DTE GEN OF MIL OPS

सत्यमेव जयते

ARMY CYBER SECURITY POLICY 2017

ARMY CYBER SECURITY POLICY - 2017

No information given in this document is to be published or communicated either directly or indirectly to any person or group not authorized to possess it.

Issued vide Integrated HQ of MoD (Army) Letter Number A/12100/Policy/MO-12 dated 07 Feb 2017

CONTENTS

ARMY CYBER SECURITY POLICY - 2017

References:-

(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 Crisis Management Plan - 2013.

(e) Directive for Convergence of Information Warfare, Information Systems and Communication Technology Functions/ Organisations to Enhance Operational Effectiveness of the Indian Army- 2014.

(f) General Staff Policies on Communication and Information System of Indian Army: 2015.

(g) Communication and Information System Directive for Indian Army 2015.

(h) National Information Security Policy Guidelines Version 5 – 2016.

Note.

1. All standard definitions for terminologies as applicable in IT Act 2000 and IT (Amendment) Act 2008 have been included in this document.

2. All advisories mentioned in the document are hosted on the CERT-Army website, Army Data Network.

ARMY CYBER SECURITY POLICY – 2017

Introduction

1. The increased dependence on the cyberspace warrants an understanding of the challenges and threats linked with the cyber domain. With the proliferation of IT, the associated cyber threats have also increased at all levels. To combat these existential threats, a comprehensive cyber security policy incorporating the recent trends is a security and 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 the available technology. Army Cyber Security Policy – 2017 (ACSP-2017) has been formulated in accordance with the above mentioned tenets. The ACSP-2017 will serve as the core document, based on which the cyber security SOPs, guidelines and instructions at various HQs/ Units/ Establishments will be laid down.

3. All IT assets of the Indian Army (IA) and personnel handling these resources will be governed by this cyber security policy. It is imperative that all personnel are fully conversant with this policy. Contravention of any clause of this policy will be construed as a cyber-violation mandated for suitable disciplinary action. This policy supersedes the Army Cyber Security Policy - 2014 (ACSP-2014).

Aim

4. To lay down **Army Cyber Security Policy - 2017** for the IA.

Objectives

5. The objectives of ACSP - 2017 are as under:-

(a) Secure the cyber space of IA.

(b) Generate trust and confidence in IA Information and Communication Technology (ICT) infrastructure that would facilitate exchange of operational and sensitive information, without compromising security.

(c) Refine overarching cyber security policies and procedures.

(d) Lay down inherent responsibility and accountability.

(e) Safeguard digital information and ensure its availability, integrity and confidentiality during storage, processing, transit and handling.

(f) Create a culture and sense of cyber security and responsible user behaviour, through awareness, skill development, training and monitoring.

Layout

6. The layout of ACSP - 2017 is as under:-

(a) Part I : Organisation and Responsibility.

(b) Part II : Basic Cyber Security Issues.

(c) Part III : Desktop Security.

(d) Part IV : Network Security.

(e) Part V : Army Data Network(ADN) Security.

(f) Part VI : Internet Security.

(g) Part VII : Development and Deployment of Information System.

(h) Part VIII : Incident Management and Forensics.

(j) Part IX : Cyber Security Audit and Compliance.

PART I : ORGANISATION AND RESPONSIBILITIES

Organisation for Cyber Security

7. Cyber Security Forum (CSF) is the apex body for Cyber Security in IA under the Chairmanship of DGMO. It is responsible for formulating and reviewing policies related to Cyber Security in the IA.

8. Cyber Security is a command responsibility and will be executed by commanders at all levels. All formation HQ, units and establishments will nominate a Cyber Security Officer for ensuring implementation of Cyber Security policies and procedures.

Cyber Security Forum

9. CSF is responsible for formulation and review of policies related to Cyber Security in the IA. The composition of CSF is at **Appendix A**. The charter of duties of the forum is as under:-

(a) Monitor implementation of Cyber Security Policy.

(b) Review and recommend changes in Cyber Security Policy.

(c) Review Cyber Security incidents.

(d) Review vulnerability assessment.

(e) Recommend major Cyber Security initiatives.

10. **CSF Interaction**. The CSF will convene once every two years. BGS (IW) from all Command HQ and BGS from HQ ARTRAC will participate in the deliberations at CSF. CSF will address important issues of the policy as well as new developments in cyber space affecting cyber security. Amendments, if any, to Cyber Security Policy will then be issued to the environment.

Responsibility : Cyber Security

11. Cyber Security is a command responsibility and commanders at all levels will ensure fool proof cyber security at all times. They shall also ensure implementation of policies and guidelines at all times. Details of actions to be undertaken by commanders at all levels are as under:-

(a) Ensure implementation of ACSP-2017.

(b) Formulation and implementation of SOPs on information security and information assets in cyber space.

(c) Clearly define ownership and responsibilities for protection of all information assets like computers, laptops, info kiosks, printers, multi-function devices, scanners, removable media, hard disks, networking components and premises housing these assets.

(d) Ensure conduct of periodic internal and external cyber security audits to monitor the implementation and effectiveness of all cyber security measures.

(e) Conduct periodic police verification and Military Intelligence (MI) clearance of all civilians (including on-site/ Resident Engineers) employed within various formation premises, prior to and during employment.

(f) Take corrective measures/ disciplinary action on detection/ reporting of cyber security lapses.

Cyber Security Structure at IHQ of MoD (Army)

12. **Chief Information Security Officer (CISO)**. ADG/ MO (IW) is the CISO for the IA. He is the nodal authority and single point of contact for all issues related to cyber security in IA. The CISO will represent IA in all interactions with agencies at the National (all Govt/ Non-Govt organisations) and Tri-Services levels. Within IA, CISO will execute all Cyber related functions through MO-12 and Army Cyber Group. The role and functions of the Directorates and agencies with respect to cyber security is given in succeeding paras.

13. **Cyber Security Organisations of the Indian Army**. Army Cyber Group is the nodal executive agency for all cyber functions of the Indian Army. ADG MO (IW) exercises operational control over the Army Cyber Group through DGMO/ MO-12. Cyber Organisations are proposed to be raised at the Command level under the operational control of the BGS (IW). An organisation chart showing the cyber organisations and their linkages is shown below.

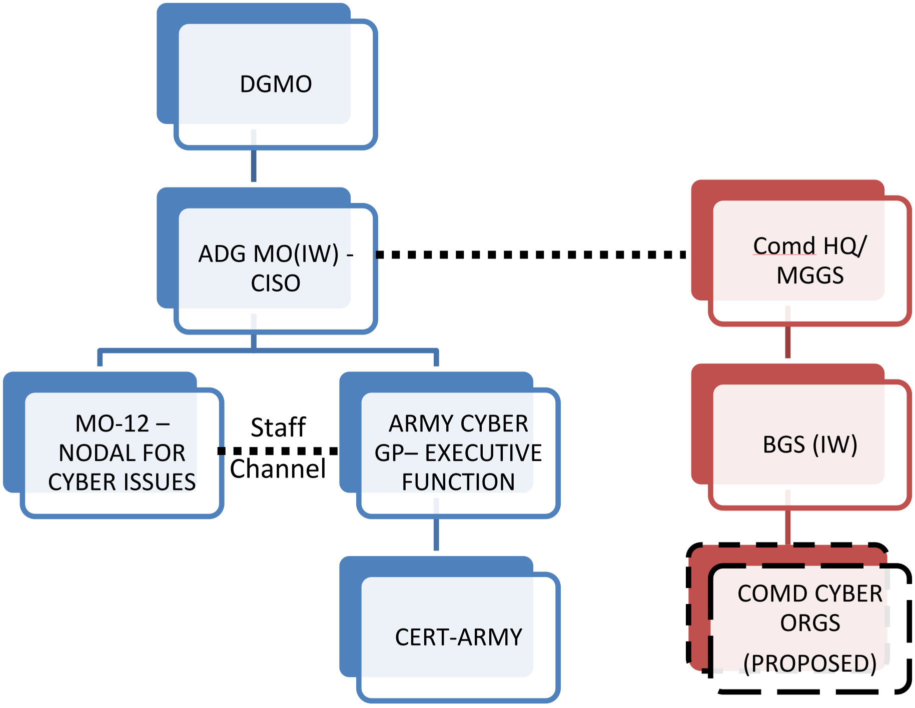
DGMO
ADG MO(IW) - CISO
Comd HQ/ MGGS
MO-12 – NODAL FOR CYBER ISSUES
Staff Channel
ARMY CYBER GP– EXECUTIVE FUNCTION
BGS (IW)
CERT-ARMY
COMD CYBER ORGS (PROPOSED)

Fig: Cyber Security Organisations of the IA

14. **Army Cyber Group**. Army Cyber Group is the nodal agency for executing all cyber functions in the IA. In addition, on behalf of the CISO, Army Cyber Group will interact with Cyber Security organisations of other Services, Govt Departments, CERT-India, Defence Research and Development Organisation (DRDO), industry and academia on all Cyber Security issues. Army Cyber Group will execute the following tasks: -

(a) Conduct external cyber security audit of all Command HQ, Directorates/ Branches at IHQ of MoD (Army), Communication Nodes and Complexes including Central and Regional Network Security Operation Centres (NSOC), Data Centres (to include CDC, NLDCs, RDCs and DRDCs), Army Data Network connected computers and network assets of Tri-Services Organisations located within Delhi, based on orders of MO Directorate.

(b) Analysis of malicious code associated with Malware.

(c) Identify Cyber threats and implement/ advice suitable mitigation measures.

(d) Coordinate with CERT-In and Tri-Services CERTs, and issue Cyber alerts/ advisories on cyber threats.

(e) Conduct Cyber Forensic examination of digital evidence on receipt of orders from MO Directorate.

(f) Carry out vetting, testing and evaluation of all IT projects/ web applications of the IA from cyber security point of view.

(g) Cyber Security vetting of websites/ web applications/ Tactical C3I applications proposed to be hosted on the Army Data Network/ Local Area Network.

(h) Undertake Remote Vulnerability Assessment/ Penetration Testing (VA/ PT) of IA networks.

(j) **Computer Emergency Response Team – Army (CERT-Army)**. CERT-Army under Army Cyber Group will be responsible to coordinate all activities related to cyber security and incident management. It will act as the nodal agency for incident reporting and response within the IA. CERT-Army will also be the nodal agency to coordinate all activities during any cyber-crisis, as specified in Army Crisis Management Plan-2013. CERT-Army will coordinate with CERT-India and leading security agencies of the country/ Original Equipment Manufacturer (OEM) for vulnerability analysis and incident management in the IA.

15. **DG Signals**. DG Signals is the custodian of the ADN and will be responsible for the following aspects related to the security of ADN: -

(a) Establish, operate, maintain and undertake security and access management of the ADN from Central Data Centre (CDC) up to (but excluding) terminal-end equipment (Refer Paragraph 9 (a) of Convergence Directive issued vide DGMO/MO-11 letter A/12314/Convergence/MO-11 dated 27 Sep 14 and Paragraphs 13 and 24 of Communication and Information System Directive 2015 issued vide DGMO/ MO-10 letter A/90222/MO 10/74 dated 16 Nov 15).

