WELCOME TO THE INFANTRY SCHOOL, MHOW

ITCA (JN) COURSE

CYBER SECURITY

AIM

TO ACQUAINT THE CLASS ABOUT CYBER SECURITY

1. **Cyber Security.** A cyber security policy is a set of guidelines, rules, and procedures established by an organization to protect its information assets, systems, and networks from cyber threats. It serves as a framework for managing cybersecurity risks and outlines the organization's approach to maintaining a secure environment.

2. **Key components of cybersecurity**.

(a) **Network Security**. This involves securing the organization's network infrastructure from unauthorized access, misuse, or disruption. It includes measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and virtual private networks (VPNs).

(b) **Data Security.** Data security focuses on protecting data from unauthorized access, disclosure, alteration, or destruction. Techniques such as encryption, access controls, data masking, and tokenization are used to safeguard sensitive information.

(c) **Endpoint Security**. Endpoint devices such as computers, laptops, smartphones, and tablets are often targeted by cyber attackers. Endpoint security solutions protect these devices from malware, ransomware, and other cyber threats.

(d) **Application Security**. Application security involves securing software applications and preventing security vulnerabilities that could be exploited by attackers. This includes secure coding practices, regular software updates, and vulnerability assessments.

(e) **Identity and Access Management (IAM).** IAM solutions manage user identities and their access to systems and resources. It includes authentication mechanisms such as passwords, multi-factor authentication (MFA), and biometric authentication to ensure only authorized users can access sensitive information.

(f) **Security Operations**. Security operations involve monitoring, detecting, and responding to security incidents in real-time. This includes security information and event management (SIEM), threat intelligence, and incident response procedures to mitigate the impact of security breaches.

(g) **Risk Management**. Cybersecurity risk management involves identifying, assessing, and prioritizing cybersecurity risks to the organization. It includes implementing controls and mitigation strategies to reduce the likelihood and impact of potential threats.

(h) **Security Awareness Training**. Educating employees about cybersecurity best practices and raising awareness about potential threats is crucial for maintaining a secure environment. Training programs help employees recognize phishing attempts, social engineering tactics, and other common cyber threats.

3. **Do’s**

(a) **Use Strong, Unique Passwords**: Use complex passwords or passphrases for all your accounts, and avoid using the same password across multiple accounts.

(b) **Enable Two-Factor Authentication (2FA)**: Whenever possible, enable 2FA for an additional layer of security, which requires a second form of verification, such as a code sent to your phone.

(c) **Keep Software Updated**: Regularly update your operating system, software applications, and antivirus programs to patch security vulnerabilities and protect against known threats.

(d) **Use Secure Connections**: When accessing sensitive information online, use secure connections such as HTTPS websites and secure Wi-Fi networks to prevent eavesdropping and man-in-the-middle attacks.

(e) **Back Up Data Regularly**: Regularly back up important data to an external hard drive, cloud storage, or other secure locations to protect against data loss due to cyberattacks or hardware failures.

(f) **Be Cautious of Suspicious Emails**: Be wary of unsolicited emails, especially those with attachments or links from unknown senders. Avoid clicking on suspicious links or downloading attachments from unfamiliar sources.

(g) **Educate Yourself**: Stay informed about the latest cybersecurity threats and best practices. Take advantage of online resources, training programs, and cybersecurity awareness materials to enhance your knowledge.

(h) **Secure Your Devices**: Use firewalls, antivirus software, and other security tools to protect your devices from malware, ransomware, and other cyber threats. Additionally, consider using encryption to protect sensitive data stored on your devices.

(j) be vulnerable to theft or unauthorized access.

4. **Don’ts**

(a) **Don't Share Personal Information**. Avoid sharing sensitive personal information such as passwords, financial details, or social security numbers over email or other insecure channels.

(b) **Don't Click on Suspicious Links**. Avoid clicking on links in emails, messages, or social media posts from unknown or untrusted sources. These links may lead to phishing websites or malware downloads.

(c) **Don't Use Public Wi-Fi for Sensitive Activities**. Avoid accessing sensitive information or conducting financial transactions over public Wi-Fi networks, as they may be insecure and susceptible to interception.

(d) **Don't Ignore Security Warnings**. Take security warnings seriously and act promptly to address any potential security threats or vulnerabilities on your devices or networks.

(e) **Don't Install Unauthorized Software**. Avoid downloading and installing software from untrusted sources, as it may contain malware or other malicious code that can compromise your system's security.

(f) **Don't Leave Devices Unattended**. Always lock your devices when they are not in use and avoid leaving them unattended in public places, as they may

(g) **Don't Use Default Settings**. Change default passwords and settings on your devices and accounts to enhance security and reduce the risk of unauthorized access.

(h) **Don't Forget to Log Out**. Always log out of your accounts and applications when you're finished using them, especially on shared or public devices, to prevent unauthorized access.

5. **Important advisory to improve cyber security are as follows**: -

(a) CS advisory on improving cyber hygiene of internet facing assets.

(b) Advisory on security measure for CCTV network

(c) Advisory to adopted secure deployment and mgt of network devices on all official nw.

(d) Secure use of broadband and FTTH modem

(e) Advisory about commonly found malicious file **dll4.exe**

(f) Advisory to use smart TVs & smart BDs

(g) Advisory to educate and update about latest phishing technique “Browser-in-the Browser”.

(h) Cyber security advisory against the use of CDsDVDs in usb flash drive mode

(j) Protection against “agent smith” malware

(k) Guidelines for secure handling and usage of official laptop and data held

(l) Guidelines for securing Wi-Fi based network (Admin credential, static DH C, Disable remote mgt, MAC address)

(m) Cyber security advisory against the use of use of social media

(n) Advisory about charging of smart devices through un-trusted USB ports (Juice Jacking)

(o) Guidelines for password management

TO ACQUAINT THE CLASS ABOUT ARMY CYBER SECURITY POLICY 2023

1. To ensure confidentiality, Integrity & avbl of IA's Info Sys & comn networks

2. A CS policy is a set of guidelines, rules, and procedures to protect its information assets, systems, and networks from cyber threats.

3. Framework for managing cyber security risks and outlines

4. **Why policy is needed.** A cyber security policy is needed to ensure that organizations can effectively mitigate cyber risks, comply with legal and regulatory requirements, protect sensitive information, maintain business continuity, and preserve trust and reputation in an increasingly interconnected and digital world.

5. **Guidelines principles**. Guiding principles to be followed for achieving Cyber Security objectives in Indian Army are enumerated below: -

(a) Defence in Depth/ Zero Trust Architecture will be adopted for all Information Systems and applications through compliance management, access control, authorisation and accountability, configuration, change management and incident management.

(b) In case of conflict between security and functionality, security will be given primacy, unless otherwise permitted by the Competent Authority with acceptance of the risks involved.

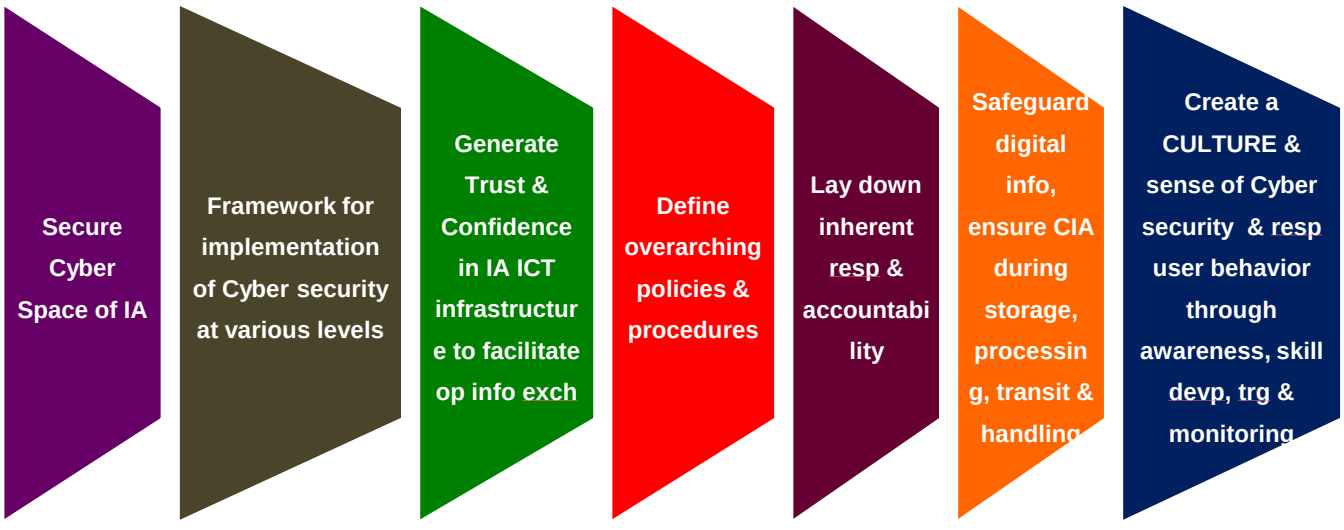
(c) Cyber Security related roles and responsibilities will be clearly defined for all stakeholders and appointments handling IT assets.

(d) Programs will be initiated to improve cyber security awareness and capacity building.

(e) Real time monitoring of all information systems and networks will be ensured and a tiered system of cyber security audit will be implemented.

(f) Policy guidelines and instructions will be continuously reviewed and updated to counter ever evolving threats.

6. **Objectives**



7. Glossary

(a) **Audit**. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

(b) **Authentication**. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

(c) **Cyber attack**. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

(d) **Defence-in-depth**. Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization

(e) **DHCP**. The Dynamic Host Configuration Protocol is a standardized network protocol that is used by network devices to configure the IP settings of another device, such as a computer, laptop or tablet.

(f) **DLP**. Data loss/leak prevention solution is a system that is designed to detect potential data breach/ data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at rest (data storage).

(g) **Remote access**. The ability for an organisation's users to access its non-public computing resources from external locations other than the organisation's facilities.

(h) **Sanitization**. Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

(j) **SSL**. A protocol used for protecting private information during transmission via the Internet. SSI- works by using a public key to encrypt data that's transferred over the SSI-connection. Most Web browsers support SSL and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:"

(k) **SNMP**. Simple Network Management Protocol is an "Internet standard protocol for managing devices on IP networks". It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention

(l) **SSH**. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels

(m) **CCOSW (Command Cyber Ops and Sp Wg)**. A specialized unit of the IA that will assist the formations in undertaking mandated cyber security functions and responsible for safe guarding the network and enhancing the cyber security posture

8. **Threat Characterisation**. There are several factors that have increased the threat surface area in the cyber space. The threat environment pertaining to critical infrastructure of Indian Army is characterised by the following aspects: -

(a) Dependence on foreign technology rather than using indigenous resources. This may result in supply chain poisoning or side channel attacks.

(b) Lack of adequate knowledge and awareness on cyber security aspects.

(c) Reliance on third party vendors for configuration of hardware and software.

(d) Non adherence to the policies promulgated by the CERT to mitigate the present day vulnerabilities in infrastructure used on network.

(e) Inadequate focus on cyber hygiene and policy compliance.

(f) Lack of adequate funds for procurement of licensed software and undue delays in procurement.

(g) Use of personal assets for exchange of official information and development of military mobile applications on Internet.

(h) Utilisation of non-vetted/ open source applications for official purposes without proper sanitisation.

9. **Threat Actors**. With the manifestation of these threats, the exploitation of critical communication infrastructure poses an adverse impact. Various threat actors and their general modus operandi are as under: -

(a) **External Actors**. These are external agents who do not have a direct or physical access to the critical infrastructure or resources of Indian Army. The details are as under: -

S No	Actors	Modus Operandi
(i)	State/ Non state actors	(aa) Create vulnerabilities in critical infrasture & services during design, development & manufacturing (ab) Discover & exploit new existing vulnerabilities in system. (ac) Cultivation of services personnel through social engineering (ad) Posts/ comments on social media to propagate contradictory agenda points. (ae) Compromise of official and personal internet facing digital artefacts (including smartphones) by using malware. (af) Create vulnerabilities by developing counterfeit mobile application. (ag) Spear phishing
(ii)	Foreign intelligence agencies	
(iii)	Criminal & Hackers group	
(iv)	Terrorists/ Extremists	

(b) **Internal Actors**. These are authorised users of the critical infrastructure or resources of Indian Army. The details are as under: -

S No	Actors	Modus Operandi
(i)	Internet Service Providers & Telecom Operators	(aa) Information disclosure in lieu of honey trap (ab) Threat infestation on systems for later exploitation by vendors, service providers (ac) Inadequate security measures during project development & implementation (ad) Information disclosure by Army personnel on social media platforms (ae) Poor cyber hygiene & non adherence of policies
(ii)	Vendors	
(iii)	Regional Engineers on contract	
(iv)	Army Personnel	

10. **Threat Prevention**

(a) **Security Clearance**. A SOP based access control mechanism for civilian service providers/vendors/ Regional Engineers be followed. No vendor/ firm would be allowed to visit army establishments/ communication hubs/ office premises housing IT equipment unless security clearance by respective Intelligence branches is issued. Following shall be ensured: -

(i) Security checks (as laid down by respective intelligence branch) for assets being handled by them. MI Directorate to lay down/ review the instructions on the subject.

(ii) CISO/ Cyber Security officer to ensure access is provided to only those resources for which clearance has been obtained is provided. A log of activities/ changes carried out on ICT assets will be invariably maintained.

(b) **Access Control**. Following aspects shall be ensured to control access to Indian Army critical IT assets/ office premises housing such assets to Vendors/ Third Party Collaboration: -

(i) The entry of third party/ Civil representatives to official premises for the purpose of accessing IT assets shall be allowed only after clearance from respective intelligence branches.

(ii) Requisition for such clearance should clearly record the reason/ need for access to civilian representative.

(iii) All such entries will be recorded and will be allowed under supervision of the asset owner/ Cyber Security Officer.

(iv) The use of any external storage device by third party/ civil rep/ vendors will be prohibited, unless permitted by CISO.

(c) **Non-Disclosure Agreement (NDA)**. NDA will be signed between the owner of the assets and the visiting/ resident Engineer stating official Indian Army data will not be shared with any unauthorised individual. Format for NDA will be promulgated by DG Signals/ respective Directorate.

