MINISTRY OF DEFENCE
DEPARTMENT OF DEFENCE PRODUCTION
DTE OF STANDARDIZATION

Cyber Security Policy
2019

Contents

DTE OF STANDARDISATION
DEPARTMENT OF DEFENCE PRODUCTION
MINISTRY OF DEFENCE
CYBER SECURITY POLICY – 2019

1. Overview

Due to rapid proliferation of information technology (IT) and its direct impact on the functioning of an organization, IT and its functional ecosystems can no longer be viewed in isolation. Proliferation of IT has its flipside too; that of induced vulnerability to threat of cyber crimes. Hence it has become organizationally imperative to safeguard the official cyber space from nefarious cyber crimes keeping the overall threat in perspective

On July 2, 2013, the Indian government has released the National Cyber Security Policy 2013. This Policy aims at protection of information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to cyber threats and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation.

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

(a) Designating a national agency to coordinate all cyber security matters.

(b) Encouraging all private and public organizations to designate a Chief Information Security Officer responsible for cyber security.

(c) Developing a dynamic legal framework to address cyber security challenges in the areas of cloud computing, mobile computing and social media.

(d) Operating a National Critical Information Infrastructure Protection Center; Promoting research and development in cyber security.

(e) Enhancing global cooperation in combating cyber security threats.

(f) Fostering education and training programs in cyber security.

(g) Establishing public and private partnerships to determine best practices in cyber security.

1.1 The key considerations for securing the cyber space include:-

1.1.1 The security of cyber space is not an optional issue but an imperative need in view of its impact on national security, public safety and economic well-being.

1.1.2 The issue of cyber security needs to move beyond traditional technological measures such as anti-virus and firewalls. It needs to be dynamic in nature and have necessary depth to detect, stop and prevent attacks.

1.1.3 Cyber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action.

1.1.4 Effective correlation of information from multiple sources and real-time monitoring of assets that need protection and at the same time ensuring that adequate expertise and process are in place to deal with crisis situations.

1.1.5 There is a need to focus on having a suitable security posture and adopt counter measures on the basis of hierarchy of priority and understanding of the inter dependencies, rather than attempting to defend against all intrusions and attacks.

1.1.6 Security is all about what people, process and technology should do and as such there is a clear need for focusing on people and processes while attempting to use the best available technological solutions, which otherwise could prove ineffective.

1.1.7 Use of adequately trained and qualified manpower along with suitable incentives for effective results in a highly specialized field of cyber security.

1.1.8 Security needs to be built-in from the conceptual design stage itself when it comes to developing and deploying critical information infrastructure, as opposed to having security as an afterthought.

1.2 Information and Communication Technologies (ICT) follow open-system architectures and standard communication protocols which are public domain knowledge. Therefore, networks and systems are vulnerable to interception, compromise, and denial of information/service unless secured by appropriately designed security measures. The formulation of comprehensive cyber security policy covering people, processes and technology issues is the starting point in establishing Information Security Management System (ISMS). The cyber security procedures and guidelines will emerge from this policy and will form the other important documents for implementing cyber security within all entities of DDP.

1.3 The current IT environment in DDP has both networked and stand alone systems. Though the networks are isolated from the Internet due to air gap being maintained, the unsupervised use of removable storage media could plug this vital gap and make our networks vulnerable to threats that exist on Internet. A major reason for loss or theft of classified information in any organisation is due to the misuse of removable storage media. As the security controls for management of removable storage media is more procedural oriented rather than technology, it will be the command responsibility to ensure proper accounting and use of such devices.

1.4 Security of information is paramount for any computer networks. In addition to the Confidentiality, Integrity and Availability of information Authentication and Non Repudiation form other important key security features of such networks. To safeguard the confidentiality of information, encryption plays an important role in storage and transmission of information.

1.5 The implementation of cyber security is based on the guiding principle that the head of the establishment will be the owner of the information assets of the establishment. To protect information assets, the owner will be responsible for assigning the security classification of all the information assets and appropriate clearance levels for the staff accessing these assets.

1.6 The Policy is applicable to all users of information resources as well as personnel tasked to undertake the administration of information systems and resources. All Departments under DDP, Ministry Of Defence will adhere to the guidelines given in this policy.

2. Scope

The policy will be read in conjunction with other instructions on the subject issued by Department of Defence Production and Ministry of Defence, Government of India from time to time. All efforts have been made to make the policy comprehensive. However, all organizations may incorporate any instructions / guidelines which they feel are relevant in their environment and requirement pertaining to computer security.

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels at Dte of Standardisation, as may be appropriate to address the challenging requirement of security in the cyber space. This policy may be treated as a broad guideline for maintaining a safe and secure cyber environment in Dte of Standardisation by which the individual organisation may derive their cyber security policy based on this template as per their requirements/context for business plans.

3. Standards and Review

This policy is based on and must be read in conjunction with the following documents:

(a) National Cyber Security Policy 2013

(b) National Information Security Policy And Guidelines (NISPG) ver 5.0

(c) Gazette of Govt of India dated 18.02.2015 on usage of IT resources in GOI and Email Policy for officers of GOI.

(d) Information Technology (IT) Security Guidelines given by Department of IT, Ministry of Communications & IT, Govt of India.