(b) Establish Central and Regional Network and Security Operations Centres (NSOCs) for functions related to management and security of ADN. (Refer Paragraph 9 (a) of Convergence Directive).The procedure to establish, operate and manage NSOCs at various levels along with recommended tools/ software required to be used in NSOC must confirm to Guidelines laid down by DG Signals.

(c) Management of Bandwidth and Internet Protocol (IP) addresses on the ADN with domain configuration up to the terminal equipment (Refer Paragraphs 15 (b) and 15 (d) of Convergence Directive and Amplifications/ Clarifications to Convergence Directive issued vide MO 11 Note A/12314/ Convergence/ MO 11 dated 25 Nov 14).

(d) **Identification and Standardisation of Pan- Army Operating System**. Central procurement and administration of security and updation software (Operating System/ Antivirus updation) on ADN. (Refer Paragraph 2 (a) of Amplifications/ Clarifications to Convergence Directive issued vide DGMO/ MO-11 Note No A/12314/ Convergence/ MO 11 dated 25 Nov 14).

16. **Directorates of IHQ of MoD (Army)**. As per requirement, establish/ maintain and secure exclusive Local Area Network (LAN) for the Directorate, not connected to the ADN and nominate a network administrator for undertaking network management, inventory management and security functions at the network level on the LAN.

Cyber Security Structure: Command HQ and Below

17. **Responsibility of Cyber Security at Various Levels**. Commanders at all levels are responsible for execution of Cyber Defence functions to ensure fool proof Cyber Security. Commanders will execute Cyber Defence functions through the following GS appointments:-

(a) **Command HQ**. BGS (IW).

(b) **Corps HQ**. Col GS (IW).

(c) **Division HQ**. Col GS (Ops).

(d) **Area HQ/ Sub Area HQ**. Col GS.

(e) **Brigade HQ**. GSO-1 (Ops).

(f) **Unit**. Nominated Cyber Security Officer.

18. **Nomination of Cyber Security Officer**. Formations/ Units will nominate Cyber Security Officer to ensure implementation of Cyber Security policies and guidelines.

19. **Responsibilities of Formation GS (IW)**. The responsibilities entrusted to the GS(IW)/ GS (Information System) Branch are specified in the **Directive for Convergence of Information Warfare, Information System and Communication Technology Functions/ Organisations to Enhance Operational Effectiveness of the Indian Army issued by DGMO (MO – 11) issued vide DGMO/MO-11 letter No A/12314/Convergence/MO-11 dated 27 Sep 14**. Responsibilities of Formation GS (IW) are as under:-

(a) All staff functions related to Cyber Defence.

(b) Cyber Security audit, both internal (for own HQ) and external (for subordinate HQ and units) including Communication Centres and Network and Security Operation Centre (NSOC) and Cyber Forensic functions, where applicable. Conduct of audits has been amplified in Part IX of this document.

(c) Timely dissemination of advisories issued by the CERT-Army/ other agencies to lower formations and units under jurisdiction.

20. **Responsibilities of Formation GS (Information System)**. Responsibilities of Formation GS (IS) are as under:-

(a) As per requirement, establish/ maintain and secure formation exclusive Local Area Network (LAN), not connected to the ADN.

(b) Management of Internet connectivity and ensure security over the same within the Formation HQ.

(c) Implementation of GS policies on Information System and IT.

(d) Coordination of information management issues within the formation.

(e) Operate/ maintain Operational Information System (OIS)/ Management Information System (MIS) applications at the Formation HQ.

(f) Nominating a network administrator for undertaking network management, inventory management and security functions at the network level for all networks other than the ADN to include any formation/ branch LAN and civil internet.

21. **Responsibilities of Formation Signals**. Formation Signals will be responsible for the following:-

(a) Establish, operate, maintain and undertake security and access management of the ADN up to (but excluding) terminal end equipment.

(b) Establish Network and Security Operations Centres (NSOC) for functions related to management and security of ADN.

(c) Management of Bandwidth and IP addresses on the ADN within the formation AOR with domain configuration up to the terminal equipment.

(d) Undertake cyber security audits on directions of Formation GS Branch till dedicated organisations for the purpose are raised.

(e) Nominating a network administrator for undertaking network management, inventory management and security functions at the network level for the Army Data Network.

Security of Cryptographic Systems/ Keys

22. The responsibilities for acquisition and deployment of cryptographic system will be as follows:-

(a) **DG Signals**. Cryptographic systems on backbone, strategic, tactical & access networks, and applications to be fielded on ADN.

(b) **DGIS**. Tactical C3I Applications/ Projects steered by DGIS, including Indian Army Information System (IAIS).

23. DG Signals/ Signals-3 will be responsible for key management for all cryptosystems in the IA. The responsibility for operation and safe custody of cryptographic system and keys issued to formations/ units/ establishments/ users will be that of formation/ unit commander/ user.

Training and Awareness

24. **Training**. Commanders will ensure that personnel are sent for various training courses, whenever detailed. Formation HQ will ensure that adequately trained Officers/ JCOs/ OR are available at all times for handling cyber security issues. Sufficient provisions for outsourcing cyber training through IT PPP have been laid down by DGIS, the same should be judiciously utilised by all concerned.

25. **Awareness**. Commanders at all levels will make concerted efforts to raise the level of cyber security awareness and inculcate good cyber hygiene amongst all users. In addition, Cyber Security Awareness should be included in Sainik Sammelans, roll calls and unit training curriculum, especially for clerks and individuals handling IT assets. It is imperative that families of all ranks be adequately sensitised on cyber security issues devolving upon social media and IT assets connected to internet including smart phones. Lessons learnt from cases on breach/ violation of cyber security should be discussed to enhance not only knowledge and awareness but also to highlight the necessity of strict implementation of ACSP.

PART II: BASIC CYBER SECURITY ISSUES

Standard Operating Procedures (SOPs)

26. SOPs will be formulated to assign responsibility and accountability for implementation and monitoring of all cyber security measures. The SOPs will be in consonance with the ACSP as well as guidelines/ advisories issued by MO Directorate and Army Cyber Group from time to time. An indicative list of SOPs is given below: -

(a) Maintenance of air gap while using intranet to include data transfer to/ from internet.

(b) Conduct of internal and external cyber security audits.

(c) Repair and maintenance of IT hardware.

(d) Network access control and log monitoring.

(e) Use of smart phones in official premises/ operational/ training areas.

Physical and Environment Security

27. **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.

28. **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.

29. **Protection from Environmental Threats**. Precautions against fire accidents, lightning and all other types of natural or man-made disasters will be taken. All data processing facilities and complexes will be equipped with adequate Fire Fighting (FF) systems, automatic smoke detectors and temperature monitoring sensors to prevent accidents. Backup of important data should be taken at regular intervals and stored securely to safeguard critical data in case of any eventuality. The data backup must be taken on Network Attached Storage (NAS) Drives or optical media like CDs/ DVDs. NAS are Ethernet based mass storage devices which interface the PC/ network securely through the network cable and not the USB port. Use of NAS Drives is authorised in the IA.

30. **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.

31. **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 centralised communication and IT premises. Internal cyber security checks should entail periodic physical inspection of cables to detect tampering at all levels.

Asset Management

32. **Inventory of Assets**. Inventory of cyber/ IT assets and infrastructure must be prepared and updated periodically by Cyber Security Officers and Network Administrators at all levels. Updated inventory list of all cyber assets will be checked during cyber security audits.

33. **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),NAS Drives, 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. Responsibility of physical security of IT assets installed by formation Signals in any unit/ directorate would be of the respective unit/ directorate.

34. **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. Explicit authority to specified persons must be issued for use of these devices and a periodic check of accounting procedure undertaken. Cyber security audits must ensure a comprehensive check of all related security aspects.

Equipment Maintenance and Repair

35. Equipment will be properly maintained to ensure its continued availability in a secure manner. Before sending a computing device/ MFD for repair or maintenance, all storage media like hard disks, CDs/ DVDs, printer cartridges etc will be removed from the computer and stored safely. Inbuilt persistent storage memory e.g. Static RAM existing within certain MFDs need to be deleted by resetting the equipment to default state prior to being forwarded for external repair. 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 the outer label containing the serial number may be shared with the vendor. A clause to this effect will be included in Request for Proposal (RFP) of all projects. In case of mobile computing devices, the secondary storage media will be removed prior to handing over of the device to the repair agency.

36. **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

37. **Ban on Universal Serial Bus (USB) Based Storage Media**. Use of removable USB based storage devices is banned within the IA. 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 the purview of this ban. Such devices will neither be procured nor be held by any office. A prior clearance/ waiver of the MO Directorate will be obtained for projects which envisage procurement of mob phones/ PDAs as part of overall projects. Waiver is accorded to on-going central projects like ACCCS/ MCCS which have in built security controls.

38. **Usage of Personal IT Devices Including Digital Cameras and Video Recorders**. Use of personal IT devices like personal laptops/ computers within official networks (ADN and civil official internet) and processing of official data on personal devices is prohibited. Personal cameras, audio and video recorders including those which are in-built in IT/ mob devices, are not allowed to be used in the office premises/ training areas/ operation locations of IA. However, for official purposes, official digital cameras, laptops and video recorders can be authorised by

an officer not below the rank of Colonel/ Lt Colonel (CO/ OC Unit) for use. The following conditions need to be adhered to strictly, while using such devices for official purposes: -

(a) Responsibility of handling the digital cameras/ laptops/ video recorders should be assigned to a nominated person.

(b) An exclusive standalone computer will be earmarked for plugging the camera/ video recorder and downloading of data. Updated antivirus must be installed on the computer for scanning downloaded photos/ videos. The downloaded data will then be transferred to any other computer by using a DVD/ CD. Care should be taken that no classified/ official data is stored or processed on this computer. Use of a separate Sanitisation Box (details given at Paragraph 57(f)) for scanning the data including photos/ videos going to be uploaded on official networks must be ensured.

(c) The digital camera/ video recorder should be connected only to the designated standalone computer, mentioned above. Under no circumstances will it be connected to any other computer, connected to ADN or civil internet.

(d) The digital camera/ video recorder or its memory card should not be sent to any civilian photo studio or to any person working in civil domain. Photos or videos if required to be printed from civil, must be burnt on DVD/ CD and sent to designated photo studios.

(e) Storage devices of these digital cameras or video recorders should be used exclusively for storage of digital media (photos/ videos) only. Under no circumstances should these be used to store or copy any other official data/ document.

(f) In case of COTS Laptops which have inbuilt video camera, the camera will be disabled using BIOS/ OS settings and hardened as per the CERT-Army advisory. These laptops would be used only as a standalone device and will not be connected to any network including civil internet.

39. **Exclusivity of Storage Devices**.

(a) Internal hard disk drives or external storage devices like NAS Drives will be exclusive to a computer/ network. Sharing of these storage devices between stand alone, isolated LAN computers, ADN or internet computers is strictly forbidden. Sharing of internal hard disk drives and NAS Drives between ADN and internet computers constitutes an air gap violation.

(b) In case information/ content needs to be transferred from Internet to ADN/ LAN/ standalone official computer, it should be done using an optical media. The content/ information of the optical media will be scanned with an updated antivirus software deployed in a Sanitisation Box (Para 57 (f) refers).

(c) The transfer of data to the computer on ADN/ exclusive formation LAN or a standalone official computer will be undertaken post sanitisation of the media. Such optical media should be formatted prior to its further use on internet computers.