(i) No data/ logs shall be shared/ handed over to the third party, unless permitted by CISO. System logs of changes/ updation carried out during such events are to be recorded and perused/ verified by the owner/ custodian of these assets.

(ii) Any update/ patches handed over by the vendor shall be deployed only after sanitisation of the CD/DVD/Blue Ray disk.

(iii) NDA with vendors will be undertaken with requisite focus on protection of information against accidental, malicious or unauthorised access to information/ system or its modifications or release.

(iv) Visit to Data Centres/ Signal Centres/ Communication Hubs should be controlled as per policy in vogue, and the same will be duly recorded.

(v) Internet connections should not be provided to the vendor until inescapable and if required should be provided under supervision.

(vi) Station level SOPs for streamlining access to vendors/ contractors, will be promulgated by formation Intelligence Branch.

11. **Accountability**. In cases, wherein access to vendors to Indian Army IT assets/ information is authorised, following norms shall be ensured: -

(a) Sign a Non-Disclosure Agreement.

(b) Bound not to engage in any illegal activity which can affect the CIA triad or privacy of system & information.

(c) Should not download, attach, change, distribute, install any software or inappropriate content unless authorized.

(d) Sanitize the data at Unit/ Formation/ Establishment Sanitisation Box before handing over.

(e) Should not be found with unauthorized portable storage devices, or attempt to deactivate, reverse, disable or by-pass any security controls.

(f) Remote/ online access shall not be provided to vendors/ firm representatives for any communication/ IT device/ network system, unless specified by CISO.

(g) Patches/updates will be downloaded on central systems & would be sanitized using antivirus before usage.

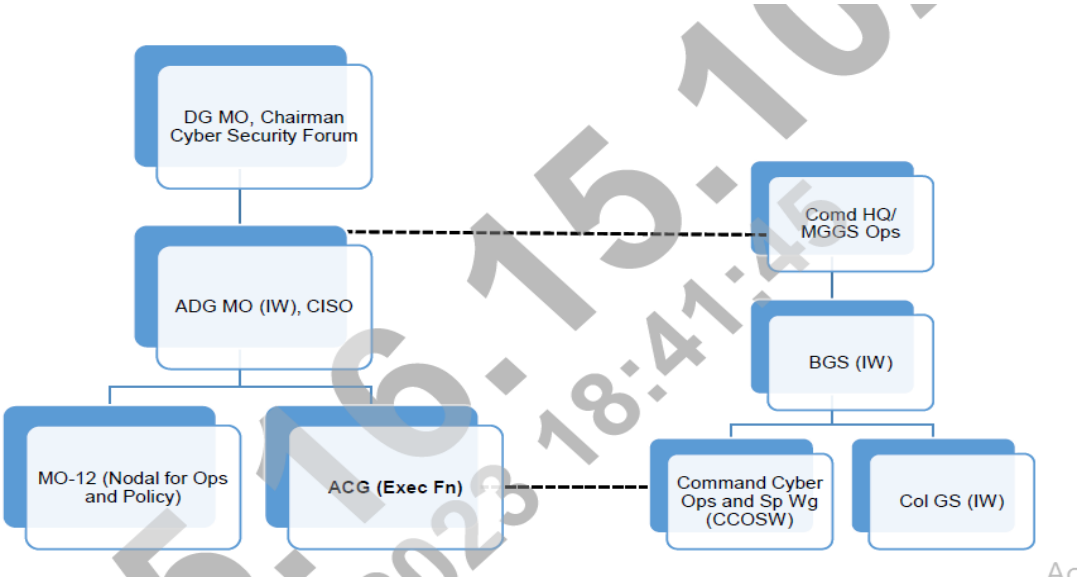
(h) Standalone computer used for downloading should have requisite updated antivirus installed.

(j) Presentations from ADN should not be shared with vendor/foreigners/ civilian’s laptop or personal asset.

(k) Presentation by vendor/ foreigners/ civilians will not be uploaded on ADN unless cleared by CISO.

ORGANISATION AND RESPONSIBILITIES

Cyber Security Organisation of the Indian Army.



12. **Cyber Security Forum (CSF)**. CSF is responsible for formulation and review of policies related to Cyber Security in the Indian Army. 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

13. **ADG MO (IW)**. ADG MO (IW) is the CISO of the Indian Army. He is the nodal authority and single point of contact for all issues related to Cyber Security in Indian Army. CISO will be responsible for interaction with all national agencies and other services including HQ IDS in the Cyber Security domain.Role and charter of CISO of Indian Army is given as under:

(a) Advise COAS/ VCOAS on cyber security issues

(b) Promulgate exec dirns for all cyber security functionaries at AHQ, Comd & lower fmns

(c) Promulgate Cyber Incident Response plan to deal with Cyber crisis

(d) Secure approval for emergent/ urgent procurement for info infra

(e) Ensure compliance to national & defence regulation/ policies wrt Cyber security

(f) Represent IA & interact with Regulatory body & external agencies

14. **Army Cyber Group**. Army Cyber Group is the primary agency for executing all cyber functions in the Indian Army on behalf of CISO. It will carry out the task of Cyber Security management of Indian Army and all units/ establishments in its Area of Responsibility, including establishment of credible domain awareness, forensic activities and audit activities. It will interact with Cyber Security organisations of other Services, Government 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) Create CERT facilities & issue reg alerts & adversaries for cyber incident Mgt & disaster rec plan

(b) Est framework for cyber security audit

(c) Conduct external cyber security audits of all Comd HQ, Dtes/ Br at IHQ of MOD (army)

(d) Provide state-of-art CERT sp malware analysis & cyber forensic services

(e) Vetting, testing & eval of IT proj, web applications & Tac C3I & wpn sys

(f) Coord with CCOSWs & regional forensic labs for cyber defence ops & forensic analysis.

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

(a) Est & op Central & Regional NOC & SOCs for mgt & security of ADN

(b) Bandwidth mgt & IP address mgt on ADN

(c) Central implementation & administration of security & updations of software patches

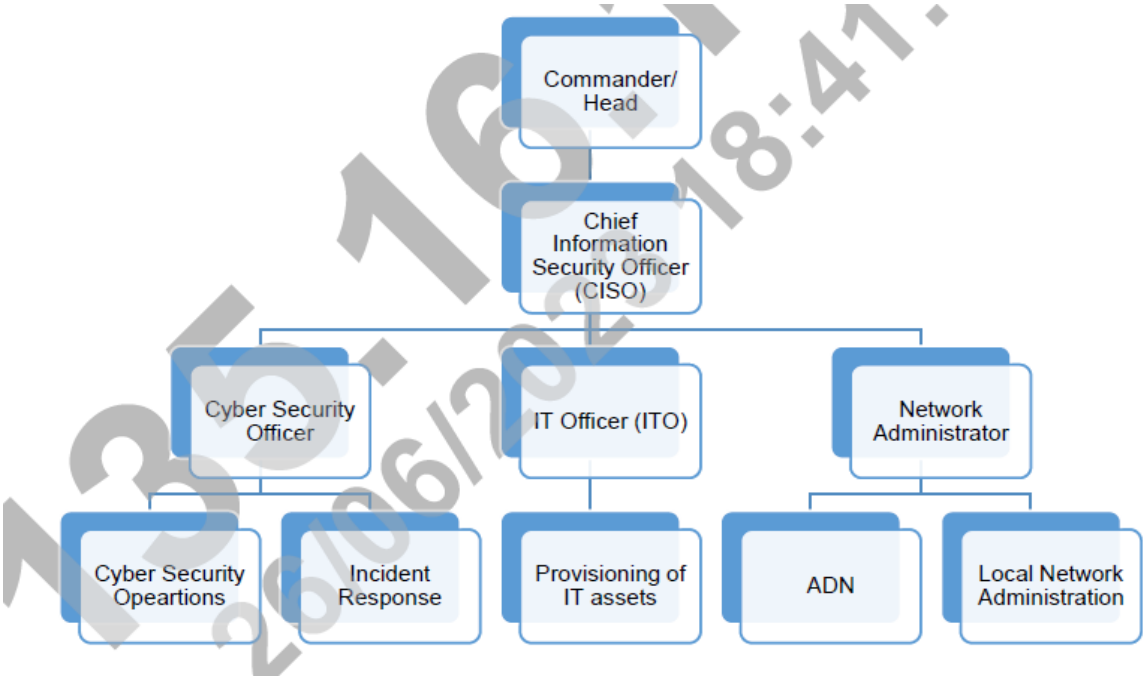
(d) Provide real time SOC feed to ACG & CCOSW

(e) Est, op & maintain Central Data Centre (CDC) & Regional data centre (RDC)

(f) Ensure compliance to CCMP & intimate any incident on ADN to Cert Army

(g) Est & mgt of Internet SOC to act as first responder

CYBER SECURITY ORG AT FMN/ UNIT/ EST LEVEL



16. **Commander/ Head**

(a) Actions by Cdr/ head of Est

(b) Ensure implementation of ACSP

(c) Est a Cyber security org with well defined resp

(d) Define ownership & resp for protection of all ICT assests

(e) Formulation & implementation of SOPs on info security & info assets in AOR

(f) Ensure conduct of periodic Internal & external Cyber security audits

(g) Trg & awareness of all cyber security reqmts

(h) Practice CCMP as per instr from DGMO/ MO – 12

17. **CISO**

(a) **Chater**

(i) Resp to Cdr/ head of est for ensuring all aspects of CS

(ii) Advisor to Cdr/ Head of est

(iii) Single Point of Contact for cyber security issues

(iv) Dply Cyber security architecture (CSO & ITO)

(v) Ensure trg of staff & awareness amongst all rks

(vi) Iden & Audit of CII in AOR & own internal audit

(vii) External audit of org under AOR

(viii) Implementation of CCMP & incident reporting

(ix) Implement procedures in accordance with laid down policies

(x) Report incidents, incl suspected to CISO

(xi) Monitor investigation of incidents as dir by CISO

(xii) Liaise with DGMO & ACG to maint up to date knowledge

(xiii) Implementation of ACG advisory wrt cyber security

(xiv) Implementation of CCMP & incident reporting

(xv) Trg of pers to implement cyber security controls

(b) **Resposibility**

(i) Annual cyber security assessment of own org

(ii) Access control

(iii) Network security

(iv) Digital Data Handling

(v) Asset & Peripheral Mgt

(vi) Internet Security

(vii) Cyber security Audit & Compliance

(viii) Selection of pers & trg

(ix) Incident Mgt, violations & Forensics

18. **Network Administrator**

(a) Resp for network mgt & network security

(b) Installation & config of firewalls at all levels

(c) Resolve network related issues

(d) Approval of pers auth to access servers & CII

(e) Implementation of DLP tool on network devices

(f) Collection & Analysis of logs for incident mgt

(g) Backup of all network devices

(h) Provide real time SOC feed to CCOSWs

(j) Ensure IP & Mac Binding of all assets

(k) Updation of all patches/antivirus

(l) Co-ord with ACG/ CCOSWs for actions on advisories issued by Cert- Army

(m) Monitor, analyse respond to suspicious security events incl Air Gap violations

(n) Report adverse cyber incident/ anomaly to CISO & Cert- Army

19. **Individual user**

(a) Access/ use/ share info only to extent authorised

(b) Authorised indls only to monitor eqpt, sys & network tfc at any time

(c) Ensure Cl/ sensitive info secured at respective work place at the end of day or extd pd of absence

(d) Sys level & user level pwd to comply with the pwd policy

(e) All computing device secured with a pwd-protected screensaver set to 5 mins or less

(f) Extreme caution when opening e-mail att on official Internet IDs

(g) Promptly report theft, loss of unauthorised disclosure of info to the Cyber security officer/ ITO/ CISO

Ser No	Network	Resp
(a)	ADN	DG Signals/ Fmn Signals User
(b)	Exclusive LAN	Fmn IS User
(c)	Standalone computer	User
(d)	Authorised internet	Fmn IS DG Signals User

Network Security

20. **Army Data Network**.

(a) Army Data Network is the operational network of the Indian Army. The ADN is physically segregated and air gapped from civil internet or any other Government/ private network/ Exclusive LAN. DG Signals/ Formation Signals is the network administrator of ADN. To ensure security of the network, centralised security overlays like Domain Controller, OS Patch Management and Anti-Virus have been implemented through DG Signals/ AHCC. SIEM tool has been implemented to obtain logs of all devices on ADN and these logs are analysed and monitored by AHCC and ACG. Owing to the security controls implemented on ADN, the network has been classified as CONFIDENTIAL. DG Signals will ensure that the security controls on ADN are updated regularly to maintain the security classification of the network.

(b) Processing of data up to security classification CONFIDENTIAL is permitted on ADN. Notwithstanding, applications hosted on ADN for storage and transmission of data will ensure implementation of suitable software encryption (128/256 AES) as per MO 10 policy in vogue. Transmission of SECRET data will continue to take place over Cipher channel on ADN, or with specific applications approved for the purpose over DCN

21. **IP Address Management**.

(a) The management of IP addresses on ADN shall be the responsibility of DG Signals.

(b) Static IP addressing shall be implemented across ADN including end point devices as well as network devices like L3 switches and routers. DG Signals shall maintain the centralised repository of formation wise IP addresses. Same shall be shared with DGMO (MO-12)/ ACG on annual/ required basis to facilitate conduct of audit, incident management and network vulnerability assessment and penetration testing.

22. **Security Controls over ADN**. ADN is the Critical Information Infrastructure of the Indian Army. DG Signals has been mandated to manage and secure ADN. Some of the mandatory security controls on the ADN to be implemented are as follows:-

(a) Active Directory/ Domain Controller.

(b) Centralised Identity and Access Management solutions.

(c) Centralised Patch Management System.

(d) End point protection software (Antivirus/Anti Malware).

(e) Centralised asset management and tracking.

(f) Centralised log monitoring/ aggregation and analysis using Security

(g) Information and Event Management (SIEM) solution.

(h) Deployment of Data Loss Prevention solution.

(i) Access to be strictly restricted to Army entities/ organisations only. Any exception to be considered on case to case basis by MO Directorate.

(j) Traceability and visibility of traffic on the ADN through deployment of hardware based firewalls have to be ensured.

