance and upkeep of server room including wiring discipline in Network and Server Racks at PC's.

(i) Ensuring timely switching on/off of computers, securing of data, and updation of Antivirus security suites at PC's.

Monthly Tasks.

(i) Monthly feedback from ECHS Cell (Station HQ) associated with PC's under respective RC, about salient operational and security concerns regarding IT assets and services of the PCs under AOR.

(ii) Ensure liquidation of observations raised during external cyber security audit at RC/PC's.

(iii) Monthly checks to ensure functional availability and preventive maintenance of IT Network and Support peripherals issues of PC's.

Quarterly Tasks.

(i) Ensuring successful conduct of Quarterly Internal and annual external cyber security audits at RC/ PC's along with timely liquidation of observations.

(ii) Feedback to CO ECHS about salient operational and security concerns regarding IT assets and services at PC's/ECHS Cell and pertinent cases of the RC/PC's under AOR.

PART I: ENDPOINT HARDENING AND SOFTWARE SECURITY

Hardware Security Management.

7. **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 Stn HQ's for each PC. 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, print outs, 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 PC/ est.

(c) **Backup and Storage of Data**. To prevent loss of data, system backup of data and system settings should be taken periodically.

8. **Authentication and Access Control.**

(a) Password based authentication and access control to be implemented.

(b) Passwords will be minimum 10 characters in 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 unauthorized 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, Tablets, etc.

Software Security Management.

9. **Software Security**.

(a) **Operating System (OS)**. **Only licensed version of OS will be used.** Installation of dual boot/ virtualized OS at user level within official computers is strictly prohibited.

(b) **Application Software**. Users will **only use licensed version of application software** duly vetted and obtained from authorized sources.

(c) **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 that of the Dir RC in consultation with Station Cdr of respective PC.

(d) **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.

(e) **System Hardening**. Commercially available software possesses inherent vulnerabilities that need to be plugged by hardening of the system. Actions necessary for ensuring system hardening are as follows:-

(i) 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.

(ii) 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 and Linux based OS are available on CERT-Army website.

10. **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, users must install, a comprehensive anti-malware security suite that provide features like anti-virus, anti-spam, anti-root kits.

11. **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.

12. **Encryption Software**. Encryption provides another layer of security to a user handling classified information/ data. Users should install file and folder encryption software like **Vera crypt** for ensuring security of information/ data.

User Access Control.

13. Access control policy ensures "Role Based Access". Network administrators at all levels will ensure implementation of the following control measures:-

(a) **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.

(b) **Password Management**. Users will implement multilevel password based authentication and access control. Multi-level passwords refer to BIOS password, user account login and screensaver password.

(c) **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.

(d) **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.

14. **Security of System Documentation**. System documents/ files (such as logs, configuration files of IT devices, photocopiers, MFD's etc) should be stored on designated computers in a secure manner to prevent unauthorised access, modification or deletion.

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

PART II: INTRA-NETWORK SECURITY

Network Management.

16. **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.

17. Access to both internal and external network services/ resources will be as: -

(a) **Remote Access Software**. Third party application software used for remote access to a system over a network, like Team Viewer and Virtual Network Computing (VNC) is prohibited from use on official computers.

(b) **Access Control**. Access to software and related information will will be restricted to authorized users only.

(c) **Security of Application Software**. The classification of an application software will be explicitly defined and documented. All applications will be duly vetted by Def Cyber Agency from cyber security point of view.

PART III: INTERNET SECURITY

Extension of Internet.

18. 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: -

(a) All internet connected computers deployed in office premises of various RC/PC/ests must be installed with a **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.

(b) A list of users authorized internet connectivity within the office premises must be maintained within Organisation.

19. Internet computer will not be connected to following devices

(a) Mobile phones

(b) "Plug and Surf" type of GSM/ CDMA USB MODEMs.

(c) Wi-Fi/ Bluetooth/ Near Field Communication (NFC) adaptors, dongles, etc.

20. **Zero Tolerance for Use of Pen Drives and Air Gap Violations**. The use of 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.

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

(a) Name of computer or user account configured on internet computers, should not reveal appointment/ identity of the person/ unit using computer.