(d) Transfer of unclassified (UNCLAS) information from official to internet computer should be restricted to bare essentials. This transfer of UNCLAS data should be undertaken under the direct supervision of an authorised officer after requisite sanitisation of the data has been ensured. On the internet, exchange of UNCLAS data or interaction with civil agencies must only be made on NIC e-mail.

Handling and Management of Classified Information

40. **Information Classification**. Information in digital form will be classified as per CHCD-2001. Security classification of a digital document needs to be mentioned in a bold font on top and bottom of the page and wherever possible use of water marking should be adopted to indicate the security classification and ownership of the document. In certain cases, it may not be feasible to specify security classification in the document itself like in case of presentations, excel sheets and automated reports. In such cases, security classification should be clearly indicated on the outer surface of the storage media and handled accordingly.

41. **Classified Information in Digital Form**. Computers/ equipment (including printers) or storage media used for processing or storing documents of classified nature (RESTRICTED/ CONFIDENTIAL) must be under the ownership of a person of rank/ designation as specified in CHCD-2001. A separate record of copies printed or stored on Optical Media/ NAS will be maintained. All details like originator and owners of info, Number of copies and page numbers as mandated by CHCD-2001 must be recorded. Details regarding handling information of RESTRICTED/ CONFIDENTIAL nature are as follows:-

(a) **Restricted Information**. Information having a security classification of RESTRICTED should be processed over pre-designated computers only. This information should be stored in an encrypted form using tools like VeraCrypt and Secure Desk. These designated computers may be connected over the network like (ADN or LAN) however, users must ensure adoption of requisite end point and network security controls. RESTRICTED documents can be transacted over a network in an encrypted format through secure emails or SFTP.

(b) **Confidential Information**. Documents with security classification as CONFIDENTIAL must be created/ stored/ processed only on standalone computers or computers which are part of an air-gapped secure LAN. All documents of CONFIDENTIAL classification, when stored on computers, will be encrypted using encryption software like Secure Desk and stored in secure data vaults created using software like VeraCrypt. Documents will be erased/ deleted securely only by using software like Eraser or Secure Desk 2.0.The secure LAN must adhere to the following norms:-

(i) The standalone LAN configured must be configured using a well engineered network topology with dedicated manageable switching elements. The switches must be kept locked preferably within an office room and their placement within common corridors accessible to unauthorised personnel should be avoided. All unused ports of the switches must be blocked physically and logically. In addition, the cabling must be laid out in a way to obviate any tampering.

(ii) All computers connected to a specific switch must be located in the same building, preferably limited to adjacent rooms only. To connect users separated by a distance in different buildings, separate switches should be placed and requisite VLAN engineered to secure the requisite connectivity between the distant switches.

(iii) The LAN must be physically separated/ air gapped from any other network.

(iv) IP Sec must be enabled on the LAN.

(v) The entire network must be MAC and IP bound.

(vi) Only authorised applications shall be installed on the network/ computers. The computers must not host any personal/ unauthorised data.

(vii) The Operating System and Antivirus shall be updated at all times using the offline updates hosted on CERT-Army/ AHCC website. Only genuine Operating System and software shall be used.

(viii) Data transfer within the LAN will take place through email service configured over the LAN or through secure protocols like SSH, SFTP etc.

(ix) CD/ DVD writer for data transfer from the LAN must be kept under supervision. The data must be burnt from a pre-designated computer only.

(x) Use of two-factor authentication for access control for computers holding data of CONFIDENTIAL nature is recommended.

(xi) Data backup in an encrypted form must be stored periodically on a NAS Drive/ CD/ DVD.

42. **TOP SECRET and SECRET Information in Digital Form**.

(a) Computers, accessories (including printer) and storage media used for processing or storing TOP SECRET and SECRET documents must be under the ownership of an officer of rank/ designation as specified in CHCD-2001.

(b) Separate records of copies printed or stored on CD/ DVD or any other authorised external storage media will be maintained. All details like originator and owners of information, number of copies and Page Numbers as mandated by CHCD-2001 must be recorded.

(c) Standalone computers will be used for creating SECRET and TOP SECRET documents. TOP SECRET and SECRET information in digital form will not be stored permanently on a computer. All such documents will be securely erased using secure erasing software like Eraser or Secure Desk 2.0 after printing required number of copies or taking backup in an encrypted CD/ DVD media.

(d) Use of two-factor authentication (like use of password alongwith biometric identification system) for accessing the computers used for creating/ processing data of SECRET/ TOP SECRET nature is mandatory.

43. **Transfer of Classified Files on AWAN**. AWAN is an application developed to handle messages having security classification up to CONFIDENTIAL. The AWAN computer must be partitioned ab-initio to create a secure drive/ vault using software like Vera Crypt. This drive would be used to temporarily store the downloaded files from AWAN. AWAN will be used as follows:-

(a) All CONFIDENTIAL messages without attachments will be typed directly into the AWAN application.

(b) RESTRICTED files sent/ received as AWAN attachments can be created/ downloaded on AWAN computer itself. However, they will be stored in encrypted form only.

(c) Following procedure will be followed for sending CONFIDENTIAL attachment (document/ presentation etc) over AWAN:-

(i) The CONFIDENTIAL file will be prepared on a standalone/ LAN computer (not connected to ADN).

(ii) This file will then be transferred to the AWAN computer post encryption using a CD/ DVD and attached directly to the AWAN message.

(iii) This file should not be copied/ retained on the AWAN computer and then attached to the AWAN message.

(d) Following procedure will be followed for downloading a CONFIDENTIAL attachment received through AWAN:-

(i) Such attachments will be downloaded on a secure encrypted drive/ partition on the AWAN computer.

(ii) These files will be transferred in an encrypted form through a CD/ DVD to the standalone computer for further processing.

(iii) The ibid data will then be securely deleted from AWAN computer.

44. **Secure Transfer of Information**. Information owners will ensure that the security classification of the information required to be transferred over a network confirms to the security classification of the network/ media. No information will be transferred over any network/ media if its security classification is higher than the security classification of network/ media. Summary in the form of Information Handling Matrix is placed at **Appendix B**.

45. **Reporting Loss of Soft Copies of Documents**. Classified document in its soft form, if lost, will be treated as loss of document in physical form. All actions will be taken as specified for loss of documents in CHCD - 2001 and Army Act.

Unauthorised Possession of Information/Data

46. **Handing/ Taking Over by All Ranks**. All ranks 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 by Commanders at all levels. The under mentioned certificate will be added in the Handing/ Taking over Certificate of all Officers and JCOs/ OR 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.

47. **Annual Certificate**. The following certificate will be furnished by the CO/ OC/ Head of all formations/ units/ establishments to their higher HQ on an annual basis:-

"It is certified that I have cautioned/ informed all personnel under my command against storing/ possessing unauthorised/ classified data in soft copy format and have obtained an undertaking from each individual to this effect."

48. **Certificate on Termination of Courses**. The under mentioned certificate will be added in the clearance certificate of all students on termination of courses at Training Establishments:-

"I am not carrying any classified/ unauthorised information/ data other than officially issued by____ (Training Establishment) in either soft/ hard copy format."

Handling of e-Learning Material

49. e-learning material is recommended to be accessed on official PCs/ Laptops which are **never used over the internet**. Personal computers, laptops or any such device used for accessing/ studying e-learning material issued by training establishments, will not be used to access internet. Personal computers, if used for running e-learning CDs must be formatted prior to being connected to the internet. Access of e-learning material and internet alternatively on the same device is prohibited. Security of e-learning training material must be ensured by the individual user.

Change Management

50. All changes in hardware, software and their configuration will be duly analysed, approved 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. Cyber Security being a command responsibility, authority for permitting formatting, recovery or repair of such systems would be as under:-

(i) **Directorates/ Branches at IHQ of MoD (Army)**. Officer nominated by head of Directorate/ Branch (not below ADG level).

(ii) **Command HQ**. MGGS.

(iii) **Corps HQ**. COS.

(iv) **Division HQ or Equivalent**. Deputy GOC.

(v) **Brigade HQ or Equivalent**. Brigade Commander.

(vi) **Unit**. CO.

(vii) **Other Organisation/ Group**. Head of the Organisation or Group/ Deputy In charge of Organisation or Group not below the rank of Colonel.

(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.

(c) **Change from Internet to ADN or Vice Versa**. Computers connected to the ADN should not be shifted for use over the internet and vice versa. In exceptional cases where the shifting of computer is unavoidable, explicit permission will be taken at appropriate level as specified at Paragraph 50(a) above and sanitisation of the computer as per CERT-Army Advisory 03/2015 must be ensured.

51. **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.

52. **Segregation of Duties**. Duties and Areas of Responsibility while handling digital assets will be segregated to reduce opportunities for unauthorised or intentional access, modification or misuse of the information within an organisation.
Security controls should be adopted which ensure that all digital assets are accounted for and ownership assigned. The responsibilities should be delineated in a manner such that accountability can be fixed in case of a cyber breach. The following violations shall be construed as major cyber security violations:-

(a) Air Gap Violation.

(b) Use of USB based storage devices, mob phones and internet dongles on official computers.

(c) Unauthorised formatting of computers.

(d) Official data on internet facing computers.

PART III: DESKTOP SECURITY

Hardware Security Management

53. **Hardware Management**.

(a) **Inventory Management of IT Assets**. Inventory of IT hardware and devices will be maintained by Cyber Security Officers and Network Administrators at all levels. 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 the equipment by respective unit/ establishment.

(c) **Backup and Storage of Data**. To prevent loss of data, backup of data and system settings should be taken periodically. Backup media to be stored in a secure water and fire proof safe to safeguard against any natural disasters.

54. **Authentication and Access Control**.

(a) Password or passphrase based authentication and access control will be implemented on all systems.

(b) A strong and effective password requires complexity. Passwords will be minimum 10 characters in length and should have a mix of alphanumeric and special characters.

(c) To protect against unauthorised physical access, user will lock the system using screensaver, login and system (BIOS) password.

(d) All users should shut down the system when leaving office premises.

(e) No ordinary user should be permitted to access/ open hardware devices except Network Administrator.

(f) Classified and critical systems should have two or three factor authentication (including biometric authentication) to restrict access by unauthorised personnel. Two factor authentication for PCs handling important data will be implemented as follows: -

(i) **TOP SECRET/ SECRET Data**. Mandatory.

(ii) **CONFIDENTIAL Data**. Preferred.

55. **Security Measures**. Features like camera, Wi-Fi, voice recording, Bluetooth, GPS and geo-tagging will be disabled on all official devices like Computers, Laptops and Tablets. Cordless mouse, keyboard and presenters are however allowed to be used. Keyboard - Video - Mouse (KVM) Switches are banned from use on desktop PCs to switch between PCs connected on different networks like ADN or civil internet. However, the same are allowed to be used to access servers like Web Server or Mail Server etc. when the servers are connected on the same network. KVM switches can also be used to toggle and monitor multiple logs of the same network in a NOC/ SOC/ System Room by Network Administrators. This would prevent any possible breach of air-gap as all devices connected to the KVM switch essentially would belong to the same network.

56. **Security of Computer Accessories**. Poor Asset Management of computer accessories increases possibility of information leakage. Commanders will ensure formulation of SOPs for handling and use of document replication devices like printers, photocopiers and scanners. Entry Register will be maintained for each document replication device to ensure proper usage.