23. **Classified Data Over ADN/ Exclusive LAN**. Computers on ADN may be used to create/ store documents up to CONFIDENTIAL security classification. Following shall be ensured: -

(a) Classified data shall be handled as per the security classification in accordance with the provisions covered in Digital Data Handling, and CHCD as amended.

(b) The exclusive LANs deployed within the formations/ units/ establishments shall only process/ store UNCLAS/ RESTRICTED data in accordance with the provisions covered in Digital Data Handling, unless they are engineered as Secure LANs, in which case they shall be permitted to handle CONFIDENTIAL Data.

(c) Security classification of Exclusive LANs shall be duly documented while seeking necessary permission to establish the same.

24. **Security Guidelines while Using ASIGMA**. ASIGMA has been developed to handle information/ data of security classification up to CONFIDENTIAL only. This implies that TOP SECRET/ SECRET files will not be transmitted using the ASIGMA application. Instructions promulgated vide CHCD on the subject are to be followed.

25. **File Transfer Protocol (FTP)**. Use of insecure FTP services within the official Indian Army Networks is not permitted. However, use of Secure FTP (SFTP) services may be configured using whitelisted software/ applications, as updated by DGIS and DG Signals on their website on ADN.

26. **Security control**.

(a) **IP Version 6**. All Network devices be IPv6 protocol complaint for ease of migration. However IPv6 functionality to be DISABLED ON ALL Networks & end point devices until migration

(b) **Remote Access**. Not permitted & should be disabled for all resources of any network in IA. Only permitted over designated secure comn channels for certain specified purposes

(c) **Voice over Internet Protocol (VoIP) Security**. Encryption of data from IP telephones (incl NFS) to server for security. Local VOIP connectivity as separate Network & not merged with ADN unless approved by DGMO

(d) **Backup** - Instrs promulgated vide CHCD to be followed. On ethernet based NAS/ DVDs. Frequency, medium & storage docu as SOPs

Internet Security

27. **Extension of Internet**. The provision of Internet connectivity will be strictly as per the Internet Governance policy issued on the subject by DGMO/MO-10. Following aspects will be ensured while extending the Internet connectivity: -

(a) Extension of Internet connectivity from the ISP to the official premises can be undertaken on all type of media (including radiating media like Wi-Max or USB Based Internet dongles).

(b) The USB based dongles shall be used with a modem only and are prohibited from being directly connected to a computer/ laptop. Devices with inbuilt Wi-Fi adaptors shall be disabled at the BIOS/ system level.

(c) Subsequent extension of Internet connectivity from the modem within the official premises to authorized subscribers will be done over wired media only.

(d) Use of hardware firewall on all Internet connections is mandatory and same will be scaled as per DGIS policy.

(e) Use of Wi-Fi/ other radiating media within office premises is not permitted.

(f) Extension of Internet to formation/ establishment headquarters should preferably be through leased line only with static IPs.

(g) All Internet connected computers of various headquarters/ units must be installed with latest BOSS OS along with requisite cyber security controls. These connections will be centrally monitored through BOSS ISOC maintained by DG Signals.

(h) A list of users authorized Internet connectivity within the office premises must be maintained by the respective Directorate/ Formation/ Unit/ Organisation. All Command GS (IW) will share the updated list of Internet footprints to include Internet computers/ users, Internet connections (having static IPs), Internet facing websites/ applications etc with DGMO (MO-12) annually, and with ACG prior to conduct of External Cyber Security Audit.

(i) Analysis of the logs generated by the perimeter protection devices must be undertaken regularly by the nominated network administrator/ cyber security officer.

(j) Network administrator will ensure modems used for provision of Internet access should enable MAC ID binding to prevent unauthorised connections on the same.

(k) DGIS (Brig IT) will be responsible for scaling and provisioning of official Internet connections. Maintenance of internal servers, routing/ extension devices, cabling and fault rectification is the responsibility of respective Internet Service Provider (ISPs). DG Signals will be responsible for registration of the BOSS OS with ISOC only.

28. **Internet Access**

(a) MAC ID binding enabled at Modems

(b) VPN for official Internet computers is prohibited

(c) Peer-to-Peer data sharing software Prohibited

(d) No official docu on pers laptops/ smartphones

(e) Phishing mails/ suspected data breaches – Report to CISO/ ISO & further to CERT-Army

(f) **Security Aspects**

(i) Maint of Air Gap

(ii) Use of Pen Drives – ZERO TOLERANCE

(iii) Official Mail/ NIC mail IDs

(iv) Official Internet computer not to be used for

(aa) Accessing pers accounts on social media

(ab) Websites pertaining to stock mkt, Betting & other business activities

(ac) Adult dating sites , Pornographic sites, Banned websites etc

(ad) Downloading movies/ music from Peer-to-peer websites

29. **Risks Associated with the Use of Smart Devices**.

(a) Use of smart devices and smartphones in military environment pose risks, which are as under: -

(b) Computing/ storage power of smart devices are equivalent of laptops/ computers. They can therefore store/ process huge volume of data.

(c) Metadata (location, call timings etc) is recorded/ maintained by service providers/ applications and can be used by hostile elements.

(d) Supply chain poisoning can cause built-in software, hardware backdoors in these devices, which can be used to control the device.

(e) Downloading of third party application makes these devices even more vulnerable.

(f) Camera, microphone can be used to capture sensitive data

(g) Personally Identifiable Information (PII) leakage

(h) Friends and family members often become source leakage of sensitive information e.g. through photos/ videos, sharing news about posting/ promotions etc.

(j) Hacked accounts of friends and family members are used to target military persons.

(k) Gathering of Personally Identified Information (PII) & bank details by means of frauds through online shopping & dating applications.

(l) Honey trap activities carried out by adversaries via various chat & social media applications.

(m) Family members shall adhere to the cyber guidelines disseminated during various Sainik Sammelans, Family Welfare Programmes, lectures & talks. Such educational/ awareness capsules should be conducted regularly at

(n) Public Wi-Fi connections - Weak security stds

(o) Untrusted Content – Unknown QR codes not be scanned

(p) Password Protection using strong PIN, pattern or fingerprint

(q) Camera/ Microphone/ Loc svc – Permissions disabled

(r) Contact list – Avoid saving contacts with Rank, unit name

(s) Cl Info – Not to be stored on mob phone

(t) Logging off websites after use

(u) Charging through un-trusted USB ports avoided

(v) Repair/ maint – Through trusted / OEM repair centres only

IT Asset & Peripheral Mgt

30. Servers will be kept in server racks under lock & key

31. USB based Pen Drive/ Flash Drive/ SD Card Readers Use other than whitelisted USB based tokens is strictly prohibited

32. **Internal CD/ DVD Drives**.

(a) ADN computers - Prohibited, except for computers iden as (DEP)

(b) Exclusive LAN - Enabled on selected computers authorised by Cyber security offr

(c) Internet PC/ laptops - Enabled on computers authorised by CS offr

(d) Sanitisation & DEP computer - Permitted

(e) Wireless Keyboard & Mouse – Not Permitted on assets having Cl SECRET & above

33. **IT Asset Management List (ITAML)**. Inventory of cyber/ IT assets and infrastructure is called IT Asset Management List (ITAML). List shall be prepared to ensure that all IT assets irrespective of the mode/ source/ purpose of procurement are accounted for and have been assigned an owner. The ITAML shall be kept updated at all times by ITO and Network Administrators at all levels. ITO will be overall responsible for preparation, maintaining and correctness of ITAML, as well as records of repair, recovery, disposal etc. in respective AoR. The IT asset details will also be uploaded on MISO IT Asset module checked during cyber security audits. In addition, following will be ensured for pan Army visibility: -

(a) DG Signals will maintain updated ITAML of all ICT assets deployed on ADN, including Servers, Routers, Switches, Printers, Scanners, MFDs, end user terminals.

(b) DGIS will maintain updated ITAML of assets in IA, including ADN, LANs, Internet and Standalone computers, irrespective of the source/ mode/ purpose of procurement.

(c) Advisory on the format for maintaining IT Asset list will be issued by DGIS.

(d) The configuration of IT Assets to be procured will be governed by DGIS policy on Standard Configuration of IT Hardware and Peripherals.

(e) The ITAML shall contain the following information (not all inclusive) about the assets:-

(i) Asset identity (Serial No/ Make/ Model No as applicable) to allow unique identification the asset.

(ii) Asset Classification (if applicable).

(iii) Name/Appointment of the Asset Owner.

(iv) Unit/ Formation/ Establishment utilising the asset.

(v) Role (ADN/ Exclusive LAN/ Standalone).

(vi) IP address (if applicable).

(vii) MAC Address (if applicable).

34. **Password Protection**. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access or exploitation of the ICT resources. Following must be ensured: -

(a) **Admin Passwords**. User accounts will be created with limited privileges for daily use. Admin account will be accessed only by network administrators for specific purposes. Passwords for admin accounts will not be shared with the users. Holders of admin passwords for IT assets including computers deployed on various networks are as under: -

(i) **ADN and Exclusive LANs**. Nominated network administrators

(ii) **Standalone and Internet computers**. Nominated Cyber Security Officer

(b) Password Register will be maintained wherein logs related to periodic change of passwords as per policy will be maintained by the user/ system administrator. **The user level passwords will not be written in the register/ any other easily accessible place to avoid unauthorised access**. However, admin passwords may be maintained in a separate register held with authorised appointments as mentioned above.

(c) All system level passwords (including Boot, Windows Administrator, application administrator accounts etc) must be changed every quarter.

(d) User level passwords (including web, email etc) must be changed at least quarterly.

(e) All user level and system level passwords must have at least eight alphanumeric characters and must contain at least four of the five following character classes below: -

(i) Lower case characters.

(ii) Upper case characters.

(iii) Numbers.

(iv) Special characters.

(f) Detailed password policy will be issued by ACG.

35. **Use of Laptops.** Use of Laptops in the IA has been authorised to all appointments tenanted by Lieutenant Colonel and above at a scale of one per officers as replacement for authorised Desktop Computer.

(a) **Usage Environment**. The Laptops are envisaged to be used on following networks in IA: -

(i) ADN/ DCN.

(ii) Standalone Mode.

(iii) Exclusive LANs.

(b) **Cyber Security of Laptops**. Though all aspects mentioned in ACSP are applicable on official Laptops to be used in IA, certain peculiar issues are highlighted in the subsequent paragraphs. Portability of the Laptop enables the officer to carry the Laptops out of the office, however, it also renders Laptops vulnerable for theft/ misuse. Since these Laptops will contain critical/ sensitive military information, their loss/compromise may have detrimental effect on the overall Cyber Security posture of the IA.

(c) **Procurement of Laptops**. Following additional security aspects will be included in the technical specification while procuring the Laptops: -

(i) **Trusted Platform Module (TPM) Security Chip**. This chip authenticates passwords, encryption keys and digital cert.

(ii) **Biometric Scanner**. Laptops must have a fingerprint scanner. This will ensure that only the authorised person has access to the Laptop.

(iii) **Laptop Lock Slots**. This Lock slot will enable the users to physically lock the laptop while on move or during absence from the office. This will ensure physical security of Laptops while on move.

(iv) **Full Disk Encryption**. The Laptop should have a facility to encrypt the complete hard disk.

36. **Inventory Mgt**. All other Laptops irrespective of the deployment environment will be registered with IT Officer. In addition, all Laptops on ADN will be registered with domain Controller and will be aligned to ADN security protocols.

37. **Carriage of Laptops**. The details are as under: -

(a) Carriage of laptops outside concerned office premises including for discharge of official tasks on TD has been permitted. However, carriage of Laptops deployed on ADN will NOT be permitted outside the office premises unless permission is obtained from an officer of the rank of Major General.

(b) A record of move of laptop in case undertaken will be maintained by the Cyber Security officer. Laptops used for storing of data with security classification of CONFIDENTAIL or above will be governed by the provision of the CHCD or MI directorate policy on subject.

PERMISSION OF CISO FOR SYS FORMATTING, UPGRADATION, REC, REPAIR & RESTORE.

Records of sys formatting reset, repairs & restore maint by ITO but only after permission of CISO	Computer connected on internet will not be used for AND/ LAN & vice versa even if formatted	**Change of appt** De-facto formatting of computers not be restored For non ADN computers, network admin will issue fresh user credentials with role based credentials User account password of IT assets being taken over will be reset by new responsible user

38. **Data Exchange Point (DEP)**. DEP is a computer earmarked and configured for data transfer to/ from the secure network. Critical asset on ADN/ exclusive LANs is the data itself. It is of paramount importance to regulate egress of data created/ present on a secure network to other networks. The effort shall be to ensure data on ADN/ exclusive LANs remains within precincts of the network and is made available to the users through secure data transmissions mechanisms such as ASIGMA/ secure email/ secure FTP/ whitelisted application etc. However, when required to transfer data to other networks/ users physically disconnected from the network, data shall be transferred through optical media/whitelisted secure media from earmarked Data Exchange Points (DEP) only. Following aspects shall be ensured: -

(a) Use of internal CD drive/ External CD writers will be permitted only for earmarked DEPs and will be properly documented and produced during the Internal and External audits. No other computer other than DEP computer shall have permission to write/ burn CD/ DVD/ Blue Ray discs. To achieve this, internal CD/DVD must be physically disabled in all other computers. The same will be confirmed by cyber security officer to CISO.

(b) DEP shall be setup with written permission. The permission must be produced during internal/ External Cyber security audits.

(c) DEP shall always be kept under supervision of nominated person.

(d) Record of all DEPs shall be held with respective Cyber Security Officers.

(e) It shall be ensured that Anti-virus software at DEP computers is kept updated at all times.

(f) Only CD/DVD/Blue Ray Discs that have been sanitised (through the Sanitisation Box) shall be used to import data.

(g) Computers identified as DEP must be prominently labelled.