(b) Unauthorised software (normally obtained as free software) will not be installed on official computers. Some examples of such software are as under:-

(i) **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.

(ii) **File Sharing Software**. These software including Torrent Clients, e-mule, 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 prone to compromise by hackers.

(iii) **Remote Access Software**. Software providing remote access to users/ agencies over internet will not be installed on official computers. Software like VNC, Team Viewer etc allow remote access of machine/data thus, rendering it vulnerable to compromise.

PART IV: ASSET MANAGEMENT AND DATA HANDLING

22. **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.

23. **Ownership and Accountability of Assets**. All cyber/ IT assets like Servers, Computers, Laptops, Routers, Switches, Unified Threat Management (UTM) devices, Firewalls, Mobile Computing Devices, Multi-function Devices (MFDs), Digital Cameras, Removable Optical Media (CDs/ DVDs), Printers, Scanners and

Smart TVs will be held on charge of a 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 handing/ taking over of digital assets, duly countersigned by superior officer, will be maintained and produced during cyber security audits.

24. **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 and Ethernet based hard drives/ Network Attached Storage (NAS) Drives. Cyber security audits must ensure a comprehensive check of all related security aspects.

25. **Equipment Maintenance and Repair**. Equipment will be properly maintained to ensure its continued availability. In case, a faulty hard disk is under warranty/ AMC, it will still be destroyed in situ by an authorised Board of Officers (BOO). Under no circumstances will it be returned to the vendor for replacement. In case the vendor insists, only details of the hard disk i.e. photo of outer label containing serial number may be shared with vendor.

26. **Disposal of Storage Media/ Printer Cartridges**. Storage media and used 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/ magnetic platter or adopting physical destruction methods like disintegration, incineration, melting and shredding. A record of all such destruction by a Board of Officers must be maintained and produced for audit.

Handling of Removable Storage Media.

27. **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 purview of this ban. Such devices will neither be procured nor be held by any office.

Unauthorised Possession of Information/Data.

28. **Handing/ Taking Over by All Ranks**. All ranks/personals will ensure that **no official data is retained on their personal IT assets**. Unauthorised possession of information/ data in soft form needs to be prevented at all levels. The under mentioned certificate will be added in the Handing/ Taking over Certificate of all key appointments handling IT assets, on being posted out:-

(a) I am not carrying soft/ hard copy of any classified/ unauthorised information/ data.

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

Change Management.

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

(a) **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.

(b) **Maintenance of Records**. 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.

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

(a) An internal audit should be conducted by the new incumbent during the change of appointment and all digital information assets taken on charge.

(b) Access rights to particular information and information processing facilities for any appointment/ user will be revoked immediately on transfer or relinquishing of the appointment.

(c) The network administrator will issue fresh user credentials with role based access rights to the new user on assumption of appointment.

(d) The Handing/ Taking over of information regarding access rights must be undertaken directly between appointments and not through clerks.

PART V : PHYSICAL AND ENVIRONMENT SECURITY

Physical and Environment Security

31. **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 unattended areas should be secured against unauthorised access.

32. **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.

33. **Power Supply**. IT equipment will be protected from power failures and other disruptions. Standby arrangements, in terms of Uninterrupted Power Supply (UPS) and backup power will be catered for.

34. **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 VI: AUDITS AND INCIDENT MANAGEMENT

Audits.

35. The Station HQ shall nominate suitable members to constitute audit teams for the PCs and RCs under their AORs. 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 agencies.

(b) **External Audits.** External audit to be undertaken on **annual basis** by nominated agencies.

Incident Reporting and Handling.

36. **Cyber Incidents**. Cyber incident is an adverse event on a computer/ information system/ network or a 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.

37. **Incident Reporting**. All cyber security incidents will be reported to CERT- Army through respective IW/GS Staff at various levels (Stn Hq/ Sub Area Hq/ Area Hq/ Corps Hq/Comd Hq with a copy to CO ECHS. Format for reporting the incident is available on the CERT-Army website as 'Incident Reporting Form'.

File No : B/49722-IT/SOP/AG/ECHS

Delhi Cantt-10

(Anurag Bhardwaj)
Col
Dir (Stats & Automation)

31 Dec 2024

Distr :-
All Br/Sec, CO ECHS
All RCs/PC