Software Security Management

57. **Software Security**. Software includes OS (like Windows/ LINUX), applications and custom developed software like Microsoft Office, Adobe Acrobat, Secure Desk, HRMS etc. While operating procedures and security measures are different for different software, following security issues will be implemented for all types of software: -

(a) **Operating System (OS)**. Only licensed version of OS will be used. Users will not install any OS other than that provided by the Network Administrator. Network Administrator and user will ensure controlled access to the OS through hardening of computers and servers. Installation of dual boot/ virtualised OS at user level within official computers is strictly prohibited.

(b) **Application Software**. Users will only use licensed version of application software duly vetted by Army Cyber Group and obtained from authorised sources. Required specific software can be installed on official computers after obtaining permission from Network Administrators.

(c) **Software Updating (Patch Management)**. Using updated versions of OS, security software, applications and Web browsers, is one of the best defence against malware and other online threats. User/ system administrators will ensure that all software is regularly updated with genuine patches. Responsibility for providing latest patches/ updates will be that of the Network Administrator. Non-installation of the Microsoft System Centre Configuration Manager (SCCM) client may cause cyber security vulnerabilities as the operating system and application installed on the computer are not updated with the latest patches/ updates. Necessary steps will be taken to ensure OS patch/ updation of PCs on ADN. Technical assistance from AHCC may be solicited in this regard.

(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. Commanders at all levels will ensure the same.

(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) The Basic Input Output System (BIOS) software installed within all computers/ servers needs to be hardened to ensure that only authorised peripherals are configured. Inbuilt/ onboard devices like internal card readers/ wireless network adapters, multiple network interfaces etc must be disabled. Moreover, the user/ cyber security officer should ensure through the OEM/ service provider that the BIOS software is updated to the latest version. The hardening of BIOS must ensure that options for multiple booting of operating system are not enabled and option to select the same is disabled. Options with respect to chassis intrusion, if available, should be enabled to ensure that any unauthorised access to the internal hardware components of the computer is blocked. Features like 'Wake on LAN' and 'USB Wake' should be disabled. It should be ensured that computers having multiple inbuilt/ onboard network interfaces are configured to activate a single Network interface only.

(ii) Each OS provides several basic and advanced features to the users. These features can be enabled or disabled based on specific services that run in the OS. By default, a number of services automatically start in the computer after installing an OS, thereby, opening a number of ports on the computer. 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.

(iii) Defining policies for password management, file permissions, user security settings, account lockout, auditing etc. are essential components of system hardening. Measures for hardening of Windows and Linux based OS are available on CERT-Army website on ADN.

(f) **Sanitisation**. To ensure sanctity of data ported from internet to ADN/ LAN, following procedure will be followed: -

(i) Data downloaded from internet include patches and updates for the firmware, document, pictures and videos. The downloaded data must be first scanned by an updated version of credible antivirus software on the internet device itself. Thereafter, the data must be copied on an optical media (CD/ DVD) and scanned on a standalone computer with updated antivirus (different antivirus software than the one deployed on internet machine). This arrangement of having an isolated computer with an updated antivirus would be referred to as the Sanitisation Box.

(ii) It must be ensured that a dedicated isolated workstation is deployed to undertake all sanitisation related tasks.

(g) **Adoption of Cyber Security Enhancing Technologies**. The deployment of the Active Directories/ Domain Controller (AD/ DC) within the ADN has laid the bed rock for adoption of cyber security enhancing technologies. Requisite impetus for adoption of similar technologies within the isolated LAN at the formation level must be ensured.

58. **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 provides integrated features like anti-virus, anti-spam, anti-root kits.

59. **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.

60. **Encryption Software**. Encryption provides another layer of security to a user handling classified information/ data. Users should install file and folder encryption software like Secure Desk and Vera crypt for ensuring security of classified information/ data. It must be ensured that Secure Desk, which is an IA proprietary software is not used on internet facing PCs. **Use of Secure Desk over internet may lead to the compromise of the software.**

User Access Control

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

(a) **Privilege Management**. Allocation and use of privileges will be restricted and controlled by Network Administrators. Principle of least privileges will be followed while using systems and services. A user must always log in with user rights and not with administrative rights. In multi-user systems, allocation of user privileges will be controlled through a formal authorisation process. Network Administrator will implement the same thereafter. Administrator accounts should always be managed by Network Administrator.

(b) **Review of User Access Rights**. Access control rules and rights must be reviewed, on required basis, to remove redundant user IDs and accounts.

(c) **Password Management**.

(i) Users will implement multi-level password based authentication and access control. Multi-level passwords refer to Basic Input Output System (BIOS) password, user account login password and screensaver password. Separate passwords for access to encrypted documents and vaults must be created.

(ii) Network Administrators will allocate passwords through a password Management process. Users can have personalised passwords, provided they conform to guidelines of selection and complexity of passwords as given at Para 54 (b) above.

(iii) Wherever feasible, files, databases and applications will be secured using application passwords.

(iv) Access to online servers hosting database or application requiring authentication will have suitable passwords for access.

(d) **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.

(e) **Data Ownership and Responsibility of End Point Terminal**. While DG Signals is responsible for implementing cyber security policies through the implementation of various technologies like Active Directory/ Domain Controller over the ADN. However, the user remains the sole owner/ custodian of data on his 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/ non-encryption of data etc.

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

63. **Unauthorised Data**. Unauthorised data like personal documents, presentations, multimedia files, pornographic content etc. will not be stored within official systems or hosted on official websites.

PART IV: NETWORK SECURITY

Network Management

64. **Types of Networks**.

(a) **Formation/ Unit/ Organisation Local Area Network (LAN)**. A computer network spanning a formation/ unit/ establishment is termed as a LAN. It is an isolated network with no connection to the ADN or any other network.

(b) **Army Data Network (ADN)**. It is the network interconnecting computers across all formations/ units/ establishments in the IA. The ADN will roll out seamlessly over static, deployable and mobile media (radiating and non-radiating) during various stages of operations. It is physically segregated and air gapped from civil internet or any other Govt/ private network/ LAN from security point of view. ADN facilitates access to multiple services/ applications hosted through servers located at formation/ unit/ establishment level. The strength of ADN lies in its exclusivity which must be ensured by users and network administrators. It must be understood that a single breach on ADN has the potential to compromise the entire network.

(c) **Internet**. It is the worldwide interconnected network of servers and computers that facilitates multitude of services, utilities and information.

65. **Responsibility of Network Management**. All networks will have nominated Network administrators with specific tasks allotted for efficient 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. The nominated network administrator will be responsible for ensuring network management, inventory management and security functions at the network level.

Design and Security Features of Networks

66. **Network Design**. The network architecture must logically separate the internal network from the external one. Devices to ensure perimeter defence such as firewalls/ Unified Threat Management (UTM), Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) will be deployed at the network gateway to ensure requisite network level protection. The logs generated by the network security devices must be monitored and analysed regularly for any intrusion/ malware activity. The network must be clearly divided into various zones having specific rule sets applicable to services hosted therein. De-Militarized Zone for web and mail

servers and Militarised Zone (to permit only authorised applications to communicate) for database servers and sensitive software applications should be created with specific access rule sets. Moreover, the network protection device (firewall/ UTM) must be configured to ensure ingress and egress filtering to block unauthorised traffic and generate logs of all activities/ anomalies detected/ blocked. A network based on thin client architecture is required to be secured as per CERT-Army advisory on the subject.

67. **Remote Access of Network**. Remote access to the resources on the LAN side of the network of any formation/ establishment will only be permitted for pre-designated and authorised users only. The privileges granted for remote access need to be restricted to the barest minimum. Permission for such remote access, if required, will be given by authorities as specified at Para 50 (a) of this document.

68. **IP Version 6**. IP version 6 (IPv6) is a new version of the Internet Protocol, designed to replace the current IP version 4 (IPv4). IPv6 solves the problem of IP address space shortages, provides enhanced security support and eliminates requirement for Network Address Translation (NAT). All network devices procured for the IA will be IPv6 protocol compliant for ease of migration to IPv6 subsequently. However, the IPv6 functionality must be disabled on all network and end point devices until the IA fully migrates to IPv6 environment.

69. **Wireless LANs**. Operational considerations at times may necessitate fielding of Wireless LANs in tactical networks. However, current commercial wireless LANs lack adequate security and, therefore, will not be permitted on ADN, or any kind of tactical, administrative or logistic network/ LAN. Use of SAG evaluated encryption algorithms and end systems are mandatory in accordance with classification desired, in case any radiating media is used. However, in exceptional cases due to unavoidable operational requirements, in case wireless LAN is required to be established, waiver be sought from the MO Directorate on case to case basis.

70. **Voice over Internet Protocol (VoIP) Security**. Voice communication through digital networks are subjected to a wide range of security issues, including eavesdropping, call misdirection, identity misrepresentation and information theft using sophisticated technology. Authentication and encryption of data from IP telephones and terminals to servers need to be implemented to secure VoIP communication. Adequate rules in the Network firewalls/ UTM, as promulgated by DG Signals, must be adhered to safeguard the VoIP network from unauthorised access. VOIP devices are required to be secured as per CERT-Army advisory on the issue.

71. **Mobile Devices/ Phones (including Smart Phones and Smart Watches/ Wearable Devices)**.

(a) Mobile/ Smart phones and smart watches/ wearable devices with data connectivity are prone to be exploited for exfiltration/ siphoning of information to remote locations/ servers without the knowledge of the user. Moreover, mobile phones with GPS facilities can be tracked in real time without the knowledge of the user.

(b) The risk posed by the mobile phones is proportional to the various advance features integrated within the device. Inbuilt features like camera, data storage capability (fixed and removable), Bluetooth, Near Field Communication (NFC), Infra-Red port, Wi-Fi and GPS cannot be completely disabled and pose a threat to data and location security.

(c) The integration of services like Short Messaging Services (SMS) provided over GSM/ LTE/ CDMA platforms should not be directly interlinked with the ADN. Applications developed/ deployed over the ADN should not provide functionalities like sending SMS over the mobile networks.

(d) All formations/ establishments will formulate SOPs on the use of such devices within sensitive locations like operation rooms, office premises and in training/ exercise/ operational locations, and the same will be strictly enforced.

72. **Policy Enforcement**.

(a) **Inventory of Software**. The Network Administrator will maintain inventory of all software held within the organisation.

(b) **Integrity Management**. The integrity of system hardware and software files will be maintained and monitored/ tracked to prevent any unauthorised access on the system and networks.

(c) **System and Access Logs**. System and user access logs including administrator activities, system faults, DNS logs and audit logs must be enabled and the data generated should be maintained for a minimum of 30 days to enable auditing, forensic exam and access control monitoring. Hardware to implement central system log servers with retention of logs for a minimum period of 90 days should be planned at all levels.

Network Access Control

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

(a) **Policy on Use of Network Services**. Policy on the use of networks and network services/ resources will be formulated by DG Signals in consonance with the ACSP. The policy must clearly specify the methodology that users need to adopt for accessing authorised networks and network services/ resources.

(b) **Equipment Identification**. The network devices and end point terminals will be configured so as to be able to uniquely and automatically identify the device on a network. The network devices must accept and forward connections only from/ to devices which are identified and bound to it. Default passwords on all network devices like Firewalls, Routers, and Switches etc will be reconfigured and administrator accounts renamed prior to deploying the IT asset for its intended task.