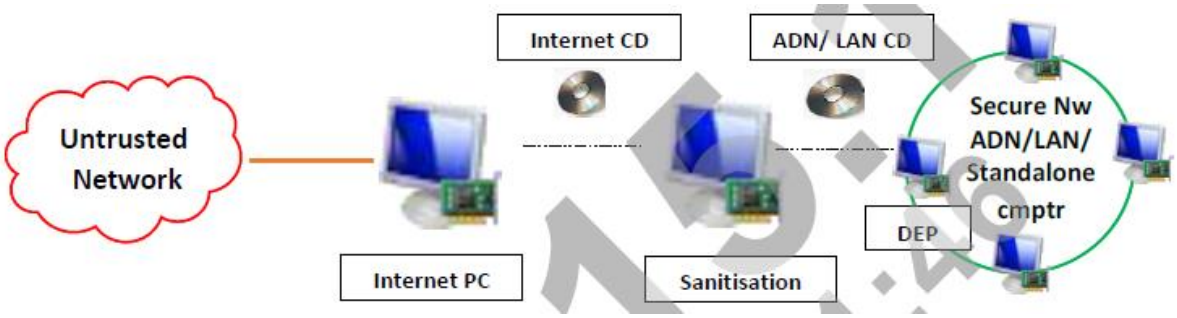
39. **Sanitisation Box**. CISOs at all levels will ensure that a standalone computer with updated antivirus solution, other than the one being used on ADN/ Internet/ Exclusive LAN computer, be earmarked to scan CD/DVD/Blue Ray Discs. Such nominated computers will be termed as Sanitisation Box. Following aspects shall be ensured: -

(a) Sanitisation Box shall be an isolated workstation deployed to undertake all sanitisation related tasks.

(b) Data downloaded from Internet to include patches and updates for the firmware, documents, pictures and videos etc must be first scanned by an updated version of credible

antivirus on the Internet computer itself. Thereafter, the data shall be copied on the sanitisation box using an optical media (CD/DVD/ Blue Ray Disk) authorised to be used on Internet and scanned through Sanitisation Box (essentially installed with updated version of antivirus software that is different from the one deployed on Internet machine).

(c) The scanned data will then be copied on a different optical media (CD/DVD/ Blue Ray Disk) authorised to be used on ADN/ Exclusive LAN/ Standalone Computer and transferred to the designated computer.



Digital Data Handling

40. **Information Classification**.

(a) Information in digital form will be classified as per CHCD.

(b) It shall be mandatory to endorse security classifications (UNCLAS/ RESTRICTED/ CONFIDENTIAL/ SECRET/ TOP SECRET) on all digital documents.

Handling Classified Documents in Digital Form

41. Computers/peripherals (including printers) or storage media used for processing or storing documents of classified nature must be under the ownership of a person of rank/ designation as specified in CHCD. No extra printouts of a document other than distribution list will be taken unless required in official correspondence. Data Loss Prevention Tool will be installed on IT assets processing Op Sensitive info. Security of digital documents shall be handled as per the following policy instructions:-

(a) **TOP SECRET & SECRET Documents**. TOP SECRET & SECRET documents in the digital format will be handled as per the following policy instructions: -

(i) TOP SECRET & SECRET document must be typed and prepared in a designated standalone computer for handling of documents of such classification.

(ii) The originator of the TOP SECRET & SECRET document will be governed as per the provisions of CHCD.

(iii) All relevant clauses of CHCD shall be applicable for handling, transmission and destruction of printed copies of the document.

(iv) Whitelisted shredder software will be used for deletion of TOP SECRET & SECRET. Advisory on secure deletion/shredder software will be issued by ACG.

(v) Copying of the 'TOP SECRET & SECRET' document into USB Drive is strictly prohibited. The same may be undertaken on a CD/DVD or approved storage media.

In such cases, the CD/DVD or earmarked hard disk must be treated in the manner similar to the security classification of the data stored.

(vi) In case backup of the 'TOP SECRET & SECRET' document in the electronic format is maintained, the device in which the back-up is being taken must also be clearly marked as TOP SECRET & SECRET and treated in the same manner.

(vii) Transmission of 'TOP SECRET' documents over any other network except the cipher channel and 'SECRET' documents over any other network except the cipher channel and Defence Communication Network (DCN) using whitelisted messaging tool is strictly prohibited.

(viii) Printouts of all documents classified as TOP SECRET & SECRET will mandatorily be watermarked to establish the intended receiver and to prevent unauthorised pilferage/ copying of the same.

(b) **CONFIDENTIAL Documents.** CONFIDENTIAL documents in the digital format will be handled as per the following policy instructions: -

(i) Confidential Information shall be created/ stored/ processed only on designated computers.

(ii) All documents of CONFIDENTIAL classification, when stored on computers, will be stored in secure data vaults created using whitelisted software like Vera Crypt/ Bit locker/ Secure Desk.

(iii) CONFIDENTIAL documents can be transacted over the AND using applications cleared/ whitelisted for handling/ transmission of CONFIDENTIAL documents including whitelisted SFTP application.

(iv) Documents will be erased/ deleted securely by using whitelisted software like Eraser or Secure Erase (latest version).

(v) Printouts of all documents classified as CONFIDENTIAL should preferably be watermarked to establish the intended receiver and to prevent unauthorised pilferage/ copying of the same.

(vi) Backup of CONFIDENTIAL documents can be stored in a digital format on a secondary storage media. In such cases, the CD/DVD or earmarked hard disk must be treated in the manner similar to the security classification of the data stored.

(c) **RESTRICTED Documents**. Restricted documents in the digital format will be handled as per the following policy instructions: -

(i) Digital documents having a security classification of RESTRICTED shall be stored in secured vault using tools like Vera Crypt and Secure Desk/ Bit locker.

(ii) The designated computers may be connected over the exclusive network/ ADN. However, users must ensure adoption of requisite controls over dissemination of data of ibid classification.

(iii) RESTRICTED documents can be transacted over the through emails/ whitelisted SFTP software.

(iv) Backup of RESTRICTED documents can be stored in a digital format on a secondary storage media.

42. **Secure Transfer of Information**. Information owners will ensure that the classified data will be transferred on a network using an application cleared for handling the classified data only. A summary in the form of Information Handling Matrix is placed at **Appendix F**.

43. **Incident Reporting**. Cyber Crisis Management Plan (CCMP) will be followed in letter and spirit for incident reporting in Indian Army. Any individual who suspects that a theft, breach or exposure of protected data or any attempt to compromise the asset has occurred must immediately provide a description of the incident via the fastest available means to the unit/ organisation CISO/ cyber security officer. Thereafter, the following actions are required to be initiated: -

(a) Upon identification of the theft or data breach, the device needs to be isolated at the earliest.

(b) BOO will be nominated by the concerned formation for immediate seizure and prelim investigation of breach or theft. Standing BOO at formation/ station level may preferably be nominated for the same. The BOO should preferably include representative of provost as member and ITO/ technical representative from local Signal unit/ detachment for technical assistance (and not as a member of BOO).

(c) The incident will also be reported to Army Cyber Group (CERT-Army) through the respective IW/ GS Staff at various levels. Any major cyber incident or a suspected targeted attack will be reported to Command GS(IW) immediately on notice of the incident. All relevant details must be reported to facilitate investigation or mitigation of the incident.

44. **Nodal Agency for Coordinating Incidents**.

(a) Respective heads of the formation will be responsible for ensuring activities related to incident reporting and subsequent investigation, if required.

(b) Army Cyber Group in coordination with DG Signals shall be responsible for coordinating all activities regarding computer security incidents/ emergencies such as limiting their spread and initiation of mitigation actions.

(c) **DG Signals**. Monthly summary of such violations including security logs such as DLP logs, Anti-virus logs, SIEM logs etc shall be compiled by DG Signals for further analysis by Army Cyber Group.

45. **CCMP**. Commanders at all levels would ensure adherence to provisions of Cyber Crisis Management Plan (CCMP) of Indian Army.

46. **Closure of Incidents**. DGMO/MO-12 will be the nodal agency in Indian Army for dealing with all types of compromised computers/ on Internet and USB violations over ADN and official Internet connections. The cases will be closed only by DGMO/MO-12 based on the Action Taken Report (ATR) report from the Command GS (IW). If the espionage angle is not ruled out by the BOO/ C of I, the case will be transferred to DGMI/ Command GS (Int) for further investigation, under intimation to all concerned. Completion report of all such cases, along with Action Taken Report (ATR), will also be forwarded to DGMO/MO-12.Cyber Violations

47. Cyber violations will be categorised according to DGMO/MO-12 letter on the subject and will be accordingly investigated, till finalisation/ completion of the case. Some of the major cyber violations on official IT assets of Indian Army are as under: -

(a) **Possession of Unauthorised Data**. Possession of unauthorised data such as SECRET/ TOP-SECRET data on ADN computer/ standalone computer not cleared for handling of the same, CONFIDENTIAL data in asset not cleared for same, possession of official data on Internet connected/ personal devices etc.

(b) **Transmission of Data through Unauthorised Media**. Involvement in act of transmission of official data that is in contravention to the provisions as given in the ACSP 2023 such as transmission using Internet based services like email, WhatsApp etc, SECRET classified documents through ASIGMA, use of shared folders etc.

(c) **Use of Non-Whitelisted Applications**. Installation of applications that have not been vetted for the said deployment environment.

(d) **Unauthorised Access**. An act of or involvement in obtaining or attempt to obtain access to any official system/ device without due permission for the same eg carrying out network scans, attempting to brute force/ bypass login mechanisms etc.

(e) **Device/ Data Integrity**. An act resulting in violating the integrity of data/ device for its malicious/ unauthorised use unless directed to do the same by authorised authority.

(f) **Unauthorised Changes**. Undertaking unauthorised changes in configuration of device/ systems that is not in accordance with the provisions of ACSP-2023/ advisories/ guidelines/ SOPs in vogue.

(g) **Unauthorised Internet Access**. Accessing official Internet by unauthorised users/ using unauthorised devices/ accessing unauthorised sites etc.

(h) **Air Gap Violation**. Any act resulting in violating the exclusiveness of ADN/ exclusive LAN assets such as use of ADN/ exclusive LAN computers/ devices on Internet, sharing of computers/ network devices on Internet and ADN/ exclusive LAN, connection of mobile phones to official computers etc.

(i) **Logs Deletion**. An act of complete or partial deletion of device/ System Logs.

(j) **Connection of Unauthorised Device**. To connect/ attempt to connect any device that is not authorised/ whitelisted to the official network.

(k) **Sharing of Credentials**. An act to share account credentials such as User name, password etc of official assets with individuals not authorised to be in possession of the same.

(l) **Storing Classified Data w/o Encryption**. Possession of classified data in an unencrypted form.

(m) **Formatting/ OS Upgradation without Permission**. Act of formatting/ OS upgrade to a computer without permission.

(n) **Unauthorised Access to CD/ DVD Writer**. Having facility to write/ burn CD/ DVD without due permission from appropriate authority to the user.

(o) **Uploading of Malicious Programs/ Codes**. Uploading/ executing of malicious codes, scripts over ADN/ exclusive LAN.

(p) **Installation of Unauthorised Software**. Installation of unauthorised software such as virtualisation server on endpoint terminals, non-applications etc.

(q) **Non-production of Asset for Audit**. An act of willingly not producing a serviceable IT asset for cyber audit (unless waiver/ exemption for the same has been obtained from appropriate authorities).

(r) **Data Loss**. An act of intentional/ unintentional loss of information/ data for which the individual(s) is responsible for its safe custody or handling. Appropriate action shall be undertaken against the offenders of cyber violations as applicable by the provisions of military law.

MAJOR DIFFERENCE ACSP-17 & ACSP-23

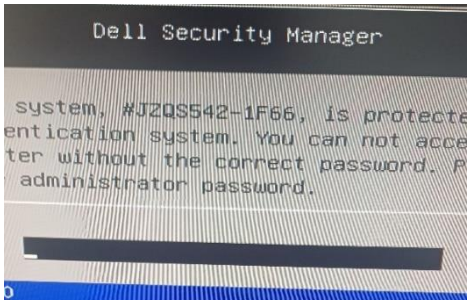
Ser No	ACSP 2023	ACSP 2017
1	CISO (Chief Info Security Offr)	CO as CISO
2	PC formatting auth : 2IC (CISO)	Formatting auth : CO
3	Maint of IT records resp : ITO	Not mentioned before
4	Internet PC will not use in ADN, Exclusive LAN/ standalone, even if formatted (Page No 43). LAN to ADN reqd CISO permission.	Under un-avoidable circumstances
5	Internal CD/DVD writers prohibited in ADN except (DEP, data exch point, spl permission)	Not prohibited rule
6	Wireless keyboard /Mouse not permitted in classified PC	Not mentioned before
7	All in one PC, Mic/webcam restriction	No restrictions, Restriction in ADN
8	PC formation/OS change will do EME Wksp only. Provision of genuine OS for the same is the resp of the respective user of the Pc	Not given by the name of EME Wksp
9	Internet resp of DGMO. DG Sigs	Not given
10	Email & WhatsApp security, NO confidential docu to be share in any condition	Not given
11	BOSS ISOC (Internal Security Oprs Center)	Not given
12	IP address mgt in briefly, Security ctrl in ADN, switches	Not before
13	ASIGMA ruling in brief	
14	DEP and Sanitation box ruling	Sanitation PC only
15	Handling of classified doc. Is brief	
16	ITAML(IT Asset Mgt List) Brief,custodian and classification	Not given
17	Cyber security of laptop is Brief	No given
18	Airgap Violation not mentioned 1.5M	Mentioned 1.5M
19	Cyber Awareness: is Roll Call, SS,FWC	
20	Smart device and public Wifi	Not before
21	PW Policy A-N-Spl 8 Characters -User not write PW-Quarterly change	PW policy 10 Characters -Monthly

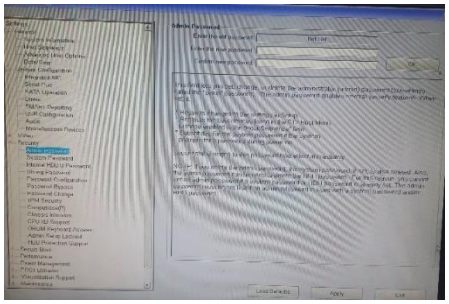
TO ACQUAINT THE CLASS ABOUT HARDENING OF PC

48. **PC Hardening**. Refers to the basic settings that is to be done with the new procured computers either using it as standalone or configuring it onto a Domain. Whenever we procure a computer in IA, the first thing we need to do is Hardening of PC

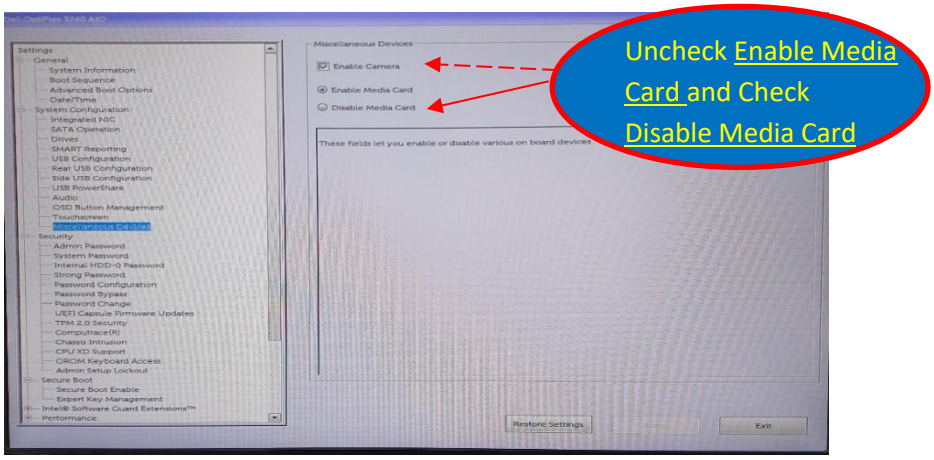
(a) **BIOS Hardening**.