(e) National Cyber Security Crises Management Plan 2015

(f) ISO/IEC 27001 (ISMS)

(g) Cyber Security Framework issued by DDP

(h) Cyber Security Policy Template 2018 issued by DDP

The policy will be reviewed on change of threat perception or occurrence of a major security incident.

4. Aim

The aim of this policy is to build a secure and resilient cyberspace for Directorate by laying down cyber security policy for establishing, implementing, monitoring, review and management of information infrastructure.

5. Objectives

5.1 The objectives of this policy are:-

5.1.1 To ensure availability of networks and information systems etc with embedded software.

5.1.2 To prevent loss, damage, modification or misuse of information by preventing unauthorised access, damage and interference to information infrastructure.

5.1.3 To create a secure cyber ecosystem for maintaining integrity of ICT products and services, including embedded software in devices weapons, platforms and munitions.

5.1.4 To create and enhance infrastructure for response, resolution and crisis management.

5.1.5 To enhance the protection and resilience of Department of Defence Production, Defence Public Sector Undertakings & Ordnance Factory Board critical information infrastructure and mandating security practices.

5.1.6 To prevent unauthorized access, damage and interference to information infrastructure.

5.1.7 To provide directions and support for Information Assurance and Risk Management (RM) in DoS organization.

5.1.8 To lay down guidelines for incident response within the DoS Organisation.

6. Organization Structure of Cyber Security Group – DoS

The organization Structure of Cyber Security Group- DDP is given in Annexure A.

6.1 Cyber Security Group – DoS The Cyber Security Group under Chief Information Security Officer of Dte of Standardisation, will act as a nodal agency to maintain the Cyber Security in DoS. All Alerts, Advisories, guidelines, policies etc issued by various national level agencies shall be disseminated through CSG-DoS.

6.2 Data Network Center (DNC) : The Data Network center constitutes the apex executionary body in the Dte of Standardisation and shall be responsible for enforcing the Cyber Security at Dte level. The respective Joint Directors are responsible for implementation of guidelines and practices at the group level.

6.3 CISO and Cyber Security Officer: As per the DDP cyber policy the Director shall nominate a CISO who will be a senior level officer and OIC (DNC) as Cyber Security Officer. The CISO shall be responsible for formulating cyber security policy and ensure implementation and operational effectiveness of cyber security measures within the organization. The CISO of the organization shall brief the Director about the Cyber Security progress once every quarter.

7. Responsibilities of Stake Holders

7.1 Responsibilities of Head of Organization

The overall responsibility for Cyber Security lies with the Head of the respective Organization. The Board of directors shall periodically review the risk and monitor progress of the Cyber Security activities in the Dte. Following needs to be ensured:-

7.1.1 Adequate funds are provisioned for cyber security activities.Cyber security audits are conducted at planned intervals as per policy and framework guidelines.

7.1.2 Ensure Inspection of each and every computer regarding implementation of Computer Security instructions. The audit observations should be meticulously recorded and they should be resolved with due monitoring.

7.1.3 Periodic cyber security audits are carried out by the Sectoral Cyber Security Cells to monitor the implementation and effectiveness of cyber security measures.

7.1.4 Each establishment clearly defines the ownership of IT asset and overall responsibility for protection of all information assets.

7.1.5 Users and administrators of information systems and networks undergo regular awareness and training on cyber security. The training of all users and Cyber security personnel should be so designed that it ensures the desired level of security compliance by each organisation as per the security needs of that organisation.

7.2 Responsibilities of System & Network Administrator: DNC

The responsibility for network operation, design, deployment, management and security of all Wide Area Networks and Local Area Networks including perimeter defence devices such as Firewalls, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) etc.

Precautions for detection, prevention and recovery controls to protect against malicious code, patch management, password management, profile management, disaster management, backup & restore, management of e-waste, security control configuration and appropriate user awareness procedures to be in place.

7.3 Employees Responsibility

The users of the respective groups must have the responsibility to use IT resources in an efficient, effective, ethical and lawful manner.

Users have the responsibility and accountability towards usage of unauthorised software, computing resources, removable media, password protection & management, wireless devices, storage of classified data.

8. Implementation of Policy

The CISOs shall ensure implementation of this Policy in the Organization & all its units through respective Information Technology Heads.

9 Human Resource Management

Human resource is the backbone of cyber security domain. All aspects of cybercrime directly or indirectly are triggered by human resource. Human Resource management is the first and foremost step towards ensuring a secure cyber environment. Appropriate training and Checks must be provided for awareness and pro-active defence mechanism. Measures related to verification, contracts of employment, nondisclosure agreements, contracts with third party, Do's and Don'ts, responsibility and commitments etc., must be enforced during various stages of engagement.

Disciplinary Process: All violations to the cyber security policy must be logged and tracked, all offences to be categorized and dealt as per the IT Act 2010 and any amendments thereof.

10 Asset Management and Holders Responsibility

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

10.1 **Inventory Management** All assets are clearly identified and an inventory of all assets drawn up for taking into consideration the asset owner, location, warranty/AMC information and a brief specification to be maintained.