(c) **Remote Diagnostic**. Many information processing setups and systems monitoring agencies are required to conduct remote diagnostics/ access activities. Remote access would be allowed only after the authorised users are provided with mechanisms for ensuring unique identification, authentication and authorisation. Physical and logical access to diagnostic and configuration ports will be disabled by default and any access provided will be controlled and monitored regularly. Remote management of network devices will be done over designated secure communication channels only.

(d) **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.

(e) **Segregation of Networks**. Information systems, users and systems will be segregated by deploying requisite security measures like creation of Zones at the firewall level and Virtual LANs (VLANs) at the network level. Controlled access will be provided based on authorisation and task.

(f) **Network Routing Control**. Routing controls will be implemented within networks to ensure that computer connections and information flows do not breach the access control policy.

(g) **Management of Network Devices**. All network switching devices used for networking must be manageable. Medium Access Control (MAC) and Internet Protocol (IP) binding should be implemented on the same based on the level of intelligence available within the device. All unused ports must be disabled/ blocked within the switches/ routers deployed over the network.

Application Access Control

74. Unauthorised access to software applications including OS will be prevented through the following measures: -

(a) **Access Restriction**. Access to software and related information will be restricted to authorised users only.

(b) **Secure Log-on Procedures**. Access to OS/ software application will be controlled through a secure log-on procedure. Log on credentials will not be transmitted or stored in clear. In case of repeated failed attempts of login, account lockout policy should be implemented to avoid brute force attacks/ unauthorised logins to the OS/ software application. Multi-factor authentication mechanisms based on the principle of **'something you know' (Password, pass-phrase, PIN), 'something you have' (Token, memory card, smart card) and 'something you are' (Biometric devices) will be incorporated for critical systems.**

(c) **Session Time Out**. Inactive sessions will be programmed to shut down after a defined period of inactivity.

(d) **Limitation of Connection Time**. Time synchronisation and time based restrictions will be implemented to provide additional security for high-risk applications.

(e) **Security Classification of Application Software**. The classification of an application system will be explicitly defined and documented by the owner of the application. Use of locally developed/ bespoke applications for hosting of operational data will not be resorted to by the users without clearance of Army Cyber Group. All applications will be duly vetted by the Army Cyber Group from cyber security point of view prior to being hosted.

Database Security

75. **Database Administrator**. A database administrator will be nominated by the application owner who will be responsible for all database functions including managing the authorised user list, access management functions and security of the

data stored in the database. No default roles will be implemented within the data base design. Roles of users will be defined explicitly and allocated by the designated database administrator.

76. **Encryption of Authentication Data**. Authentication/ user credentials stored within all database should be in an encrypted form. Users must be forced (through software design) to change default passwords at the time of initial login. Any default account existing within the database for housekeeping/ testing should be deleted/ blocked explicitly.

77. **Failed Login Attempts**. Logs for all successful/ failed login attempts will be maintained and reviewed on a regular basis. Account lock out policy should be configured for locking the user account after five failed attempts by the user.

78. **Data Security, Ownership and Back Up**. Ownership of data stored within the database will rest with the Database Administrator and the security of data will be ensured by the Database Administrator. There may be instances where the application is able to generate information of much higher significance than the information fed to the database. Responsibility of security of any such information prepared by collating base data will be of the authorised user who is authorised to access the collated/ aggregated information. Back up of data will be taken and tested regularly as per the backup policy of the establishment and criticality of information. Off-site backup should be maintained for sensitive data. For obtaining backups, network based storage device should be connected for minimum duration only.

Security of Servers

79. **Configuration**. Separate servers should be configured to cater for each role i.e. web application, database, authentication, application, etc., wherever possible. All servers will be placed in conjunction with the firewall/ Unified Threat Management (UTM), in separate task specific designated zones as given at Para 66 above. The server must be adequately protected using updated protection software. Formations may resort to virtualisation of Servers as per existing Policy issued vide DGMO/ MO-10 letter number A/900057/8/MO10/92 dated 22 Feb 2013.

80. **Server Hardening**. Server OS and applications must be regularly updated. All non-essential services, applications or protocols enabled on the servers must be removed/ disabled. All unused accounts, default or sample files will be removed by the network administrator. The Servers will be hardened as per the CERT-Army advisory on the subject.

81. **Access Control**. Physical and Logical access to all servers will be restricted and controlled. Network Administrator must change authentication passwords for administrative tools bi-monthly. Default passwords of the administrative tools must be reconfigured.

82. **Anti-Malware and Software Firewall**. All servers will be loaded with software based firewall and comprehensive anti-malware software (antivirus etc). These must be updated and the logs generated analysed regularly.

83. **Ports and Services**. Unwanted services on all servers must be disabled. Open ports/ services should be restricted for intended users only. Perimeter firewalls should enable incoming access on specific IP address and ports being utilised by internal servers for hosting various network based services within the formation (e.g. web, mail, DNS, antivirus, etc). All ports enabled on the formation firewall/ UTM should be bound to specific IP addresses. Hardening of the firewall should be undertaken as per directions issued by DG Signals.

84. **Removal of Accounts/ Content**. All unused accounts/ contents from server will be removed to avoid unintended disclosure of data/ system information.

85. **Application Security**. In addition to security measures specified above, different application servers, like Active Directory/ Domain Controller (AD/ DC), Web Server, Mail Server, etc need to be configured securely based on the applications hosted by them.

86. **Audit Logs**. Audit/ access/ system logs will be enabled within all servers/ systems and these should be analysed periodically. All user and system level audit logs will be retained for duration of 30 days and network administration audit logs will be retained for a period of 90 days. Logs indicating activities of intrusion or attacks will be processed as per policy enunciated in Part IX of this policy.

PART V - ARMY DATA NETWORK (ADN) SECURITY

Defining and Securing the ADN

87. Details pertaining to the scope of the ADN and implementation of security measures over it are as under:-

(a) **Scope of ADN**. The ADN comprises of network elements and end-point devices connected pan-Army over various types of media. DG Signals is responsible for securing and managing the ADN as well as all network elements including formation LANs connected to ADN. All network elements/ formation LANs connected to the ADN will be construed as ADN itself and will confirm to all security rules as applicable to the ADN.

(b) **Securing the ADN**. ADN is a Critical Information Infrastructure of the Indian Army and DG Signals has been mandated to secure the ADN. Some of the mandatory requirements on the ADN which will be checked during internal and external cyber security audits are as under: -

(i) Active Directory/ Domain Controller, SCCM client and end point protection software (Trend Micro) will be implemented on all devices on LAN side of the network by the formation as per the policies given by DG Signals to enforce cyber security policies on end point terminals.

(ii) All computers and networking elements are required to be MAC and IP bound.

(iii) NSOC is required to be implemented at the formation level as per DG Signals guidelines.

(iv) All end point terminals must have a unique IP address confirming to the IP addressing scheme promulgated by DG Signals. Network Address Translation (NAT) or use of private IP address on the ADN is strictly forbidden.

(c) **Access Management on the ADN**. On the LAN side, ADN can be logically separated into Virtual LANs (VLANs) for segregating network traffic and increasing security. Within the VLANs, rule sets can be configured to provide varying degrees of ADN access to users on the network so that some users on the network can be blocked access to ADN with their access restricted to within the formation LAN, while some others can be accorded full ADN access. Inter-VLAN routing will be restricted with strong Access Control List (ACL) defined at the Layer 3 Switch.

(d) **Classified Data Over ADN/ LAN**. Computers on ADN may be used to create/ store documents upto RESTRICTED security classification, provided such data is stored in an encrypted format through secure desk software in secure vaults like VeraCrypt and is transmitted only over the AWAN application. Within a formation/ directorate encrypted RESTRICTED files can also be exchanged over secure email services running within the directorate/ formation or by using secure protocols like SFTP, SSH etc. The isolated LANs deployed within the formations/ units are presently 'UNCLAS' Networks. The security classification of isolated LANs can be enhanced to prevent any cyber security breach with the implementation of requisite cyber security control as enunciated vide Para 41 of the policy.

88. **Services/ Applications on ADN**. ADN offers various services and applications like IA Web Portal, Army Portal e-mail, Digi-locker etc to IA users. An important application running on ADN is AWAN. It must be understood that AWAN is not a network, but a desktop to desktop messaging application running over the ADN. This implies that software for AWAN application needs to be installed on designated ADN computer. User based AWAN tokens are used to provide dual factor authentication for accessing the AWAN application.

89. **Security Guidelines while Using AWAN**. AWAN has been developed to handle information/ data of security classification up to CONFIDENTIAL. This implies that TOP SECRET/ SECRET files will not be transmitted using the AWAN application. Guidelines for sending classification messages/ attachments over AWAN are given at Paragraph 43.

Hosting of Websites/ Web Applications on ADN

90. **Web Applications/ Services**. All web services hosted over the ADN must ensure implementation of cyber security controls like SSH, TLS, HTTPS etc. Policy for creating, hosting and maintenance of websites on the ADN has been issued vide DGMO letter number A/12100/Policy/MO12 dated 01 Feb 2016. This policy regulates establishment of servers, hosting of websites and content hosted therein.

91. **Hosting of Websites/ Web Applications**. Any website/ web application (including blogs, forums, chat servers, in-house application etc.) will be hosted on ADN only after security vetting by Army Cyber Group. The validity of cyber security clearance accorded for websites is for a period of three yrs. Sponsor Directorate/ HQ will also obtain clearance for the content hosted within the website from DGMI/ MI-11. Responsibility of updating these websites/ web applications, thereafter, and security of content, will be that of the Sponsor Directorate/ HQ. In case, an upgrade of the website/ web application is undertaken at any stage, fresh cyber security clearance needs to be obtained from Army Cyber Group.

92. **Intellectual Property Rights (IPR)**. Content hosted within the websites/ web applications hosted over the ADN should not violate any IPR and copyright regulations.

93. **File Transfer Protocol (FTP)**. Use of insecure FTP services within the official IA Networks is not permitted. However, use of Secure FTP (SFTP) services may be configured using network technologies like Secure Socket Layer/ Transport Layer Security (SSL/ TLS) protocols. Access using folder sharing and default shares using Windows Port 445 is not permitted within the official IA Networks. Use of TCP Port 445 and 3389 will be governed by DG Signals instructions on the issue.

Monitoring of ADN

94. **Integrity Management**. Integrity of system hardware configuration and critical software files will be maintained and monitored to prevent any unauthorised activity on the systems and networks.

95. **Analysis of System Logs**. Logs of user activities, exceptions, login failure, faults and information of security events will be analysed periodically and any incident will be reported to formation GS (IW) Branch. The logs will be maintained for a minimum of 30 days to enable forensic investigation and monitoring access. Procedure for monitoring and analysis of logs of network elements, firewalls and DNS Servers should be established as relevant and the results be reviewed regularly.

96. **Monitoring System Use**. Real time monitoring of the ADN at the formation level would be carried out by establishment of NSOCs which would be governed by the guidelines issued by DG Signals. Procedure for monitoring use of information processing facilities will be established and results of monitoring activities will be reviewed regularly. However, use of network penetration tools is not permitted within the official IA Networks without explicit permission of DGMO.