(i) Procedure to set BIOS password:-

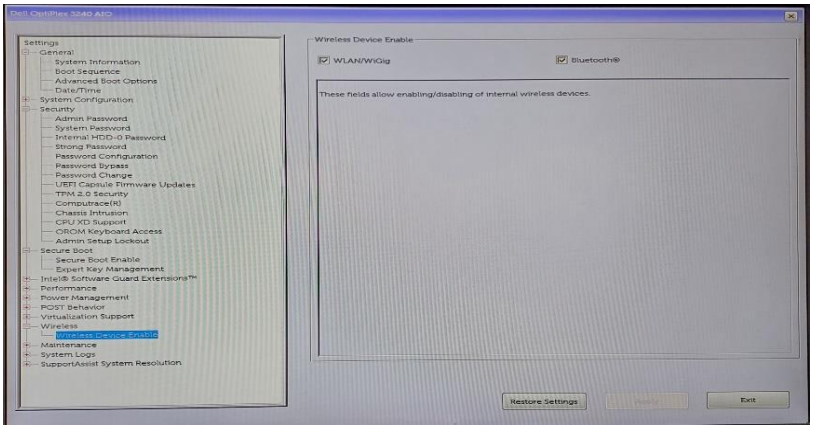




(ii) Card Reader disabled : -



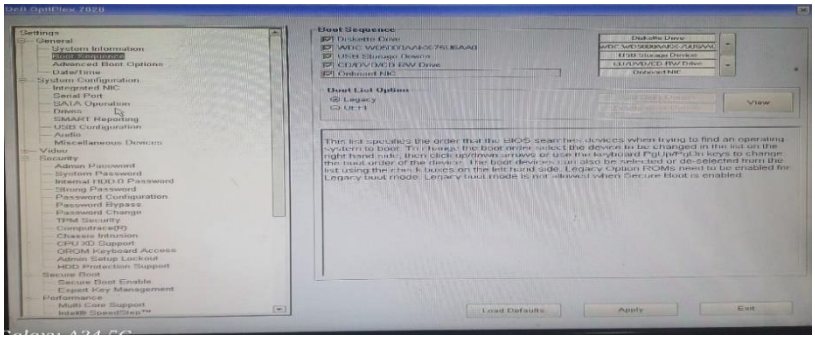
(iii) Procedure to disabled Wireless network Adapter:-



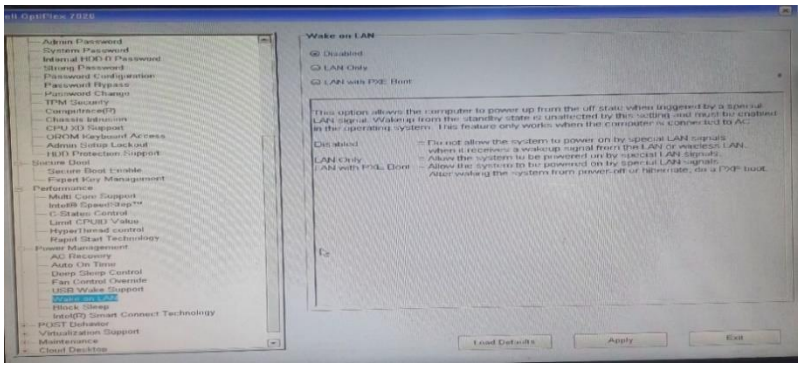
.

(iv) Procedure to disabled to Multiple network card.

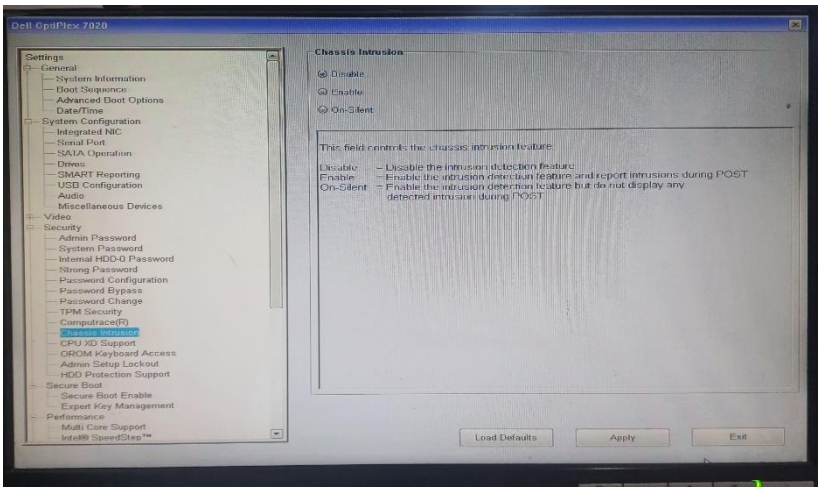
(v) Procedure to disabled Multiple booting ko disable-



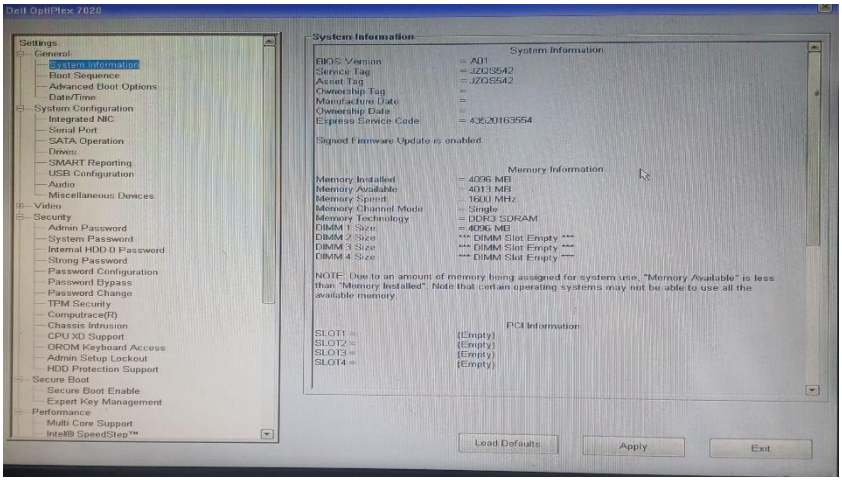
(vi) Procedure to disabled Wake on LAN:



(vii) Procedure to enable Chassis Intrusion-



(viii) BIOS update (to be done only when needed with no other option).



49. **<u>Genuine OS</u>**.

(a) Procedure to check OS specifications:

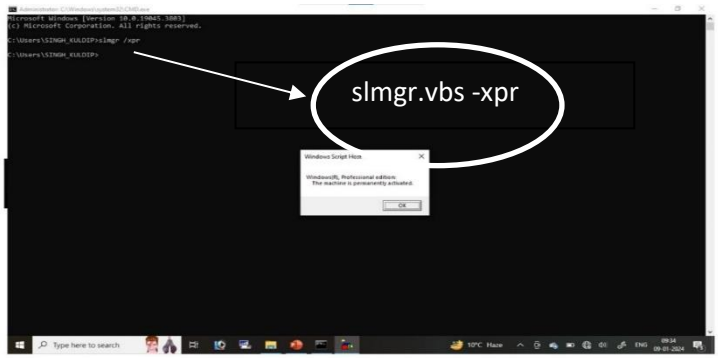
(b) Press Window+R in Keyboard.

(c) Type CMD and press enter.

(d) Type systeminfo and press enter.

(e) Type “slmgr.vbs -xpr” and press enter.

(f) Right click on This PC icon and click on properties.



(g) besides OS specifications some hardening pts are as follows: -

(i) “Allow Remote Assistance connection to this Computer” should be unchecked.

(ii) USB port should be disabled.

(iii) System Date & Time should be correct.

(iv) PC/ IT eqpts should be labelled.

(v) Rename administrator.

(vi) Create user account.

(vii) IPv6 should be disabled.

50. **According to CS policy following services should be disabled**

(a) Bluetooth support services

(b) Computer browser (Standalone)

(c) Fax

(d) IP helper

(e) Remote desktop sharing

(f) Routing & remote

(g) SNMP

(h) Wireless

(i) Bluetooth support

(j) FTP publishing (win XP)

(k) Remote registery

(l) SSDP

(m) Telnet

51. **According to CS policy following policy should be implemented**

(a) Password policy

(b) Acct logout policy

(c) Audit policy

(d) No of user account present

(e) Guest account enable

(f) Display last user name enable

(g) Clear virtual memory enable

(h) Usage of admin account on daily work

TO ACQUAINT THE CLASS ABOUT AUDITING OF PCs, MFDs AND SWITCHES

52. **Types of Audit and Responsibilities**. The various types of cyber security audit to be undertaken are as under: -

(a) **Internal Audit**. The scope of the Internal Audit will include all IT Assets and Network peripheral assets. These will be conducted by concerned formations/ units/ establishments and will be performed by organisations' internal audit staff i.e. within the existing resources of the organisation thrice a year. Out of the three internal audits, one audit may be conducted as a surprise audit by the formation/ unit/ establishment. Actions taken on the observations raised during the previous cyber security audit to be verified and endorsed in the instant report. Detailed mechanism for Network Audit will be promulgated by CERT-Army.

(b) **External Audit**. External Audits at all levels shall be conducted by one up formation/ establishment unless specified. Reports of these audits will be mandatorily included as part of Annual Administrative Inspection by formation Commanders.

53. Details of external cyber security audits are as under: -

(a) **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/ establishments at Delhi.

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

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

(d) **Tri-Services Formation/ Establishments**. ADN connected IT assets (including end-point devices and network elements) of all Tri- Services formation and establishments will be audited by the formation responsible for extending the ADN connection. Audit of these establishments at Delhi will be undertaken by ACG.

(e) **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. Special audit of any subordinate unit/ formation/ establishment can be ordered by the higher formation/ unit Cdr/ head of the establishment. In addition, surprise audit of any unit/ formation/ establishment of Indian Army may be conducted on orders of DGMO.

54. **Conduct**

(a) Remote audit will be undertaken centrally by the authorised auditing agency at all levels. Majority of the parameters will be checked online through the Remote Audit Too developed by ACG. One internal audit to be conducted physically.(i.e. third audit) in the year shall be undertaken physically covering all assets deployed on ADN/ Exclusive network.

(b) Computers of certain critical appointments (as promulgated by one-up higher formation (CISO) shall be audited physically by the external audit teams. However, in case

violations indicating serious gaps in security controls (such as USB violations, air-gap violations etc) are observed, the external audit team may undertake physical audit of all computers of the affected formation/ branch/ directorate/unit

55. **Composition of the Team**. Internal cyber security audits of Command HQ and External cyber security audits of Corps HQ/ other establishments directly under Command will be conducted by dedicated section of Command Cyber Operations and Support Wing (CCOSW). Till such time dedicated cyber organisations are raised at lower formation levels, cyber security audits would be conducted by formation Signals as part of all arms team detailed under the aegis of GS (IW)/ GS (Ops) at respective level. Data bank of qualified manpower may be identified and maintained at formation level and detailed for the said task.

Note: Cdrs at all levels shall ensure conduct of Internal & External cyber audit

56. **List of documents prior to CS audit**

(a) ACSP 2023 & policies/ advisories/ SOPs

(b) Inventory list highlighting BER/ faulty devices & action taken

(c) Part-I orders: ownership

(d) Record of removal storage

(e) Record of destruction of storage media

(f) Record of sanction for formatting/ upgradtion

(g) Password record register

(h) Printout record register

(j) Permission to use external CD/ DVD writer

(k) H/T over certificate

CS audit of PCs

57. **Win Password**

(a) Windows must have complex PW to (alphanumeric)of min 8 characters

58. **Screen Saver Password**

(a) There must be screen saver PW to ensure screen gets lock within one minute

59. **OS Installed Date**

(a) Only activated OS to be installed in PC.