10.2 **Allocation & Return of Assets** Asset owner will carry out proper handing/taking over of all information assets in his/her possession upon transfer or relinquishing of appointment including secure deletion of information, if any.

10.3 **Removal of Access Rights** The access rights of all users of information and information processing facilities will be removed immediately upon transfer or relinquishing of appointment.

10.4 **Access Privileges** The access control and access rights to be defined for all the IT assets and physical/logical access to be defined.

11 Physical & Equipment Security

11.1 Physical Security

11.1.1 **Secure Areas** Classified information processing facilities will be housed in secure areas, protected by a defined security perimeter implemented through state of the art physical security systems. Entry to secure areas will be controlled, regulated and monitored to ensure that only authorised personnel are allowed access.

11.1.2 **Physical Security Perimeter** Security perimeters (such as Electrical fencing, Surveillance systems, access card controlled entry points or manned reception desks) will be used to protect areas that contain information and information processing facilities.

11.1.3 **Protection against External and Environmental Threats** Physical protection against damage from fire, flood, lightening and other forms of natural or man-made disasters will be applied. Fire detection and suppression systems will be provided in compliance with existing orders at all critical information and network nodes. Lightening protection system will be installed in all premises housing critical information processing facilities.

11.2 Equipment Security

11.2.1 **Support Utilities** Equipment will be protected from power failures and other disruptions by having adequate standby arrangements.

11.2.2 **Network Cabling** All network cabling and test points will be protected from unauthorised interception and damage. Physical check of cables to detect tampering will be carried out as part of the existing security checks at all levels.

11.2.3 **Equipment Maintenance** Equipment will be correctly maintained to ensure its continued availability and integrity. Before sending a computing device for repair or maintenance, all primary storage media like hard-disks and secondary storage devices will be removed from the computer system and kept at secure location with the user or persons nominated within an establishment. The repair and maintenance will be carried out and tested using test drives available with such repair and maintenance agencies in the presence of an IT skilled nominated person of the establishment. Internal drives will be securely erased and formatted when relocated for fresh installation.

11.2.4 **Secure Disposal or Re-Use of Equipment** Devices containing critical information will be securely disposed off. Prior to disposal or reuse of an equipment the information will be destroyed, securely deleted or overwritten to make the original information non-retrievable rather than using the standard delete or format function.

11.2.5 **Tempest Proofing** Eavesdropping through capture and processing of electromagnetic radiation will be prevented for highly classified systems.

12 Network Security

12.1 **Network Security Management Controls** Networks will be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit by incorporating appropriate security solutions at physical, network, transport and application layers.

12.2 **IP version 6 (IPv6)** is a new version of the Internet Protocol, designed as a successor to the current IP version 4 (IPv4). IPv6 will not only solve the problem for address space shortages but also provides efficient management of address space, enhanced security support and elimination of network address translation. All network devices procured for the Dte will incorporate IPv6 protocol suite for ease in migration of existing IPv4 devices to IPv6 in a phased manner. Adequate bandwidth will be built up to cater to the requirements of voice, data and video conferencing.

12.3 **Network Entities:** Networked computers will have only Network Printers and Network Scanners and will not be connected to individual printers and scanners. Depending on the sensitivity of the data being handled, the printer/scanner will be shared among a defined close user group. Standalone printers and scanners required in case of non networked environments will be appropriately monitored by the nominated Network Administrator of the establishment. In addition, networked computers will not have writing devices like CD/ DVD writers etc. All computers will have their CD/ DVD writers removed and USB ports controlled/disabled.

13 Mobile Telecom Security

13.1 When using mobile computing devices such as notebooks, palmtops, laptops, and PDAs etc special care will be taken to ensure that information is not compromised or lost due to theft. Technologies like Wi-Fi, Blue Tooth, GPRS, Wi-Max etc. will not be used. The responsibility of disabling these Services, if available in any IT equipment, is of the user of the equipment.

13.2 All official information stored/ kept on portable media will be in encrypted form. Secure erasing of files on mobile computing devices will be ensured before reuse.

13.3 Appropriate standard operating procedures will be established at all levels based on this policy for accounting and protection of mobile computing devices from damage, theft and unauthorised access.

13.4 Voice communication networks are subjected to wide range of security issues, including eavesdropping, call misdirection, identity misrepresentation and information theft. Authentication and encryption of data from IP telephones and terminals to servers will be implemented to secure VoIP communication.

14 Security in Support Processes

14.1 Change Control Procedures

The implementation of changes will be controlled through formal change control procedures. Introduction of new systems and major changes to existing systems will be properly documented. The process will ensure that existing security and control procedures are not compromised.

14.2 Technical Review of Applications after Operating System Changes

Application control and integrity procedures will be reviewed to ensure that they have not been compromised by the operating system changes.

14.3 File Integrity

File integrity check for both operating system and application software will be implemented.

14.4 Disabling Unwanted Services

All unwanted default services must be disabled on a given operating system. Only those utilities will be enabled on computers, which are required by the user.

14.5 Authorized Software

Only authorized, licensed, updated and open source software will be used.

14.6 Outsourced Software Development

Outsourced software development will be supervised and monitored by the concerned establishment.