PART VI: INTERNET SECURITY

Extension of Internet

97. The hiring of internet connectivity will be ensured primarily from Govt affiliated Internet Service Provider (ISP) only. In cases, where the Govt based ISPs are unable to provide the requisite service, internet connectivity may be hired from other private agencies in consultation with the local IFA. The extension and securing of internet connectivity will be as under: -

(a) Extension of internet connectivity from the ISP to the premises of user can be undertaken on all type of media (including radiating media like Wi-Max or USB Based internet dongles). The USB Based dongles are required to be used with a modem only and are prohibited from being directly connected to a computer/ laptop, details of technical connectivity are given in the Army Cyber Group advisory on the subject. Subsequent extension of internet connectivity from the modem within the official premises to authorised subscribers will be done over wired media only. Use of Wi-Fi/ other radiating media within office premises is not permitted. As far as possible, number of internet connections should be kept to barest minimum by establishing common terminal for use of internet.

(b) Wi-Fi used within social places like Officers Mess, Institutes, Clubs, Guest Rooms and other recreational places will be subject to approval and adoption of laid down security controls issued from time to time. In general, the Wi-Fi network should not broadcast its ID and must be encrypted using WPA-2 or higher grade of security. In addition, the Wi-Fi coverage be restricted to minimum essential area by positioning the device appropriately and limiting power output. The default username and password of the Wi-Fi routers must also be changed prior to and periodically during deployment.

(c) All internet connected computers deployed in the office premises of various HQ/ units must be installed with a standardised OS 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 at the BIOS/ system level.

(d) A list of users authorised internet connectivity within the office premises must be maintained by the respective Directorate/ Formation/ Unit/ Organisation. This list should be authorised by the competent authority as specified in Paragraph 50(a) above.

(e) Extension of internet from a central point with adequate controls must be implemented within Formation HQ/ Unit, if possible. Such centralised internet connectivity must be secured by usage of Firewalls, UTM at the network level for enhanced cyber security. Analysis of the logs generated by the protection devices must be undertaken regularly by the nominated network administrator.

98. **BOSS OS**. BOSS OS has been developed and further customised for the requirements of the Indian Army by C-DAC, Chennai. As per Policy on Standardisation of Operating System issued vide DGMO/MO-12 letter No A/12100/MO-12 dated 18 Sep 16, all official internet facing PCs of the Indian Army are required to be installed with the customised BOSS OS provided by DG Signals. The BOSS OS is required to be audited as per CERT-Army advisory on the subject. The source code of BOSS OS is proprietary of Indian Army and hence its proliferation needs to be controlled at all levels.

Maintenance of Air Gap

99. Strict air-gap between Internet, ADN and LANs/ standalone computers will be ensured at all times. Due to the technological development, various techniques have emerged allowing malwares to pilfer data from air-gaped network/ devices. Guidelines issued vide CERT-Army Advisory 01/2013 – “Air Gap and Measures to Maintain It”, will be strictly adhered to. The following will be ensured at all times for maintenance of air-gap:-

(a) Computers connected on ADN and Internet should be physically separated to avoid breach of air gap and a min separation distance of 1.5 Metres is recommended. Internet Café be established in a separate room under the supervision of an officer for providing centralised internet access.

(b) Computers connected on ADN and Internet will have clear labelling, marking and colour coding of UTP cables, switches and CPU. Computers once used for official tasks will not be used to access the civil internet.

(c) Computers connected to the internet will be installed with a current, licensed and updated OS along with requisite and updated protection software.

(d) Personal computers or laptops used for accessing internet will not be used for accessing/ studying e-learning material.

(e) Any official internet computer will not be connected to the following devices: -

(i) Mobile phones.

(ii) ‘Plug and Surf’ type of GSM/ CDMA USB MODEMs.

(iii) Wi-Fi/ Bluetooth/ Near Field Communication (NFC) adaptors or dongles.

100. **Zero Tolerance for Use of Pen Drives and Air Gap Violations**. There will be ‘**Zero Tolerance’** towards use of pen drives and incident of air gap violations. The following Cyber Security Creed will be displayed prominently on all computers: -

(a) Pen Drive is a cyber-bomb, shun it.

(b) No official data will be processed or stored on internet PC (for internet PCs).

Prevention of Data Leakage

101. 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 the appointment/ identity of the person/ unit using the 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 the internet will not be installed on official computers. The software like VNC, Team Viewer etc allow remote access of the machine/ data thus, rendering it vulnerable to compromise.

(c) **Gifted Pen Drives**. Instances have come to light wherein civilian vendors have gifted pen drives/ external hard disks/ mobile phones etc as promotional material in various exhibitions/ seminars. On examination of these devices, malware capable of compromising computers/ data was found on these devices. All ranks must be sensitised on this prevalent modus-operandi adopted by hackers/ enemy agents. It is once again reiterated that use of USB based storage devices like pen drives/ hard disks on official computers is prohibited.

Hosting of Websites on Internet

102. **Web Hosting Policy**. Hosting of Websites on Internet is governed by ADG PI letter number A/80013/I/PI dated 26 Jul 2006. Salient aspects of the same are as under:-

(a) All Websites hosted on Internet will be a part of the IA Web Portal. Hosting of independent web sites is not permitted.

(b) Internet based Websites will be hosted on NIC Servers only.

(c) Internet websites will comply with Guidelines for Indian Government Website (GIGW) prepared by National Informatics Centre (NIC).

(d) Security vetting will be carried out by Computer Emergency Response Team – India (CERT-In) empanelled auditors, prior to being hosted on the internet and thereafter on regular intervals not less than twice a year. A list of the empanelled cyber security auditing agencies has been listed on the CERT-India Website ‘www.cert-in.org.in’ as well as the CERT-Army website on the ADN.

(e) Content proposed to be hosted within websites on the internet will be vetted by DGMI/ MI-11 from military security point of view, prior to being uploaded on the internet.

NIC e-Mail Accounts

103. NIC e-mail accounts may be used for personal and official communication of UNCLAS nature only. Generic NIC e-mail IDs will have to be created to facilitate such communication. The policy for creation and use of NIC e-mail IDs has been disseminated to the environment vide DGMO/ MO-12 letter number A/12108/NIC/MO 12 dated 20 Nov 2013 and even number dated 28 May 2015. Salient aspects of the policy are as under: -

(a) **Generic NIC e-mail IDs**. Only generic IDs, that do not reveal the identity or appointment of user, will be used. For e.g. blue_robin, kalpavriksha, etc.

(b) **Nodal Agency in IA for Creation of NIC e-mail IDs**. NIC based e-mail IDs will be created by Army Cyber Group for use in e-procurement/ official tasks. The e-mail accounts created are official in nature and need to be handed over on relief. Ordnance Services Computer Centre (OSCC)/ DGOS has been tasked to create personal NIC based e-mail accounts for all officers of the IA (refer AGs Branch/ PS(3) letter number PC B/25531/AG/PS-3(P) dated 28 Apr 2015).

(c) **Procedure for Creation of NIC e-mail IDs**.

(i) Users will process official NIC based e-mail application as per the prescribed format through Command HQ/ Coordination Section of respective Directorates at IHQ of MoD (Army). These applications will then be forwarded to DGMI/ MI-11 for necessary security clearance.

(ii) Post security clearance, DGMI/ MI-11 will forward these applications to the Army Cyber Group.

(iii) Army Cyber Group will create the NIC based e-mail ID and intimate the same to users on their registered mobile numbers.

(d) **Migration from Appointment based IDs to Generic Name based IDs**. Users in possession of appointment based IDs are required to migrate to generic NIC e-mail IDs as per the prevalent policy.

Access to Social Networking Websites

104. **Social Networking Websites**. Social networking sites like Facebook, Twitter, and public forums, blogs, etc are permitted for private communication in personal capacity only. These platforms have become popular with the Defence personnel for sharing of views, pictures, etc with public/ group/ friends. However, it must be understood that data shared over these sites is inherently insecure and prone to misuse. Detailed security instructions in this regard have been disseminated to the environment vide DGMI/ MI-11letter number A/38024/1/MI-11 dated 03 Oct 2011.

105. **Precautions while using Social Networking**. Following precautions/ measures will be adopted while accessing social networking sites for private use:-

(a) No individual will reveal his personal identity by way of rank, appointment, official address or post photographs in uniform on such networking sites.

(b) A user should not create or join communities/ groups/ e-mail-IDs revealing course, batch, unit, or any affiliation with Indian Army, for e.g. NDA 59, DSSC 50, YO 120, tiger36sikh@rediffmail.com etc.

(c) Users will not create or join any community/ group that is related to terrorism, anti-national elements, political/ religious affiliations etc.

(d) Users will not forward/ originate derogatory messages that may cause embarrassment to the Govt/ organisation/ establishment. In this connection, guidelines issued by DGMI/ MI - 11 vide their letter number A/38024/1/MI-11 dated 03 Oct 2011 and supplement issued on 21 Aug 2014 will be strictly adhered to.

106. **Matrimonial Websites**. Keeping in view the requirement of matrimonial websites, dispensation for revealing limited identity on such sites has been accorded. Individuals can post photo in civil dress only and mention Defence Service as profession, but should not disclose their Indian Army/ unit identity.

107. **Online Polling, Campaigns and Forums**. Indian Army personnel are restricted from participating in any online polling, campaigns, forums, etc related to Armed Forces or Govt of India. Online interaction with media houses, foreign nationals/ agencies/ orgs, retired service personnel on official matters is also prohibited.

108. **Limit Online Exposure**. In order to obviate disclosure of identity online, information pertaining to phone number, address, place of employment, employer details or of military value should not be posted. Individuals with malicious intent attempt to glean available information over the internet and use it to target or harass an individual. Hence, it is prudent to limit access of information to ‘your friends’ only, on Social Networking Websites. All ‘tags’ by public/ friends also disclose identity, hence it is important to remove unwarranted ‘tags’. Geo-tagging (posts ‘tagged’ to/ associated with locations) of military installations/ establishments is prohibited.

109. **Stock Trading**. Use of official communication devices/ computers/ bandwidth for online stock trading or any other online financial activity is prohibited.

PART VII : DEVELOPMENT AND DEPLOYMENT OF INFORMATION SYSTEMS

Authorisation Process

110. Authorisation for acquisition or development of new Information and Communication Technology (ICT) hardware/ software, establishment of networks, Operational Information System (OIS), Management Information System (MIS), Geographical Information System (GIS) projects will take into account all existing cyber security policies/ guidelines before induction and deployment.

Security Issues during Application Development

111. Application development will address all security issues at each stage of Software Development Life Cycle (SDLC) in order to minimise application level vulnerabilities. In addition to the policy on development of software applications, the issues that merit attention are as under:-

(a) **Level of Security**. Based on security classification of the application, network, and data to be handled, the level of security required will be specified clearly and incorporated from the design stage itself.

(b) **Input Data Validation**. Data entered into a database, application or automated system must be validated to ensure its correctness, accuracy and consistency. The validation process must be multistage with role based definition of tasks like data entry, approver, verifier etc.

(c) **Output Data Validation**. Data output from a database, application or automated system must be verified to ensure that the processing of stored information is correct and appropriate.

(d) **Control of Internal Processing**. Validation checks will be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

(e) **Message Integrity**. Requirements for ensuring authenticity and protection of message integrity during processing and transit will be identified and appropriate security measures implemented within the applications.