(b) No PC should be running in win 10 and lower ver

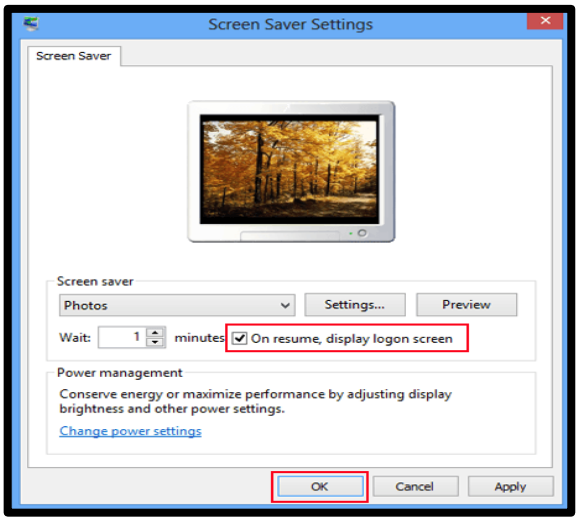
60. **PW Policy**

(a) Password policy must be implemented

(b) PW should not repeat

(c) PW should be complex

(d) Three layer PW policy needs to be adhered



61. **Account lockout policy**

(a) Account lockout policy needs to be implemented

(b) On three invalid attempts account should get locked

62. **No of User**

(a) There must be only user for one PC

(b) No user should be using Admin User for daily usage wk

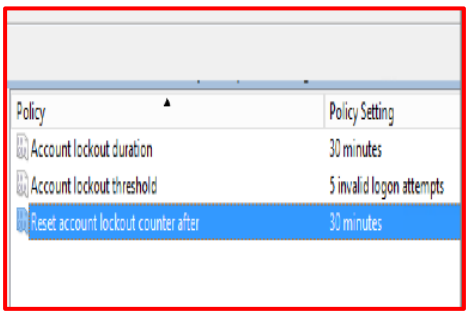
63. **Administrator renamed**

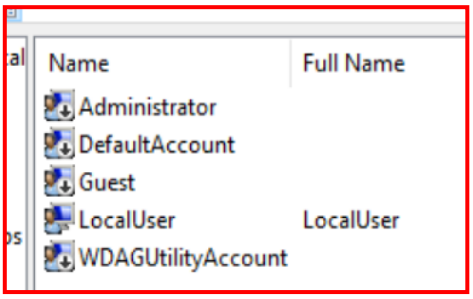
(a) Administrator account name must be renamed

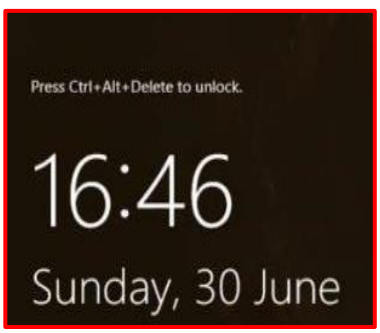
64. **Ctrl + Alt + Del**

(a) This policy must be enabled as it disables the account name

(b) User only who knows the username and PW credentials can login







65. **USB Ports management**

(a) All the USB ports are rewd to be disabled from BIOS and services

(b) All the USB ports except keyboard and mouse need to be sealed phy

(c) If camera is being used in particular PC then BRO has to be done and sanction has to be taken

66. **Remote Service**

(a) All the remote services needs to be disabled to mitigate remote connectivity

67. **Data on Desktop**

(a) User is not permitted to store data in desktop

(b) Desktop data is more prone to breach

68. **No Back up of Data**. User is reqd to take backup of data on reg basis

69. **PC not labeled**

(a) Labelling of PC is must

(b) Username and co-user name must be displayed

(c) Labelling of Grant and serial number is must

(d) Labelling of LAN cables is must if feasible different colour codes to be used for each NW

70. **Cl data exists in PC**

(a) Cl data should not be stored in PC

(b) Only auth user can store that data and that must be encrypted

71. **Usage of Encryption Tool**

(a) IA has provide two Encryption Tools (Secure Desk and Vera Crypt)

(b) User can use both also

(c) All the data needs to be encrypted and only data of current usage to be decrypted

(d) Encryption password management has to be ensured

72. **Official Data on Internet PC**

(a) User is not permitted to store any of the official data in internet PC

(b) Internet PC to be used only for unofficial deeds

73. **Air Gap Maint**

(a) Air gap maint is must to ensure any human fault

(b) There must be min of 1.5mtr gap between LAN and Internet PC

74. **Unwanted Sites access**

(a) Internet must be used cautiously

(b) No logs to be deleted

(c) No unwanted sites to be accessed

75. **Sys date and time wrong**

(a) Sys time and date must be right

(b) This helps in creating right time and date logs in PC

(c) This helps in investigation as and when reqd

76. **Management of CD and DVD and other storage devices**

(a) CD and DVD must be controlled by nominated pers

(b) Each and every CD/DVD record needs to be maint

(c) Issue and Receive enrty to be made deliberately

(d) All the CD and DVD needs to have official stamp and Marking with serial number

(e) Disposal of redundant CD & DVD must be carried reg

(f) Register must be updated reg and surprise checks to be carried out

77. **PC log in and log out record register not maint**

(a) PC log in and Log out register must be maint by the user

(b) This ensures the usage and logs

78. **PC Log book not maint**

(a) PC log book must be held with user

(b) Any HW replacement and faulty details needs to be scrutinised

(c) All the repairs details needs to endorsed in the log book

79. **Physical security**

(a) All the Cyber devices needs to be locked Physically

(b) If feasible cabinets to be made for extra Security

80. **Sanitisation Box**

(a) Each Br should have Sanitisation Box

(b) Any data coming from outside must be scanned

(c) Once data is sanitised then only can be stored in PC

81. **Asset Mgt**

(a) Each BR should have dedicated IT NCO

(b) Owner ship and accountability of assets

(c) Equipment maintenance & repair

(d) Disposal of storage media & printer cartridges

(e) Handing Taking register

(f) Adherence to Army Cyber Policy

82. Auditing a PC typically involves assessing its hardware and software configurations, security settings, and usage patterns.

83. Here's a basic outline of how you might approach auditing a PC:

84. **Hardware Audit:**

(a) Check the specifications of the PC including CPU, RAM, storage capacity, and other hardware components.

(b) Inspect for any physical damage or signs of wear and tear.

(c) Verify peripheral devices (e.g., monitor, keyboard, mouse) and ensure they are functioning properly.

85. **Software Audit:**

(a) Document all installed software including the operating system, drivers, applications, and utilities.

(b) Ensure that software licenses are valid and up-to-date.

(c) Identify any unauthorized or unapproved software installations.

(d) Check for any software updates or patches that need to be applied.

86. **Security Audit:**

(a) Review antivirus and antimalware software installations and update status.

(b) Check firewall settings and ensure they are configured correctly.

(c) Verify user access controls and permissions to sensitive files and directories.

(d) Assess the strength of passwords and ensure they adhere to security best practices.

(e) Check for any unauthorized network connections or open ports.

87. **Data Audit:**

(a) Evaluate data storage practices and identify any sensitive or confidential information stored on the PC.

(b) Ensure data backup processes are in place and functioning correctly.

(c) Assess data encryption settings to protect sensitive information.

88. **Usage Audit:**

(a) Review user activity logs to identify any unusual or unauthorized behaviour.

(b) Analyse internet browsing history and application usage patterns.

(c) Assess system performance and identify any bottlenecks or issues affecting productivity.

89. **Compliance Audit:**

(a) Ensure the PC complies with relevant industry standards and regulations (e.g., GDPR, HIPAA, PCI DSS).

(b) Verify adherence to organizational policies and procedures related to IT security and data management.

90. **Documentation:**

(a) Document findings, recommendations, and any corrective actions needed.

(b) Prepare a comprehensive audit report summarizing the results of the audit and outlining steps for improvement.

91. **Follow-Up:**

(a) Schedule regular audits to ensure ongoing compliance and security.

(b) Implement any recommended changes or improvements identified during the audit process.

92. By conducting a thorough audit of the PC, you can identify potential vulnerabilities, mitigate security risks, and optimize performance to ensure the PC operates efficiently and securely.

Audit of MFD

93. Generally MFDs comes with fwg services: -

(a) Printer/Copier/Scanner/FAX

(b) Wired Network Connectivity

(c) Wireless Networking Wi-Fi/Bluetooth

(d) Removable Memory

(e) Hard Drives

(f) Operating System

(g) Web Server

(h) User Accounts

(j) Remote Access

(k) Landline Connection

(l) Scan to Network Share or PC

(m) E-mail Integration

(n) Web Submission of Print Jobs

(o) Web Browser

94. **Security implemented on MFDs**

(a) Locking compartment

(b) Strong password controls at the console

(c) Settings administration locked down to authorized individuals

(d) web interface turned off

(e) Turn wireless off

(f) Set automatically wiping copies after a job prints

(g) Set IP address to manual

(h) Secure port to be used

(j) Mac binding to be done from administration

(k) Performing an audit of a Multi-Function Device (MFD) involves assessing various aspects of its functionality, security, and compliance. Here's a general outline of the steps you might take in conducting such an audit:

95. **Identify Audit Objectives**. Determine the purpose and scope of the audit. This could include assessing the MFD's efficiency, security measures, compliance with regulations, and adherence to organizational policies.

96. **Review Documentation**. Gather relevant documentation such as user manuals, service agreements, security policies, and any previous audit reports.

97. **Physical Inspection**. Physically inspect the MFD to ensure it is properly installed and maintained. Check for any physical damage or signs of tampering.

98. **Functionality Assessment**.

(a) Test the MFD's core functions such as printing, scanning and copying to ensure they are working properly.

(b) Verify that the MFD integrates seamlessly with the organization's network and software systems.

99. **Security Assessment**.

(a) Evaluate the MFD's security features, including user authentication mechanisms, data encryption capabilities, and access controls.

(b) Check for vulnerabilities such as default passwords, unsecured network connections, and outdated firmware.

100. **Data Privacy Compliance**.

(a) Ensure that the MFD complies with relevant data privacy regulations such as GDPR, HIPAA, or CCPA.

(b) Review the MFD's data handling practices, including how it stores, processes, and transmits sensitive information.

101. **Network Security**. Assess the MFD's impact on the organization's overall network security. Look for any vulnerabilities that could be exploited by attackers to gain unauthorized access to network resources.

102. **User Training and Awareness**.

(a) Evaluate whether users have been adequately trained on how to use the MFD securely.

(b) Provide recommendations for improving user awareness of security best practices related to MFD usage.

103. **Environmental Impact:**

(a) Consider the environmental impact of the MFD, such as its energy consumption and disposal of consumables like toner cartridges.

104. **Reporting and Recommendations:**

(a) Document the findings of the audit, including any issues or deficiencies identified.

(b) Provide recommendations for addressing these issues, such as implementing security patches, updating policies, or conducting additional training.

105. **Follow-Up:**

(a) Monitor the implementation of recommended actions and follow up to ensure that any identified issues have been addressed effectively.

(b) Schedule periodic audits to maintain the security and functionality of the MFD over time.

106. **Documentation and Reporting:**

(a) Prepare a comprehensive audit report summarizing the findings, recommendations, and any actions taken in response to the audit.

(b) Share the report with relevant stakeholders, including IT personnel, management, and any external auditors or regulatory bodies.

107. By following these steps, you can conduct a thorough audit of a Multi-Function Device to ensure its functionality, security, and compliance with organizational policies and regulatory requirements.

108. **Audit of a Network Switch**. According to CS policy Switching devices used for networking must be manageable. MAC Add & IP should be binded and unused ports must be disabled and block. Auditing a network switch involves assessing its configuration, performance, security measures, and compliance with relevant standards and policies. Here's a comprehensive guide on how to conduct such an audit:

(a) **Identify Audit Objectives**. Define the purpose and scope of the audit, including assessing the switch's configuration, security, performance, and compliance with organizational policies and industry standards.

(b) **Review Documentation**. Gather documentation such as switch manuals, network diagrams, configuration files, and any previous audit reports.

(c) **Physical Inspection**. Physically inspect the switch to ensure it is properly installed, labeled, and ventilated. Check for any signs of damage or tampering.

(d) **Configuration Assessment**.

(i) Review the switch's configuration settings to ensure they align with best practices and organizational policies.

(ii) Verify that VLANs, spanning tree protocol (STP), port security, and other features are configured correctly.

(iii) Check for any unused or deprecated configurations that could pose security risks or impact performance.

(e) **Performance Evaluation**.

(i) Assess the switch's performance metrics such as throughput, latency, and packet loss.

(ii) Use network monitoring tools to analyze traffic patterns and identify any bottlenecks or performance issues.

(f) **Security Assessment**.

(i) Evaluate the switch's security features, including access control lists (ACLs), port security, and authentication mechanisms.

(ii) Check for vulnerabilities such as default passwords, outdated firmware, and misconfigured security settings.

(iii) Assess the switch's compliance with security standards such as ISO 27001 or NIST Cybersecurity Framework.

(g) **Network Segmentation**.

(i) Review the switch's role in network segmentation and segregation of critical assets from less secure areas.

(ii) Ensure that VLANs and access control mechanisms are implemented to enforce segmentation policies effectively.

(h) **Logging and Monitoring**.

(i) Review the switch's logging and monitoring capabilities, including syslog, SNMP, and NetFlow.

(ii) Ensure that logs are generated, stored securely, and regularly reviewed for security incidents and performance trends.

(j) **User Training and Awareness**.

(i) Evaluate whether network administrators and users are adequately trained on how to use the switch securely.

(ii) Provide recommendations for improving user awareness of security best practices related to switch management and usage.

(k) **Documentation and Reporting**.

(i) Document the findings of the audit, including any issues or deficiencies identified, as well as recommendations for remediation.

(ii) Prepare a comprehensive audit report summarizing the audit process, findings, recommendations, and any actions taken in response to the audit.

(iii) Share the report with relevant stakeholders, including IT personnel, management, and any external auditors or regulatory bodies.

109. By following these steps, you can conduct a thorough audit of a network switch to ensure its configuration, performance, security, and compliance with organizational policies and industry standards.

110. **implementation of security at server.** Implementing security at a server level involves various measures to protect the server from unauthorized access, data breaches, and other security threats. Here's a comprehensive guide to implementing security at a server level:

(a) **Update Software Regularly**. Keep server operating systems, applications, and software up to date with the latest security patches and updates to address vulnerabilities.

(b) **Use Strong Authentication**. Implement strong password policies or use multifactor authentication (MFA) to enhance authentication security. Utilize tools like SSH keys for secure remote access.

(c) **Firewall Configuration**. Configure firewalls to filter network traffic and only allow necessary connections. Use intrusion detection and prevention systems (IDPS) to monitor and block suspicious activity.

(d) **Encryption**. Encrypt sensitive data both in transit and at rest using protocols like SSL/TLS for data transmission and disk encryption for stored data.

(e) **Access Control**. Limit access to the server by granting permissions based on roles and responsibilities. Use access control lists (ACLs) to define who can access specific resources.

(f) **Regular Backups**. Implement regular backups of critical data to mitigate the impact of data loss due to security incidents or hardware failures. Store backups securely and test restoration processes periodically.