14.7 Cloud Services:

Cloud computing envisages use of computing resources that are delivered as a service over a network. The infrastructure of cloud entrusts remote services with a user's data, software and computation of the information/ data stored on remote servers. Hence it is necessary for the organisation to ensure that the security of the data is not compromised while hiring cloud services. Following addition measures will be adopted to ensure security over cloud services.

(a) The cloud services are hired preferably from Government/ PSU agencies.

(b) Ensure that cloud provider is using strong encryption methods.

(c) Data backup may be managed by the organization/ enterprise itself.

(d) There must be barriers to keep critical information separate from other information and organisations.

(e) Cloud-Organization and Cloud-Cloud inter linkages must be secured.

(f) It should be ensured that the information data is accessible to authorized users only.

(g) Logs at provider's end should be maintained and stored in encrypted from. Access to logs must be limited to minimum persons.

(h) Security related issues/ aspects may be covered under Service Level Agreements (SLA).

(j) As a rule, access to critical information should be minimum particularity from mobile endpoints. In cases, when it is required to access the information from mobile endpoints, their access points,devices or end points must be secured. This is equally applicable to cloud connectivity as well.

(k) There should be adequate authentication mechanism to avoid any chances where an attacker can pose as a cloud subscriber.

(l) Threat/ Risk management and mitigation strategy on cloud security should be part of IS Policy.

(m) There should be a breach reporting mechanism for any security related incident not only in the data that provider holds for subscriber but also the data it holds about the subscriber.

(n) Client side and server side systems must be protected by timely updating, patching etc.

(o) Access to information, network services, operation system, application and system should be controlled.

15 Secure Configuration and Access Control

15.1 Logical Access Control

15.1.1 **User Authentication** All systems and devices will implement strong pass phrase based authentication. In addition, the classified systems will have two/ three factor authentication implemented to prevent unauthorised access to systems and devices based on the classification of info/data being handled.

15.1.2 **User Access Control** The access control policy will ensure Role Based Access Control. Information systems that process classified data will have Mandatory Access Controls (MACs) in place. Following additional measures will be adopted:-

15.1.2.1 **User Registration** There will be a formal user registration and de-registration procedure in place for granting and revoking access to information systems and resources.

15.1.2.2 **User Privilege Management** The allocation and use of privileges will be restricted and controlled. Principle of least privileges will be followed while using systems and services.Multi-user systems that require protection against unauthorised access will have allocation of privileges controlled through a formal authorisation process.

15.1.2.3 **Review of User Access Rights** The access control rules and rights will be periodically reviewed and redundant user IDs and accounts will be investigated and removed.

15.1.2.4 **User Password Management** The allocation of passwords will be controlled through a formal password management process. Users will follow password guidelines in the selection and use of passwords.

15.1.2.5 **Password Use** Users will be required to follow best security practices in the selection and use of passwords.

15.1.2.6 **Unattended User Equipment** Users will ensure that unattended equipment has appropriate physical and logical protection.

15.1.2.7 **Clear Desk and Clear Screen Policy** No removable storage media will be left unattended in office desks and work areas. All desktops and servers will have clear screen policy when not in use.

15.2 Network Access Control

Access to both internal and external network services/resources will be controlled.

15.2.1 **Policy on Use of Network Services** A policy on the use of networks and network services/resources will be formulated which must be consistent with the access control policy. The policy must clearly specify the networks and network services/resources which are allowed to be accessed.

15.2.2 **User Authentication for External Connections** Appropriate identification, authentication and authorisation methods will be used to control access by remote users.

15.2.3 **Equipment Identification in Networks** Equipment identification will be implemented to authenticate connections from specific locations and devices.

15.2.4 **Remote Diagnostic and Configuration Port Protection** Many information processing facilities and systems require remote diagnostics by maintenance engineers. Physical and logical access to diagnostic and configuration ports will be controlled and monitored. Remote management of network devices will be done only through secure communication channels.

15.2.5 **Segregation in Networks** Groups of information services, users, and information systems will be segregated by deploying secure gateway appliances.

15.2.6 **Network Connection Control** For shared networks, the capability of users to connect to the network will be restricted in line with the access control policy and requirements of the applications. The connection capability of users will be restricted through network gateways that filter traffic by means of pre-defined tables or rules.

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

15.3 Operating System Access Control

15.3.1 **Secure Log-on Procedures** Access to operating systems will be controlled by a secure log-on procedure. Log on credentials will neither be transmitted nor stored in clear. Multi factor authentication mechanisms based on the principal of “something you know” (Password, pass-phrase, PIN etc), “something you have” (Token,

memory card, smart card etc) and “something you are” (Biometric devices) will be incorporated for critical systems.

15.3.2 **Use of Unlicensed Software** No unlicensed/ pirated software will be used by users in official systems as they may contain malicious code.

15.3.3 **Session Time Out** Inactive sessions will be made to shut down after a defined period of inactivity. The sessions should be shut down to prevent access by unauthorized persons and denial of service attacks. Time-outs can be tuned to clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity.

15.3.4 **Limitation of Connection Time** Restrictions on connection times will be used to provide additional security for high-risk applications. Such critical applications must have multi-layered authentication mechanisms incorporated.