(f) **Architecture**. It is preferred that to overcome the threat posed by deployment of stubs/ clients on computers in the ADN, all applications being developed for deployment within the Army Network (ADN/ LAN) should be browser based and platform independent. Use of web browser based application is a preferred model to be adopted for all future software application developed as they overcome limitation of specific hardware and software platforms requirements. Requisite application level security needs to be incorporated from the design stage of the application.

(g) **Business Intelligence (BI) Tools**. A number of software applications are being developed where BI tools form an integral part of the overall solution. BI tools, like MISO, collate and present data collected from subordinate entities like units/ formations. While at unit level, such data may have limited operational value, collated data bears operational significance. To restrict the access to collated BI information in all such applications hosted over the network, a minimum of two factor authentication must be implemented.

Security of System Files

112. **Access to Programme Source Code**. During the process of software development, access to programme source code and associated designs, specifications, verification and validation plans etc will be strictly controlled. This will be done to prevent introduction of unauthorised functionality, back-doors and unintentional changes.

113. **Protection of Test Data**. During software development the test data will be carefully selected and protected. Military marked maps/ classified information should not be used as test data or copied on storage media of the vendor.

Security in Development and Support Processes

114. **Control Procedures**. Introduction of new systems and major changes to existing systems will be properly documented. This will ensure that existing security and control procedures are not compromised.

115. **Technical Review of Applications**. Measures will be instituted to ensure that the application executes only tasks that it is designated for.

116. **File Integrity**. Integrity check for OS and all application software will be implemented. This will ensure that the software and subsequently its upgrades do not modify any of the other installed software/ OS pre-existing within the device.

117. **Controlling Non-Essential Services**. The application should not enable default services that are not required for the functioning of that application.

118. **Authorised Software**. Only authorised and licensed software will be used ensuring their regular updation/ patching. No development stack (eg XAMPP) will be used in the production model to host a live application due to lack of security features.

119. **Outsourced Software Development**. Outsourced software development will be supervised and monitored by the concerned establishment. The IPR of the

software so developed will be centrally held by Army Software Development Centre (ASDC)/ DGIS (earmarked as the Central Repository for all software products) post completion of the project. This aspect will be prominently highlighted in the RFP as well as in the contract agreement undertaken with the vendor/ Original Equipment Manufacturers (OEM). Hosting of software developed by third party will be governed by DGMO/MO-12 letter number A/12108/CS/MO-12 dated 26 Nov 2015.

120. **Embedded Software**. While procuring hardware and software, Original Equipment Manufacturers (OEM)/ Licensed Software suppliers will certify that the product being supplied is free from embedded/ malicious hardware and software. Source codes for the embedded software should be made available and incorporated as part of contract while procuring systems, wherever feasible.

Security Vetting of IT Projects

121. Comments of Army Cyber Group will be obtained in respect of the SDLC right from the conception stage. The Request for Proposal (RFP) will only be issued by the user to the vendor post cyber security vetting by Army Cyber Group. All IT Projects undertaken for deployment on the ADN and those sanctioned out of IT Fund will be vetted by Army Cyber Group from cyber security perspective. List of all IT projects/ applications/ websites vetted/ being vetted by Army Cyber Group will be hosted on the CERT-Army website for reference.

Acquisition and Development of Cryptographic Controls

122. **Policy on Cryptographic Controls**. Govt of India Crypto System Acquisition Policy and Cipher Policy Committee (CPC) guidelines will govern acquisition and development of cryptographic controls.

123. **Certifying Authority and Key Management**. DG Signals will function as Controller of Certifying Authorities (CA) in the IA. Suitable policy addendum will be issued by DG Signals as and when Root Certifying Authority for the Indian Army is established.

Third Party Service Delivery Management

124. Civilians, if employed/ hired on/ for IA Software development projects, would be subjected to strict Service Level Agreements and Non-Disclosure Agreements with penalty clauses. Non-military agencies can be involved only in case of provision of installation, training and repair, but not for administration and operation of installed networks. The user agency will ensure periodic Military Intelligence clearance of all civil resident engineer employees required for continued technical support for certain highly technical ICT systems.

PART VIII: INCIDENT MANAGEMENT AND FORENSICS

Incident Reporting and Handling

125. **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.

126. **Incident Reporting**. All cyber security incidents will be reported to CERT-Army through the respective IW/ GS Staff at various levels. Any major cyber incident or a suspected targeted attack will also be reported to MO Directorate directly. All relevant details must be reported to facilitate investigation or mitigation of the incident. Format for reporting the incident is available on the CERT-Army website as 'Incident Reporting Form'. Reporting of cyber incidents to CERT-Army can be done through any of the following means:-

(a) **AWAN**. AWAN address of Army Cyber Group and DGMO/ MO-12.

(b) **Telephone**.

(i)	**DGMO / MO 12**.	33478, 33173.
(ii)	**CERT-Army**.	39707, 011 - 25691530 (Civil).

(c)	**Fax (CERT-Army)**.	011-25691530 (Civil).
(d)	**E-mail(CERT-Army)**.	certarmy@nic.in.

(e) **Malware Analysis (Malicious E-Mail Received Over Internet)**. sendmalware@rediffmail.com.

127. **Incidents Involving Loss of Official/Classified Information**. Such incidents will be reported through proper channel as per the existing procedure given at Paragraph 142 of CHCD-2001.

128. **Nodal Agency for Coordinating Incidents**.

(a) Respective commanders will be responsible for coordinating all activities related to incident reporting and subsequent investigation, if required.

(b) Army Cyber Group (CERT-Army) will be responsible for coordinating all activities regarding computer security incidents/ emergencies such as limiting their spread and initiation of mitigation actions.

(c) Detailed guidelines on the subject have been issued separately as part of Army Crisis Management Plan - 2013.

Cyber Forensic Investigations

129. **Forensic Lab at Army Cyber Group**. Cyber forensics of digital evidence is required to be conducted on occurrence of a cyber security breach, in such a manner that it is tenable in a court of law. Forensic Lab at the Army Cyber Group carries out forensic analysis in the IA and has been accredited as 'Examiner of Electronic Evidence within Indian Army' under Section 79A of IT Act 2000 and IT (Amendment) Act 2008. This implies that forensic analysis undertaken by Army Cyber Group is admissible as evidence in courts of law.

130. **Actions by Formations for Seeking Forensic Investigation**.

(a) **Intimation of Cyber Security Breaches**. Cyber security breaches like loss of classified information or compromise of a computer are normally reported by following agencies: -

(i) Intelligence agencies like IB or DGMI.

(ii) Formations.

(iii) Army Cyber Group (CERT-Army).

(b) **Actions to be Undertaken**. In order to identify the likely source of breach/ leakage of information for facilitating subsequent forensic investigation, actions to be undertaken at formation level are as under: -

(i) Reporting of the incident as per Paragraph 126 above.

(ii) Conduct preliminary investigation to ascertain the degree of cyber security breach/ loss of data by convening Board of Officers (BOO)/ Court of Inquiry (as applicable).

(iii) Based on the degree of breach and recommendations of BOO/ C of I, if further legal action is warranted then the digital evidence be seized and forwarded for forensic analysis to Army Cyber Group, as per procedure given in Paragraph 131. Otherwise, the case be disposed at formation level with intimation to DGMO/ MO-12. The seizure of digital evidence can be undertaken by the same BOO / Court of Inquiry as mentioned at Sub Para (ii) above and necessary instructions may be included in the initial convening order itself.

131. **Permission for Forensic Investigation**. Having initiated the C of I and seizure of the digital evidence, the need for forensic investigation will be established prior to seeking permission for the same. The permission for undertaking forensic investigation will be sought by Command (IW) Branch/ Directorate of IHQ of MoD (Army) from DGMO/MO-12. The request for forensic investigation will be sent along with a brief of the case. The brief will give out aim of the investigation and relevant background. Permission to undertake forensic investigation will be accorded by MO Directorate.

132. **Instructions for Seizure and Submission of Digital Evidence**. Detailed instructions for seizure of digital evidence have been promulgated in Advisory 03/2013 on 'SOP for Handling for Cyber Security Incident Requiring Forensic Analysis' issued by CERT-Army vide their Letter number B/51084/ArCyGp/T-3 dated 30 May 2013. Advice on technical aspects regarding seizure of evidences can be sought from CERT-Army on as required basis to ensure legal tenability of the evidence submitted. Salient aspects to be kept in mind while seizing and dispatching the digital evidence to Army Cyber Group are summarized as under:-

(a) A BOO having reasonable understanding of computers will be ordered for the purpose of seizing the suspected digital evidence.

(b) Digital evidence will be properly documented, photographed, labelled and inventory prepared before being sealed and packed as per procedures.

(c) Details of chain of custody of all the evidence will be maintained, as per prescribed format given in the Army Cyber Group SOP on the sub. 'Chain of Custody' form is a legal document, hence it is mandatory for BOO to obtain signatures of owner of the seized digital evidence during seizure process. The requisite forms required to be provided for submission of digital evidence can be downloaded from the CERT-Army Website.

(d) The digital evidence will be protected from heat, humidity, magnetic fields, shocks or vibrations during storage and transportation.

(e) The digital evidence will be dispatched to Army Cyber Group, only if permission for forensic investigation is accorded by MO Directorate.

(f) **Brief of Case and Questionnaire**. The investigating agency must also submit a brief of the case giving aim of the investigation and relevant background to the Army Cyber Group to assist in cyber forensic investigations. A questionnaire is also required to be prepared for seeking answers to specific requirements of the case.

(g) While handing over digital evidence to Army Cyber Group, 'Hash Signature' of the digital media will be obtained from Army Cyber Group to validate integrity of the evidence.

(h) **Seizure of Mobile Phone**. BOO will ensure that all accessories such as memory card, SIM card and charger is seized and forwarded for forensic investigation along with the mobile devices during the seizure of the evidence.

(j) **Tampering of Evidence**. It should be ensured that the digital evidence is not tampered by means such as ‘wiping’ or formatting or replacement of storage media by the owner before seizure. Seizure BOO should ensure that the digital evidence is not tampered with during and after seizure.

(k) **Passwords**. The seizure BOO should ensure that the owner of the digital evidence provides relevant passwords for the seized device and they should be mentioned in the brief of the case. For computers, passwords such as BIOS, System key, Operating System, Screensaver, Bitlocker and third party encryption, if any, should be provided. For mobile phones, pattern lock, PIN, login and mobile encryption passwords, if any, should be provided.

133. **Actions by Cyber Forensics Laboratory of Army Cyber Group**.

(a) Evidence will be extracted, preserved and analysed by Army Cyber Group using sound forensic practices, to ensure its admissibility in court of law.

(b) The Forensic Analysis Report will be submitted to the DGMO for further action.

(c) The Cyber Forensic Laboratory at Army Cyber Group will retain one copy of the Report. Army Cyber Group will maintain the digital image of the hard disk for a period of 180 days after disposal of the case calculated from the date of signing indicated in the forensic report. This paragraph to be read in conjunction with Paragraph 25 of Advisory 03/2013 on 'SOP for Handling for Cyber Security Incident Requiring Forensic Analysis' issued by CERT-Army vide their Letter Number B/51084/ArCyGp/T-3 dated 30 May 2013.

134. In addition to identification of the cyber threat, pin-pointing cause and damage resulting from the cyber incident, Army Cyber Group and formations will also draw out appropriate lessons. Lessons so learnt from such incidents will be disclosed during User Awareness Training as part of External Cyber Audits.