(g) **Logging and Monitoring**. Enable logging for server activities and monitor logs regularly for unusual behavior or security incidents. Use security information and event management (SIEM) systems for centralized log management and analysis.

(h) **Antivirus and Antimalware Software**. Install and regularly update antivirus and antimalware software to detect and remove malicious software from the server.

(j) **Patch Management**. Establish a patch management process to systematically apply security patches and updates to server software and firmware.

(k) **Secure Remote Access**. Use secure protocols like SSH or VPN for remote access to the server. Implement measures such as IP whitelisting and two-factor authentication to secure remote connections.

(l) **Secure Configuration**. Follow security best practices when configuring server settings and services. Disable unnecessary services, close unused ports, and configure services securely.

(m) **Incident Response Plan**. Develop and regularly update an incident response plan to respond effectively to security incidents. Define roles and responsibilities, escalation procedures, and communication protocols.

(n) **Regular Security Audits and Penetration Testing**. Conduct regular security audits and penetration tests to identify vulnerabilities and weaknesses in the server infrastructure. Remediate findings promptly to improve security posture.

(o) **Employee Training and Awareness**. Provide security awareness training to employees to educate them about security best practices, phishing awareness, and the importance of safeguarding sensitive information.

(p) **Vendor and Third-Party Security**. Assess the security posture of third-party vendors and service providers who have access to the server or handle sensitive data. Ensure they adhere to security standards and compliance requirements.

111. By implementing these security measures at the server level, you can strengthen the overall security posture of your infrastructure and protect against various cyber threats. Additionally, staying vigilant and proactive in monitoring and adapting security measures to evolving threats is essential for maintaining a secure server environment

112. **Implementation of security at firewall**. Implementing security at the firewall is crucial for protecting a network from various cyber threats. Here's a step-by-step guide on how to effectively implement security measures at the firewall:

(a) **Define Security Policies.** Clearly define the security policies that the firewall will enforce. This includes identifying acceptable and unacceptable traffic, access control rules, and logging requirements.

(b) **Segmentation.** Implement network segmentation to divide the network into separate security zones based on the level of trust. For example, separate internal networks from external-facing systems like web servers.

(c) **Access Control Lists (ACLs).** Configure ACLs to control traffic flow between different network segments and to specify which types of traffic are allowed or denied. Use specific rules to permit necessary traffic and block unauthorized or malicious traffic.

(d) **Stateful Inspection**. Enable stateful packet inspection on the firewall to monitor the state of active connections and enforce security policies based on the context of each connection. This helps prevent attacks like spoofing and session hijacking.

(e) **Application Layer Filtering.** Implement application-layer filtering to inspect traffic at the application layer (Layer 7 of the OSI model) and enforce policies based on the specific protocols and applications being used. This helps detect and block threats like malware and unauthorized access attempts.

(f) **Intrusion Detection and Prevention System (IDPS).** Integrate an Intrusion Detection and Prevention System with the firewall to identify and block suspicious or malicious traffic patterns in real-time. This adds an additional layer of defense against advanced threats.

(g) **Virtual Private Network (VPN) Configuration.** Configure VPN tunnels on the firewall to provide secure remote access for authorized users and to encrypt traffic between remote locations. Ensure that VPN connections are properly authenticated and encrypted to protect sensitive data in transit.

(h) **Logging and Monitoring.** Enable logging on the firewall to record details of network traffic, security events, and policy violations. Regularly review firewall logs to identify potential security incidents and to ensure compliance with security policies.

(i) **Regular Updates and Patch Management.** Keep the firewall firmware and security rules up-to-date by applying vendor-supplied patches and updates in a timely manner. Regularly review and update firewall configurations to adapt to evolving security threats and organizational requirements.

(j) **Security Policy Review and Audit**. Conduct regular reviews and audits of firewall security policies to ensure they remain effective and aligned with business objectives. Evaluate firewall logs and performance metrics to identify areas for improvement and optimization.

(k) **Employee Training and Awareness**. Educate network administrators and users about the importance of firewall security and best practices for securely accessing and using network resources. Provide training on how to recognize and respond to security threats and incidents.

(l) **Incident Response Plan**. Develop an incident response plan that outlines procedures for responding to firewall-related security incidents, including steps for containing, investigating, and mitigating potential threats. Regularly test and update the incident response plan to ensure its effectiveness.

113. By following these steps, organizations can effectively implement security measures at the firewall to protect their networks from a wide range of cyber threats and vulnerabilities from a wide range of cyber threats and vulnerabilities.

114. **Cloud Computing**. Cloud computing is the delivery of computing services such as server, storage, database, networking tool & software over the internet.

(a) **Characteristics of Cloud computing**:

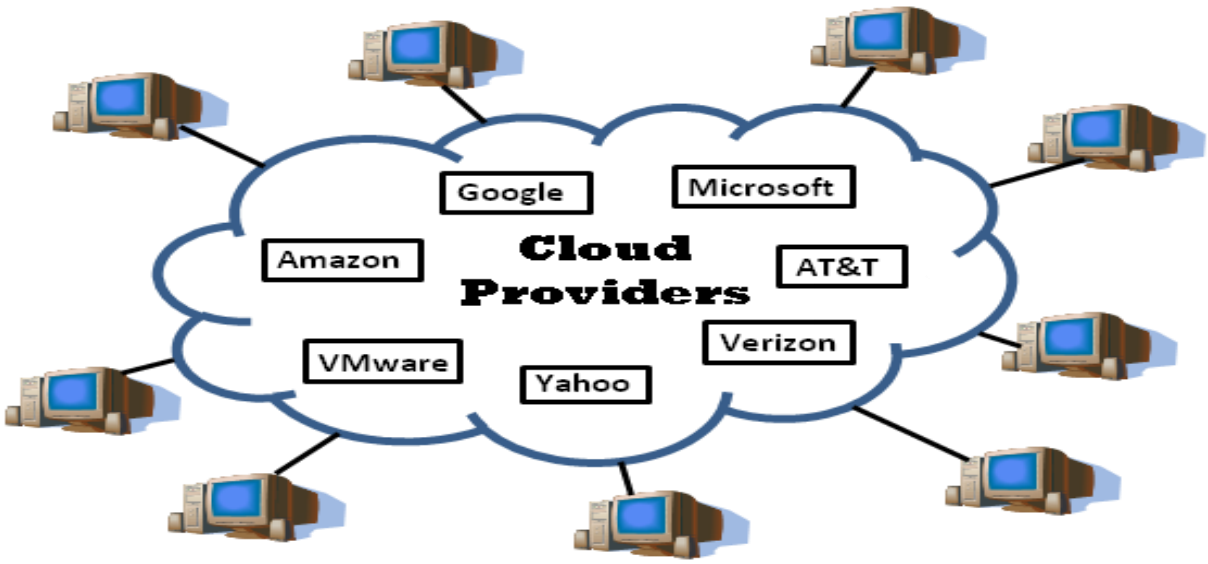
(i) On-Demand self services

(ii) Broad network access

(iii) Resource pooling

(iv) Rapid elasticity

(v) Measured services (Pay as you go)

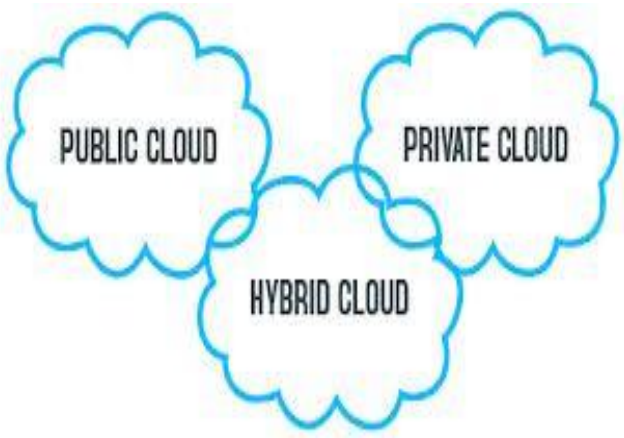


115. **Types of cloud**: -

(a) Public cloud

(b) Private cloud

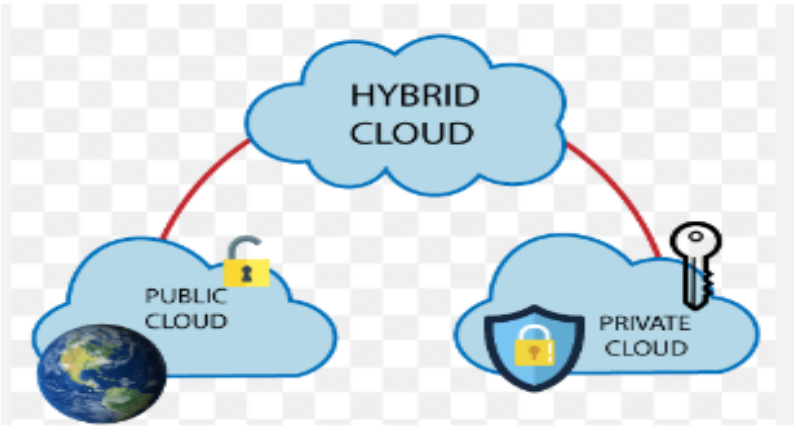
(c) Hybrid cloud



116. **Public cloud**. Public clouds deliver resources, such as compute, storage, network, develop-and-deploy environments, and applications over the internet. They are owned and run by third-party cloud service providers like Google Cloud.

117. **Private Cloud.** Private clouds are built, run, and used by a single organization, typically located on-premises. They provide greater control, customization, and data security but come with similar costs and resource limitations associated with traditional IT environments.

118. **Hybrid Cloud**. Environments that mix at least one private computing environment (traditional IT infrastructure or private cloud, including edge) with one or more public clouds are called hybrid clouds. They allow you to leverage the resources and services from different computing environments and choose which is the most optimal for the workloads.



119. **Types of cloud services:**

(a) SaaS (Software as a service)- End User

(b) PaaS (Platform as a service)- Developer

(i) Hardware and software tools

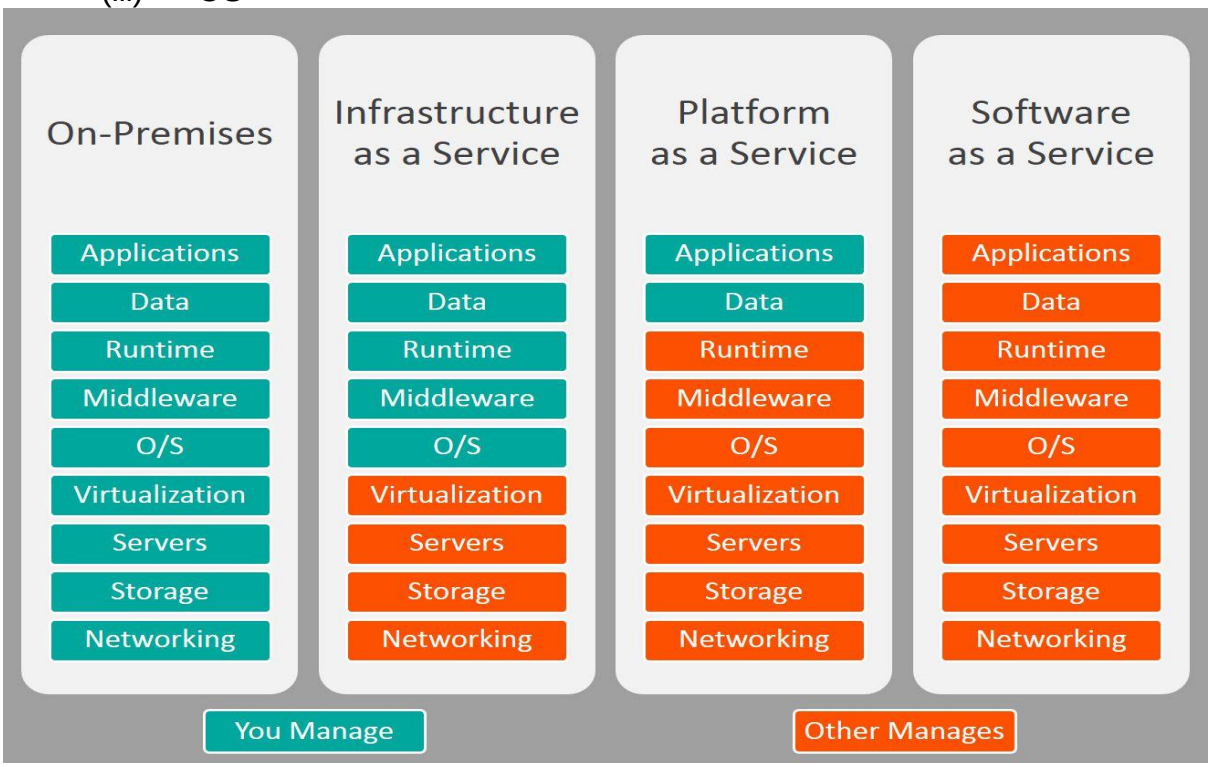
(ii) Tools needed for application development

(c) IaaS (Infrastructure as a Service)

(i) Data Centres

(ii) Storage

(iii) OS



120. **SaaS (Software as a service).** SaaS provide a full application stack as a services that customer can access and use. SaaS solution often come as ready-to-use application, which are managed and maintained by the cloud service provider.

121. **PaaS (Platform as a service).** It delivers and manages hardware and software resources for developing, testing, delivering, and managing cloud applications. Providers typically offer middleware, development tools, and cloud databases within their PaaS offerings.

122. **IaaS (Infrastructure as a Service).** It delivers on-demand infrastructure resources, such as compute, storage, networking, and virtualization. With IaaS, the service provider owns and operates the infrastructure, but customers will need to purchase and manage software, such as operating systems, middleware, data, and applications.

123. **Advantages of cloud:**

(a) Flexibility

(b) Low cost

(c) Management of data

(d) Device diversity

(e) Increased storage

(f) Customized setting

124. **Disadvantages of cloud**

(a) Dependency

(b) Risk

(c) Requires a constant internet connection

(d) Security

(e) Migration issue

125. **Cloud Security**. Cloud security is a crucial aspect of modern IT infrastructure, given the increasing adoption of cloud services for data storage, computing, and application deployment. Here's a comprehensive overview of cloud security considerations and best practices:

(a) **Data Encryption.** Encrypt data both at rest and in transit using strong encryption algorithms. Utilize encryption mechanisms provided by cloud service providers or implement your own encryption solutions for added security.