15.4 Application and Information Access Control

15.4.1 **Information Access Restriction** Logical access to application software and information will be restricted to authorised users only.

15.4.2 **Classified System Isolation** Classified systems above CONFIDENTIAL will have a dedicated and isolated computing environment.

16 Monitoring

16.1 Integrity Management

The integrity of system hardware configuration info and critical software files will be maintained and monitored/tracked to ensure any unauthorized activity on the systems and networks.

16.2 Audit Logging

Audit logs recording user activities, exceptions, and information security events will be maintained to enable future investigations and access control monitoring.

16.3 Monitoring System Use

Procedures for monitoring use of information processing facilities will be established and the results of the monitoring activities reviewed regularly.

16.4 Protection of Log Information

The log information will be protected against tampering and unauthorised access.

16.5 Administrator Logs

Administrator activities will be logged.

16.6 Fault Logging

Faults will be logged, analysed, and appropriate action will be taken.

16.7 Clock Synchronization

For static networks the clocks of all devices and systems will be synchronised with an agreed accurate time source to ensure incident tracking and log analysis.

17 Cryptographic Controls

17.1 Information Classification

Information in electronic form will be classified as per the Nature of Information Content in the Documents.

17.2 Classified System Isolation

Systems handling/processing classified information with security classification of CONFIDENTIAL and above will have a dedicated and isolated computing environment. All such systems will be housed in a secure area with stringent physical access control mechanisms in place.

17.3 Secure Transfer of Classified Information

The information owners will ensure that the security classification of the information required to be transferred over a network must commensurate with the security classification of the network/media.

17.4 Secure Storage

17.4.1 Storing SECRET and TOP SECRET Information in Electronic Form

17.4.1.1 Classified information above CONFIDENTIAL, will not be stored permanently on a computer.

17.4.1.2 Whenever there is a requirement of storing classified information above CONFIDENTIAL in electronic form, such information will be transferred to a removable storage media such as external hard disk, DVD, CD, etc and all such media will then be handled as per the procedures for handling documents of similar classification.

17.4.1.3 After such information has been transferred to an external removable media, it will then be securely erased from the originating computer/media. It will be ensured that there is no data remanence in the originating computer including page files, swap areas, slack areas, RAM etc.

17.4.1.4 Secure methods and erasers may be used to securely delete classified data files from the originating computer. Hard Disks should be defragmented and the appropriate tools be used for wiping out free space.

17.4.1.5 To safeguard against loss/theft of classified data in storage media, encryption techniques will be used to ensure confidentiality of data at rest.

17.4.2 Storing classified Information Up to CONFIDENTIAL in Electronic Form

All classified information up to CONFIDENTIAL when stored on hard disks or any other secondary memory device will be encrypted using encryption software.

17.4.3 **Disk Partition:** The device or partition of a hard disk which will host the data will be separate from the device or partition of hard disk on which operating system and applications are installed.

18 Operational Control

18.1 Standard Operating Procedures

SOPs will be developed and documented to ensure adequate responsibilities and accountability for implementation and monitoring of cyber security measures. Following SOPs will be maintained by each establishment specific to their functioning:-

18.1.1 Responsibility for security.

18.1.2 Internal security audit.

18.1.3 User access management.

18.1.4 Network access control.

18.1.5 Patch and virus management.

18.1.6 Handling of removable media and portable computing devices.

18.1.7 Incident reporting and handling.

18.1.8 Backup and recovery for business continuity.

18.1.9 Repair and maintenance.

18.1.10 Installation of software.

18.1.11 Starting and stopping of classified applications and security solutions.

18.1.12 Key Management.

18.1.13 Change Management.

18.1.14 Crisis Management

18.1.15 Third Party Services

18.2 Change Management

Operational systems and application software will be subject to strict change management control to ensure that all changes to equipment, software or operating procedures are duly analyzed, approved, supervised and carried out in a controlled manner to prevent inadvertent failures.

18.3 Segregation of Duties

Duties and areas of responsibility will be segregated to reduce opportunities for unauthorised or intentional modification or misuse of the organization’s assets.

18.4 Controls against Malicious Code

Prevention, detection and recovery measures to protect against all types of malicious codes like virus, spy ware, etc. will be implemented on all desktops, servers and at the gateways to the internal networks.

18.5 Patch and Signature Management

All devices and system software will be kept updated with the latest patches and signatures to ensure protection against known vulnerabilities at all times. The network administrator shall remain updated on the latest vulnerabilities notified by CERT-In.

18.6 Back-Up

Back-up of information and software will be taken and tested regularly in accordance with the backup policy of the establishment and criticality of information.

19 Handling of Storage and Removable Media

19.1 Management of Removable Storage Media

All secondary mass storage devices such as CD/DVD Writers, removable hard drives, etc when authorised for use by the head of the establishment will be properly controlled and accounted for by the nominated controlling officer. Instructions on storage of classified documents on removable media as well as computer systems will be adhered at all times. Any data to be copied from a computer into a secondary storage device will have the authorisation of a nominated controlling officer and records of the same maintained. Transfer of data between networked computers will be done through the network only.