PART IX: CYBER SECURITY AUDIT AND COMPLIANCE

Cyber Security Audit

135. Cyber Security Audits will be conducted for all formations/ units/ establishments to ensure implementation/ adherence to Cyber Security policies/ guidelines/ advisories issued by DGMO/MO-12 and Army Cyber Group. Standardised tools for conduct of audits will be provided by the Army Cyber Group. The IT assets to be audited by the cyber security audit team as per CERT-Army advisory for each device are as under: -

(a) All computers working on ADN/ LAN/ Internet/ Standalone mode.

(b) Network Attached Storage (NAS).

(c) All switches, firewalls and UTMs.

(d) Servers (Web, Application, Antivirus, Domain Controller etc).

(e) Multi-Function Devices (MFDs).

(f) Asynchronous Digital Subscriber Line (ADSL) modems.

(g) Smart appliances like TVs (Internet of Things (IoT) devices).

(h) Any other IT asset held within premises (including Biometric/ Surveillance setup).

Types of Audit and Responsibilities

136. The various types of cyber security audits to be undertaken are as under:-

(a) **Internal Audit**. These will be conducted by concerned formations/ units/ establishments thrice a year. Out of three internal audits, one audit may be conducted as a surprise audit by the formation/ establishment. Actions taken on the observations raised during the previous cyber security audit to be verified and endorsed in the instant report. Analysis of various network logs will be undertaken as part of the internal audit.

(b) **External Audit**. The External Audit teams at all levels will audit all IT assets as mentioned at Para 135 above. They would be responsible to go through the audit reports of internal audits along with analysis of the logs of network devices, firewalls and servers. The audit logs of Domain Name System (DNS) Server/ firewalls will be made available to the Cyber Audit

Team by the formation/ establishment being audited. The audit team will involve the internal cyber security audit team during the external audit in order to train the internal audit team of the formation. A cyber security awareness lecture will also be conducted during the external audit. The External Cyber Audit will be conducted by various cyber security audit teams on an annual basis. The external audit teams will utilise the latest audit tools which would be updated by CERT-Army on their website on ADN. Details of external cyber security are as under:-

(i) **Army Cyber Group**. Army Cyber Group audit team will conduct external cyber security audit of all Command HQ, Directorates/ Branches under Integrated HQ of MoD (Army) and ADN connected IT assets of Tri-Services organisations in Delhi.

(ii) **'One Up' Formation**. The one-up higher formation is responsible for conducting audit of all IT assets of subordinate formations/ units/ establishments on its Order of Battle.

(iii) **Training Establishments**. External cyber security audit of all Category A establishments would be conducted under the aegis of HQ ARTRAC. Category B training establishments would be audited by the Command HQ on which the establishment is administratively dependent.

(iv) **Tri-Services Establishments**. ADN connected IT assets (including end-point devices and network elements) of all Tri-Services establishments will be audited by the formation responsible for extending the ADN connection.

(c) **Special Audit**. Special cases/ circumstances will mandate conduct of special audit, wherein audit team from the higher formation will be tasked to conduct external audit. Army Cyber Group is the nominated central agency for undertaking special audit of any organisation on directions of the MO Directorate. Cyber audits of official IT assets and networks will not be outsourced to any Govt/ civil/ commercial agency due to security reasons.

(d) **Cyber Audit of IT Assets Deployed within other Defence Ests**. The Formation Commander will ensure that the internal and external cyber security audits of all IT assets deployed within the defence establishments affiliated with the Indian Army like MES establishments, ECHS etc are undertaken as applicable for other formations/ units.

(e) **Composition of Audit Team**. Till such time dedicated Cyber Organisations are raised, cyber security audits would be conducted by teams composed of personnel deputed by IW/ GS Branch at all levels. The formations will ensure the training and empowerment of such teams to enable them for audit.

137. **Audit Logs**. As a policy, logging of auditing controls within all IT systems and network devices will be enabled by default. At the system level, access to audit logs will be restricted to the nominated Cyber Security Officer/ Network Administrator only. All user and system level audit logs will be retained for duration of 30 days and network administration audit logs will be retained for a period of 90 days. Requisite audit logs will be made available to the external cyber security audit team on demand during the conduct of the audit. The responsibility for monitoring of the various logs against existing policy/ guidelines will be defined at the formation level.

138. **Vulnerability Analysis and Penetration Testing (VA/ PT)**. The Army Cyber Group is mandated to undertake VA/ PT of all official information systems and networks. This being a specialised task with implications on end-user data integrity, will not be undertaken by any other formation/ unit/ agency. Thus, conduct of VA/ PT by any other formation/ unit not specifically mandated by the MO Directorate is prohibited and would be construed as a violation of the Cyber Security policy.

Compliance

139. **Information Technology Act 2000 and Information Technology (Amendment) Act 2008**. It is mandatory for all users to abide by all provisions of IT Act 2000 and IT (Amendment) Act 2008 and any violations observed will be prosecutable in a court of law. Salient aspects of the IT Act are given at **Appendix C**.

140. **Intellectual Property Rights (IPR)**. Use of pirated software on computers and hosting of unauthorised/ copyright data such as music, videos, photos, etc on the websites of ADN is in violation of the IPR, therefore prohibited.

Conclusion

141. The ACSP-2017 has been conceptualised to evolve as a document for handling pertinent issues on cyber security. This dimension being extremely vibrant, results in several queries being raised from various quarters requiring immediate attention. Pertinent issues have been discussed in the Cyber Security Forum-2015, collated, a consensus obtained and incorporated in the ibid policy.

142. The policy in its present form provides a comprehensive document defining guidelines for compliance/ adherence in the cyber domain. Adherence to the instructions/ guidelines would ensure a robust cyber security posture. This policy supersedes the Army Cyber Security Policy-2014 (ACSP-2014).

Sd/- x x x x x
(JK Sharma)
Maj Gen
ADGMO(IW)

Case Number : A/12100/Policy/MO-12

Directorate General of Military Operations
IHQ of MoD (Army)
DHQ PO New Delhi-110011

Date: 07 Feb 2017

Distribution:-

All Branches/Directorates of
IHQ of MoD (Army)

All Command HQ GS (IW)
All Corps HQ GS (IW)
All Division HQ GS (Ops)

} - Hard and soft copy of ACSP-2017 will be issued down to Unit/ Training Establishment level.

Appendix A
(Refers to Paragraph 9 of
ACSP-2017)

COMPOSITION OF CYBER SECURITY FORUM (CSF)

1. Composition of the CSF is as follows: -

(a) **Chairman**. DGMO.

(b) **Members**.

(i) ADG MO (IW).

(ii) ADG T.

(iii) ADG Tac C.

(iv) ADG IS (B).

(v) ADG MI (B).

(vi) ADG Inf.

(vii) ADG MF.

(viii) ADG Arty.

(ix) ADG (E-in-C Branch).

(x) ADG MT.

(xi) ADG EME (B).

(xii) BGS, ARTRAC and BGS (IW) of all Commands.

(xiii) Commander, IW Wing, Army War College.

(xiv) Commander, IT Wing, MCTE.

(xv) Commander, Army Cyber Group.

(xvi) Commandant, Army HQ Computer Centre (AHCC).

(xvii) Director, Army Cyber Group as Member Secretary.

Appendix B
(Refers to Paragraph 44 of
ACSP-2017)

INFORMATION HANDLING MATRIX

Ser No	Issue		Restricted	Confidential	Secret/ Top Secret
(a)	**Type of PC/ Network**	**Data Creation**	• ADN • Secure LAN • Standalone PC	• Secure LAN not connected to the ADN (Ref Para 41) • Standalone PC	Standalone PC
		Data at Rest	• ADN • Secure LAN • Standalone PC	• ADN • Secure LAN not connected to the ADN (Ref Para 41) • Standalone PC	• Not stored on End Pt Device • Data must be securely copied on an optical media and erased from the PC securely after use
		Data Transfer	• **ADN** – AWAN, Local Email of encrypted file within Dte/ Fmn • **LAN** – Email, SFTP	• **ADN**- AWAN • **Secure LAN** – Email, SFTP	-
(b)	**Data Encryption**		Mandatory using Veracrypt/ Secure Desk	Mandatory using Veracrypt/ Secure Desk	Mandatory using Veracrypt/ Secure Desk
(c)	**Two-Factor Authentication**		-	Preferred	Mandatory (Biometric on standalone PC)

Appendix C
(Refers to Paragraph 139 of
ACSP-2017)

IT ACT 2000 AND IT (AMENDMENT) ACT, 2008

1. The relevant extracts of IT Act 2000 and IT (Amendment) Act, 2008 are explained in the following paragraphs.

2. **(Section 43) Penalty and Compensation for Damage to Computer, Computer System etc**. It will be construed as an offence, if any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network:-

(a) Accesses or secures access to such computer resource; **or**

(b) Downloads, copies or extracts any data, computer database or information held in such computer including removable storage medium; **or**

(c) Introduces Virus etc, damages, disrupts, manipulates, causes denial of access, alters or steals any computer system or information held therein.

3. **(Section 66 A) Punishment for Sending Offensive Messages Through Communication Service etc (Presently under Reconsideration/ Revision)**. Any person who sends **(must be understood as even forwarding and not just originating)** by means of a computer resource of a communication device: -

(a) Any information that is grossly offensive or has menacing character; **or**

(b) Any information which he knows to be false, but transmits it for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will; **or**

(c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages **Shall be punishable.**

4. **(Section 66 C) Punishment for Identity Theft**. It will be a punishable offence to fraudulently or dishonestly make use of the electronic signature, password or any other unique identity feature of any other person.

5. **(Section 66 E) Punishment for Violation of Privacy**. It is an offence to intentionally or knowingly capture, publish or transmit the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person.

6. **(Section 66 F)(1) Punishment for Cyber Terrorism**. The act, with an intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people of:-

(a) Denying or cause the denial of access to any person without authority to access computer resource; **or**

(b) Attempting to penetrate or access a computer resource without authority or exceeding authority access; **or**

(c) Introduce any computer contaminant;

And by doing so is likely to cause death or injuries to persons or damage to property or adversely affects the Critical Information Infrastructure specified under Sec 81; **or**

Knowingly or intentionally penetrates or accesses a computer resource without authority which is restricted for reasons of the security of the state or foreign relations or may cause injury to the interest of the sovereignty and integrity of India, the security of the state, public order, decency or morality shall be construed as **cyber terrorism**.

7. **Section 67: Publishing of Information which is Obscene in Electronic Form**. It will be a punishable offence to publish or transmit or cause to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it.

8. **(Section 67 A) Punishment for Publishing or Transmitting Material Containing Sexually Explicit Act etc in Electronic Form**. It will be a punishable offence to publish or transmit in the electronic form any material which contains sexually explicit act or conduct.

9. **(Section 67 B) Punishment for Publishing or Transmitting Material Depicting Children (less than 18 yrs of age) in Sexually Explicit Act etc in Electronic Form**. It will be a punishable offence to:-

(a) Publish or transmit material in any electronic form which depicts children in sexually explicit act or conduct; **or**

(b) Create text or digital images, collect, seek, browse, download, advertise, promote, exchange or distribute material in electronic form depicting children in obscene or indecent or sexually explicit manner.