(b) **Identity and Access Management (IAM).** Implement robust IAM policies to manage user access to cloud resources. Use principles of least privilege and multi-factor authentication (MFA) to control access to sensitive data and services.

(c) **Network Security.** Configure network security groups, firewalls, and virtual private clouds (VPCs) to control inbound and outbound traffic to cloud resources. Use segmentation to isolate sensitive workloads from less secure environments.

(d) **Secure Configuration.** Follow security best practices provided by cloud service providers for configuring cloud resources securely. Regularly audit and update configurations to address security vulnerabilities and compliance requirements.

(e) **Logging and Monitoring.** Enable logging and monitoring services provided by cloud platforms to track user activities, resource usage, and security events. Utilize security information and event management (SIEM) tools for centralized log analysis and threat detection.

(f) **Incident Response and Forensics.** Develop incident response plans and procedures for responding to security incidents in the cloud. Conduct regular drills and exercises to test the effectiveness of incident response processes. Preserve forensic evidence for investigation and analysis.

(g) **Compliance and Governance.** Ensure compliance with industry regulations and standards relevant to your organization, such as GDPR, HIPAA, PCI DSS, etc. Implement governance frameworks and controls to enforce security policies and regulatory requirements in the cloud.

(h) **Data Loss Prevention (DLP).** Implement DLP solutions to prevent unauthorized access, sharing, or leakage of sensitive data in the cloud. Use data classification tools to identify and classify sensitive information, and enforce appropriate access controls and encryption measures.

(j) **Backup and Disaster Recovery.** Implement backup and disaster recovery strategies to ensure data resilience and business continuity in the event of data loss or service disruptions. Regularly test backup and recovery processes to verify their effectiveness.

(k) **Vendor Risk Management.** Assess the security posture of cloud service providers through vendor risk assessments. Evaluate factors such as data security, compliance certifications, incident response capabilities, and service level agreements (SLAs) before selecting a cloud provider.

(l) **Employee Training and Awareness.** Provide comprehensive training and awareness programs for employees to educate them about cloud security risks, best practices, and their responsibilities in maintaining a secure cloud environment.

(m) **Continuous Improvement.** Implement a continuous improvement process for cloud security, including regular security assessments, vulnerability scanning, and penetration testing. Stay informed about emerging threats and security trends to adapt and enhance cloud security measures accordingly.

126. By incorporating these best practices into your cloud security strategy, you can effectively mitigate risks and ensure the confidentiality, integrity, and availability of your data and applications in the cloud applications in the cloud.

TO ACQUAINT THE CLASS ABOUT ONLINE THREATES

127. An introduction to computer science attacks, also known as cyber attacks, is essential for understanding the various threats and vulnerabilities that exist in the digital world. Here's a basic overview:

128. **What is a Cyber Attack?** A cyber attack refers to any malicious attempt to compromise the confidentiality, integrity, or availability of computer systems, networks, or data. These attacks can target individuals, organizations, or even entire nations, and they can have serious consequences ranging from financial loss to reputational damage and even national security risks.

129. **Phishing**. Phishing attacks attempt to trick users into revealing sensitive information, such as passwords or credit card details, by impersonating legitimate sources like banks, social media platforms, or colleagues. Example: You receive an email that appears to be from your bank, urging you to click a link to verify your account details. Clicking the link takes you to a fake website that looks real, where you unknowingly enter your login credentials.

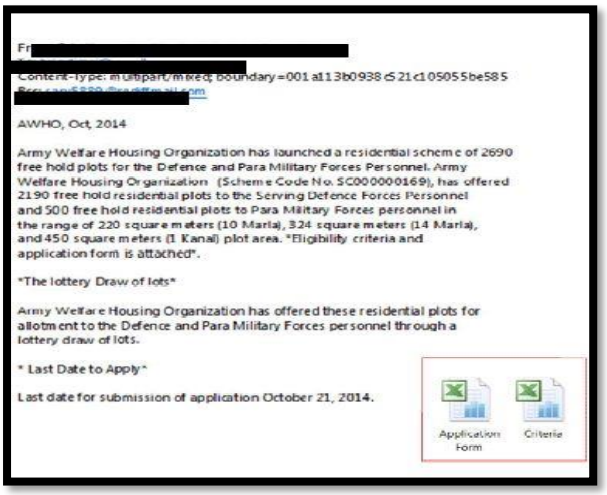
130. **Prevention**:

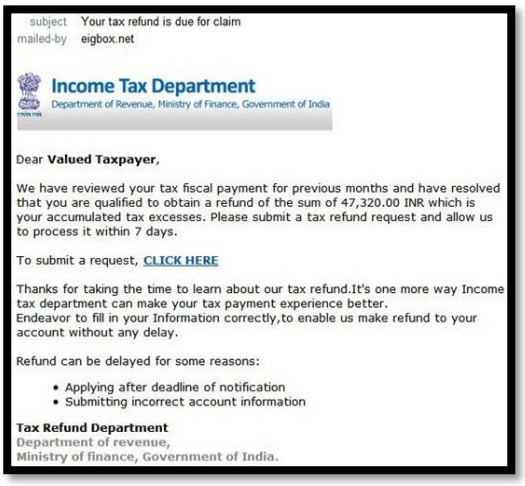
(a) Be cautious of unsolicited emails, texts, or calls.

(b) Verify sender legitimacy before clicking links or opening attachments.

(c) Check website URLs carefully for typos or inconsistencies.

(d) Don't share personal information through suspicious channels.



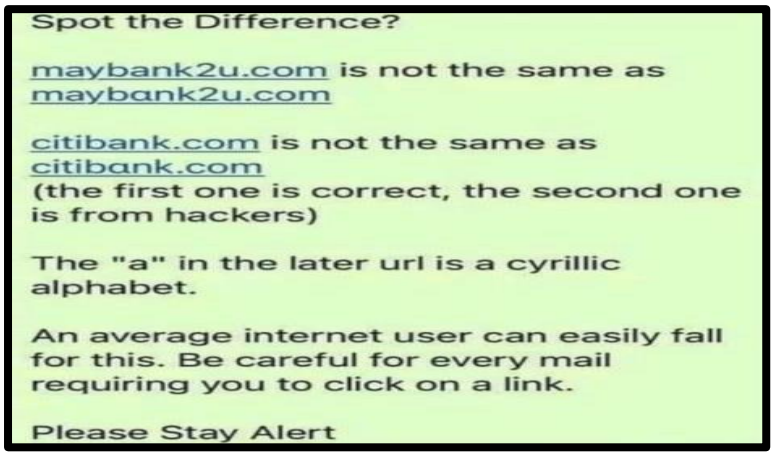


131. **How to identify phishing mails**

(a) Hover over on 'From'

(b) Are URLs legitimate?

(c) Incorrect formatting & grammar Hackers use this purposefully



132. **Malware.** Malware (malicious software) is a broad term encompassing various software programs designed to harm a computer system. This can include viruses, worms, Trojans, spyware, and ransomware. Example: You download a seemingly harmless file from the internet, but it secretly installs malware on your computer. This malware could steal your data, corrupt files, or lock you out of your system entirely.

133. **Common types of malware**:

(a) **Viruses:** Malicious programs that replicate themselves by attaching to other files or programs and spread throughout a system.

(b) **Worms:** Self-replicating malware that spreads across networks, exploiting vulnerabilities to infect other devices.

(c) **Trojans:** Malware disguised as legitimate software, which may provide attackers with unauthorized access to a system or steal sensitive information.

(d) **Ransomware:** Malware that encrypts files or locks users out of their systems until a ransom is paid.

(e) **Spyware:** Malware designed to secretly monitor and gather information about a user's activities without their consent.

(f) **Adware:** Malware that displays unwanted advertisements and may track users' browsing habits for advertising purposes.

134. **Prevention**:

(a) Download software only from trusted sources (e.g., official app stores).

(b) Use antivirus and anti-malware software and keep them updated.

(c) Be cautious of opening attachments from unknown senders.

(d) Regularly back up your important data.

135. **Cyber espionage**.

(a) **Description**. Cyber espionage involves the unauthorized access to computer systems to steal confidential information. This is often conducted by nation-states or organized crime groups targeting businesses, government agencies, or individuals with access to valuable data**.**

(b) **Example**: Hackers exploit a vulnerability in a company's software to gain access to their network and steal sensitive data, such as trade secrets or customer information.

(c) **Prevention**:

(i) Keep software applications updated to patch security vulnerabilities.

(ii) Implement strong network security measures like firewalls and intrusion detection systems.

(iii) Educate employees on cyber security best practices, including password hygiene and avoiding suspicious links.

136. **Hacking:**

(a) **Description**. Hacking is the general term for gaining unauthorized access to a computer system or network. Hackers can have various motives, including stealing data, disrupting operations, or installing malware.

(b) **Example**. A hacker discovers a weakness in a website's security and exploits it to gain access to user accounts or databases.

(c) **Prevention**:

(i) Use strong, unique passwords for all online accounts.

(ii) Enable two-factor authentication (2FA) whenever available.

(iii) Be mindful of what information you share online and on social media.

(iv) Keep your operating system and software updated with security patches.

137. **What we lost**

(a) Confidential Data.

(b) Strategic Planing.

(c) Bank A/C Details.

(d) Personal Information. Credit Cards Information

CYBER SECURTY AUDIT: IMPLEMENTATION CHECK LIST

S/No	Implementations
1.	**BIOS Password** :- Restart cmptr – press Delete/F2/F7 – boot setting – set user password – confirm password – F10 – yes – exit.
2.	**Win Password** :- Rt click on my cmptr – manage – system tools - local users & groups – users – rt clict on user name – set password – type password – confirm password - ok
3.	**Default share exits** :- Rt click on my cmptr – manage – system tools - shared folders – shares – select all – rt click – stop sharing.
4.	**Guest acct disable** :- Rt click my cmptr – manage – system tools – local users and groups – users – rt click on Guest – properties – check 'acct is disabled' box.
5.	**Administrator rename** :- Rt click my cmptr – manage – system tools – local users and groups – users – rt click on administrator – rename – (type name).
6.	**Create New user** :- Rt click my cmptr – manage - system tools – Local users and groups – rt click on users – new user – type user name – type password – uncheck the user must change password on next logon.
7.	**Screen Saver Password** :- Rt click on desktop – Personalize – screen saver – wait (type – 2), check on box before on resume, display log on screen.
8.	**Welcome Screen available** :– Run cmd – secpol.msc – local policies – security options – interactive logon: 1. Massage title for users…. (Type – Info) & 2. Massage text for users…. (Type – Restrictions – Vide ACSP 2017 and advisories to the effect have been enforced. All activities on this machine are being logged continuously).
9.	**Password policy implemented** :- Run cmd – secpol.msc – account policies – password policies – Enforce password history (3) – max PW age (15) – Min PW age (3) – Min PW length (8) – PW must meet complexity reqmt – enable.

10.	**Account Lockout policy implemented** :- Run cmd – secpol.msc – account policies – Acct lockout policies – Acct lockout threshold (3 invalid logons) – ok.
11.	**Audit Policy Implemented** :- Run cmd – secpol.msc – local policies – audit policies – double click on every option – check success & failure box – ok.
12.	**Ctrl + Alt + Del Disabled** :- Run cmd – secpol.msc – local policies – security options – interactive logon : Do not reqd Ctr+Alt+Delete – disable.
13.	**Display Last User Name Enabled** :- Run cmd – secpol.msc – local policies – security options – interactive logon : Do not display last user name – enable.
14.	**Clear Virtual Memory enable** :- Run cmd – secpol.msc – local policies – security options – Shutdown clear virtual memory pagefile – enable.
15.	**SCCM installed for Intranet** :- Contact to Seg Det.
16.	Encryption Tool Installed / Not Being Used. (S Desk/V Crypt/True Crypt)
17.	**USB Port Disable** :- Run cmd – regedit – Hkey local machine – system – services – control set1 – services – USBSTORE – start – change value 3 to 4. Do same procedure in Controlset001, 002 and CurrentControlSet. Run cmd – gpedit.msc – cmptr configuration - administrative templates – system – Removable Storage Access – enable removable disks 1. Deny execute, 2. Deny read, 3. Deny write access. Do same procedure in User configuration.
18.	**Folder Sharing exists** :- Run cmd - regedit – Hkey local machine – system – services – control set1 – services – Lanman server – parameters – rt click in right side pan – new - select DWORD (32Bit) or QWORD (64 Bit) – rename new value #1 to AutoShareServer and again - – rt click in right side pan – new - select DWORD (32Bit) or QWORD (64 Bit) – rename new value #1 to AutoShareWks. Do same procedure in Controlset001, 002 and CurrentControlSet.
19.	**Foreign IP address disable** :- Run cmd – ncpa.cpl – double click on local area connection – properties – uncheck – IPV 6.
20.	**Open ports (135-139,445,5800,5900,3389)** :- Control panel – windows firewall – advanced setting – rt click on inbound rules – new rule – port – next – type in specific local ports ‘135-139,445,5800,5900,3389’ – next – block the connection – next – next – type name ‘Cyber’ – finish. Same procedure in Outbound rues.
21.	**Firewall on** :- Control panel – windows firewall – turn windows firewall on or off – check on ‘Turn on windows firewall’ two places.
22.	**Remote Assistance Disable** :- Rt click on my cmptr – properties – remote setting – in remote tab - in remote assistance option - uncheck ‘Allow remote assistance connection to this cmptr’ – in remote desktop option – check ‘don’t allow connection to this cmptr’ – apply – ok.
23.	**Disable Services** Run cmd – services.msc – select & disable following services Bluetooth support services Computer Browser (standalone)

	Distributed Link Tracking Client Fax FTP Publishing (Win XP) IIS Admin (Win XP) IP Helper Net meeting Remote Desktop Sharing Remote Desktop Remote auto connection manager Remote Registry Routing & Remote Access SNMP (Service / Trap) SSDP Telnet Wireless (‘0’Configured/Auto Configured