19.2 Management of Drives/Ports

In order to prevent information theft, all writable drives like DVD/CD Write drive, USB Ports etc. will be securely disabled using appropriate software on all computers, including standalone computers held with the clerical staff. However, when authorised by the appropriate authority due to need for data backup and/or emergency transfer of data warranting use of such devices/ports, they will be enabled / configured only on computers of nominated officers in a given establishment for the specific period only. In addition, computer having classified information will not have internal CD writer. Based on the minimum inescapable requirement, a given establishment will have only a few external CD writers held with the nominated controlling officer. Similarly a minimum number of Internal CD writers, if required will be retained only with the nominated officers in the establishment. Access to such devices will be controlled by means of appropriate hardware and software mechanisms. A record of data burnt on CDs/ DVDs will be maintained.

19.3 Retention of Removable Media

Existing policies and guidelines on retention of documents in physical forms will be applicable to the documents stored in electronic form.

19.4 Disposal of Storage Media

Storage media will be disposed of securely when no longer required, by physically destroying the storage media under a board of officers.

19.5 Security and Storage of System Documentation

System documentation will be protected against unauthorised access by storing them in appropriate storage drive with desired access and encryption levels.

20 Electronic Messaging

20.1 Information sent through electronic messaging will be appropriately protected against incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay and denial of service. E-mail attachment will not be opened directly. It will be saved on the media and duly scanned for malware before use.

20.2 E-mails received and sent for an account holder shall have default retention policies as laid down by each organisation. Appropriate backup shall be ensured prior to application of the retention policy.

21 Internet

21.1 Air Gap

A computer used for creating and storing official documents/information or a networked computer connected on a LAN will not be connected or used to access the Internet. No mobile phones with internet facilities will be connected to any computer being used for official purposes. The computer name of the internet computer shall not reveal the appointment or the establishment's identity. All down loaded data will be duly scanned for malware before use.

21.2 Resource for Internet Access

Designated computer having NO official data/ information can only be used to access Internet. No official or classified official work will be carried out on computers connected to Internet. Even if the content bears no classification, any work that can lead to security breaches or can jeopardize the organisational functioning/National Interests should not be carried out on the computers connected to the Internet. No removable media containing official information will be placed in or connected to the computer connected to Internet.

21.3 Website Hosting

All Internet web site to be designed by NIC empanelled vendor & and the same to be audited for GIGW compliance by CERT-In. All Internet websites will be preferably hosted on NIC Web Servers.

22 Information Systems Acquisition and Development

22.1 An authorisation process for new information processing facilities like procurement of Hardware/ Software, establishment of LAN/ WAN, development of software, automation etc. will take into account the existing cyber security policies/guidelines before authorizing the induction of such IT infrastructure to ensure that all relevant cyber security requirements are met.

22.2 **Correct Processing in Applications** To minimize the application level vulnerabilities, all application development will address the security issues at each stage of Software Development Life Cycle (SDLC). Following issues will be addressed during software development:-

22.2.1 **Input Data Validation** Data input to applications must be validated to ensure that this data is correct and appropriate and Input field is not subject to exploitation.

22.2.2 **Output Data Validation** Data output from an application must be validated to ensure that the processing of stored information is correct and controlled.

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

22.2.4 **Message Integrity** Requirements for ensuring authenticity and protecting message integrity in applications will be identified, and appropriate security measures identified and implemented.

23 Embedded Software

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

24 Cyber Audit

24.1 Compliance with Security Policies and Standards

24.1.1 Audit plays a critical role in monitoring implementation of security policies and standards. As a policy auditing in all systems and network devices shall be enabled. The capability to log and audit all print jobs of classified information will also be ensured. At the system level, access to audit logs will be restricted to Cyber Security Officer and administrator only.

24.1.2 **Frequency of Audit** To ensure compliance of cyber security policy each establishment will carry out audits as per the periodicity laid down by DDP.

25 Cyber Crisis and Incident Management

25.1 Cyber Crisis Management

All Functionaries of Information Security Organization will acquaint themselves with “Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism issued by Ministry of Electronics & Information Technology, Government of India to facilitate its implementation in all Organizations.

25.2 Incident Prevention, Reporting and Handling

25.2.1 All cyber security incidents will be reported by Local Cyber Security Cells to Sectoral Cyber Security Cells which in turn will report to CERT-IN and Cyber Security Group – DDP on priority.

25.2.2 Cyber Security Group – DDP will coordinate with CERT-In to obtain alerts and warning of attacks and various actions to be taken to avoid any cyber security incident.

25.2.3 **Learning from Information Security Incidents** Cyber Security Group – DDP will review all reported incidents in consultation with CERT-In and draw out appropriate lessons from these incidents to be used in user awareness training as case studies subsequently.

The Incident Handling Process and the Channel of Reporting is given in Annexure B.

26 User Education, Training and Cyber Security Awareness

26.1 Cyber Security Education and Training

User awareness and training being one of the major cyber security measure, adequate impetus will be given to cyber security training at all levels. Adequate funds for advanced/outsourced training, whenever required will be made available.

26.2 Cyber Security Awareness

(a) To promote and launch a comprehensive Cyber Security Awareness Program in relation to national awareness program on security of cyberspace.

(b) To sustain security literacy awareness and publicity campaign through electronic media to help the staff of organisation to be aware of the challenges of cyber security.

(c) To conduct, support and enable cyber security workshops/ seminars and certifications.

27 Information Sharing and Co-operation

(a) To develop bilateral and multi-lateral relationships in the area of cyber security with other cyber entities in the country.

(b) To enhance National cooperation among security agencies, Law Enforcement Agencies and judicial systems.

(c) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resistance of systems including critical information infrastructure.

28 Promotion of Research & Development in Cyber Security

(a) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals in cyber security technology. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

(b) To encourage Research & Development to counter a wider range of cyber security challenges prevailing in cyber field.

(c) To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.

(d) To set up Centres of Excellence and Security Operational Centres (SOCs) in areas of strategic importance for the point of security of cyber space.

(e) To collaborate in joint Research & Development projects with industry and other research organisations in frontline technologies and solution oriented research.

29 Business Continuity Plan/ Contingency Plan

A business continuity process and Disaster recovery management process for IT systems should be in place to minimize the impact of any disaster on the organisation. This to be achieved by:

29.1 Develop the continuity planning policy statement

29.2 Conduct the Business Impact Analysis (BIA)

29.3 Identify preventive controls

29.4 Develop recovery strategies

29.5 Develop contingency plan

29.6 Test the plan and conduct training and exercises

29.7 Maintain the plan.

Business continuity should be a part of the security program taking into consideration the threats to the organisation. Preventive mechanisms to be put in place to reduce the possibility of the organization's experiencing a disaster or lesson the amount of damage if a disaster does hits. Recovery strategies by defining the recovery mechanism and strategies on how to rescue the organisation to be

implemented in terms of business process recovery, facility recovery, supply and technology recovery, user environment recovery and data recovery.

30 Risk Management

Risk Management along with business discipline if applied can ensure a business continuity continuous to achieve a strategy for profitable growth. What impacts the organisation in a negative way and having an action plan for each threat with applicable probability and severity is to be put in place. In any business servers will fail, attacks will persist and some will eventually succeed therefore it is important to forecast uncertainty, map the threats and create counter measures to potential threats as it pertains to the use of technology within an enterprise.

IT risk management framework must focus on:-

(a) Identify the threats

(b) Map the severity and probability of each threat

(c) Determine the impact of each threat

(d) Implement control recommendations

31 Do's and Dont's

Certain conventional cyber security norms and best practices are enlisted as do's and dont's and followed at the Dte of Standardisation. They are attached as annexure B.

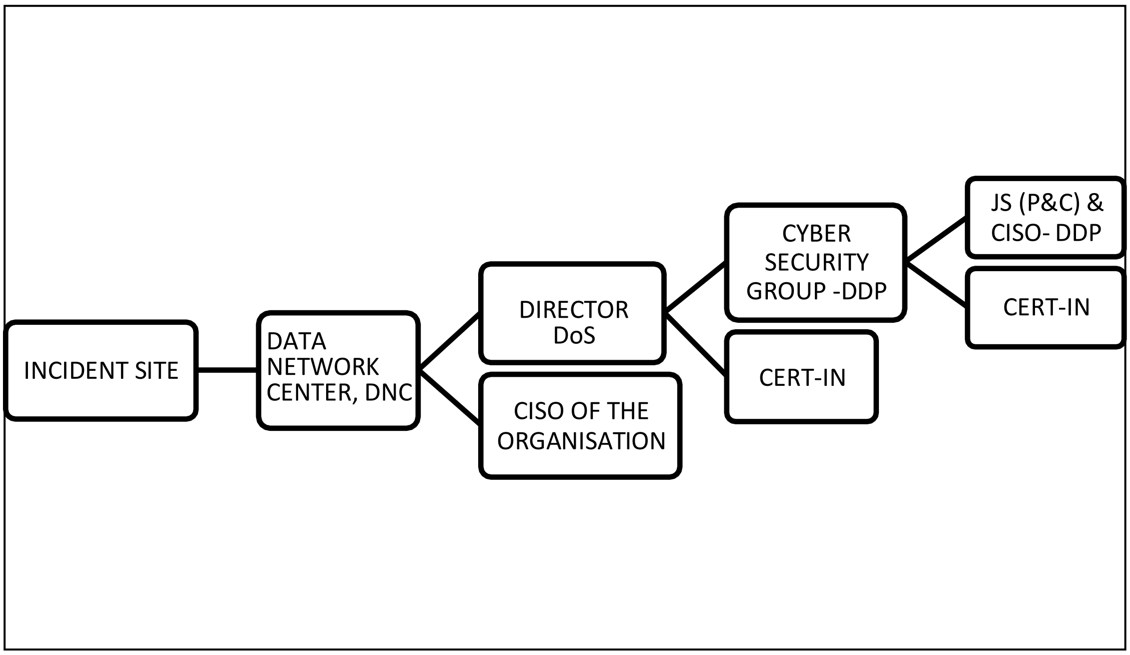
32 Summary

32.1 Information has been an important part of any organization. With ever increasing dependence on Information and Communication Technologies (ICT) for conduct of warfare and the emerging threats in cyberspace, security of information in storage, processing and transmission is the greatest challenge. However, adoption of secure technologies, with proper configuration and use of encryption technologies along with procedural control will make deployment of networks and information systems for conduct of network centric operations a reality at Dte of Standardisation.

Annexure A

(Refers to paragraph 25 of DoS Cyber Security Policy – 2019)

CHANNEL OF REPORTING



Annexure B
(refers to paragraph 31 of the
DoS Cyber Security Policy 2019)

DO's AND DONT's: CYBER SECURITY

DO's

1. Ensure physical security of computer/ laptop and other IT assets.

2. Ensure effective physical access control procedures by using multi-level passwords.

3. Always use screen saver password, user login password and power on password.

4. The passwords must be a complex one and hard to guess, change them every 15 days.

5. The contents of CDs and flash drive are as good as written files. The external storage media containing classified data should be marked and treated like other classified documents.

6. All classified documents must be stored in an encrypted form in PCs as well as external storage devices.

7. In a multi user system, a user log to be maintained.

8. Before deleting the sensitive files, overwrite the files with some junk data to prevent restoration of sensitive data by any means or delete the data by using secure delete option.

9. Avoid storing of files on desktop and C drive of the PC.

10. CD drive to be disabled and external CD writers are to be kept under the custody of Gp 'A' officer only.

11. Ensure safe custody of computer storage media like CDs/DVDs, pen drive etc.

12. Every new incoming storage media and software should be tested for malwares.

13. Always use original software purchased from the authorized vendors.

14. Use a standalone computer for internet work and no official work is to be permitted on that PC.

15. Ensure proper marking of removable media like CD/DVD. The defective CD/DVD to be physically broken and destruction certificate for the same to be kept for auditing purposes.

16. Always use UPS to ensure uninterrupted power supply and to prevent any corruption of data and software.

17. Ensure centralized printing of all documents. Network printer must be located in a secure place.

18. Maintenance and rectification of PC faults to be undertaken in the presence of individual user. Under no circumstances the PC to be handed over to outside maintenance engineer alone.

19. Always keep the PC updated with antivirus and OS update patches.

20. Portable storage media used on internet machine to be scanned for spyware, Trojan viruses and other suspicious malware before being used on departmental LAN systems.

21. Ensure first boot device is the internal HDD.

22. Install latest software patches.

23. Install a personal firewall.

24. Never log in as Admin for day to day work.

25. Take regular backups.

26. Disable services that are not required.

27. Always lock account while leaving the computer.

28. Encrypt sensitive data on HDD.

29. Wipe data from unused portion of the disk.

30. **Local Security Policy**:

(a) Show a customized warning screen.
(b) Only have one Admin account.
(c) Set a strong Password policy.
(d) Set a strong Account lockout policy.
(e) Disable file sharing.
(f) Enable auditing.
(g) Disable Guest account if not required.

31. Stay alert and report suspicious activity.

32. Always use password protect for sensitive files and devices.

33. Be cautious of suspicious e-mails and links.

34. Delete information when it is no longer needed.

35. Be aware of your surrounding when printing, copying, facing or discussing sensitive information.

36. Physically secure your laptop and never leave it unattended.

DONT's

1. Don't let any unauthorized person use your computer system.

2. Never select the "Remember my password" option.

3. Don't share your password with anyone, not even your colleagues.

4. Don't reveal the admin/ root password to any unauthorized person.

5. Do not connect your computer storing classified data to internet.

6. Don't allow staff to bring their own devices or software to run on the official computer.

7. Don't use pirated or gifted copies of software as these may contain viruses and even facilitate intrusion into the system.

8. Don't play computer games. These could be the main carriers of computer viruses for an intruder to break into your computer system.

9. Don't store TOP SECRET or SECRET information permanently in the hard disk of PC. Whenever TOP SECRET or SECRET information is processed on the PC, erase the information immediately from the disk after the processing is over.

10. When CDs or DVDs are used for working on TOP SECERT or SECRET information it should be handled in accordance with the instructions for handling TOP SECERT or SECRET documents. It will be the responsibility of the authorized officer under whose supervision the work is being carried out.

11. Don't carry CDs or removable devices outside the office building. In case a device has to be taken outside the office building, its movement will be with the prior approval of the officer-in-charge. A record of the movement indicating full details like date or time of its being taken out, name of the officer taking it out and purpose, date and its time of its return etc will be maintained.

12. Don't become a member of any unofficial chat club. Don't use official Internet for joining any official chat club.

13. Don't download free songs/ videos or any objectionable material on PCs where official work is carried out as such downloads often contains malware.

14. Do not use pen drives/ USB data storage devices on official PCs.

15. Do not use/ install freely available screen saver on internet as these may have encoded spyware/ Trojan.

16. Don't be tricked into giving away confidential information.

17. Don't use unprotected computers on public networks for carrying out official work.

18. Don't leave sensitive information unattended on your desktop on official PCs.

19. Don't install unauthorised software programs on your office computer.

20. Don’t post any private or sensitive information on any social media.

21. Don’t open mail or attachment from an untrusted source. Report the same immediately as cyber attackers often trick you into visiting malicious sites and downloading malware to steal data & damage networks.

22. Never reply to emails requesting personal or financial information.