MINISTRY OF DEFENCE
DEPARTMENT OF DEFENCE PRODUCTION

Cyber Security Policy 2018

BEML Ltd.
Ver. 0.0

Content

1. Overview 4
2. Scope 7
3. Standards and Review...7
4. Aim 8
5. Objectives..8
6. Organization Structure of Cyber Security Group – BEML LTD. 8
7. Responsibilities of Stake Holders & Assurance Level 10
8. Implementation of Policy..11
9. Human Resource Management 11
10. Asset Management and Holders Responsibility 12
11. Physical & Equipment Security 12
12. Network Security 14
13. Mobile Telecom Security 15
14. Security in Support Processes..15
15. Secure Configuration and Access Control 17
16. Monitoring...20
17. Cryptographic Controls 21
18. Operational Control...23
19. Handling of Storage and Removable Media.........................24
20. Electronic Messaging...25
21. Internet 26
22. Information Systems Acquisition and Development 26
23. Embedded Software 27
24. Cyber Audit...27
25. Cyber Crisis and Incident Management 28
26. User Education, Training and Cyber Security Awareness.....28
27. Information Sharing and Co-operation 29
28. Promotion of Research & Development in Cyber Security....29
29. Business Continuity Plan/ Contingency Plan 31
30. Risk Management...31

31. Summary 32
Annexure A...33
ORGANIZATION STRUCTURE 33
CHANNEL OF REPORTING 34

CYBER SECURITY POLICY – 2018

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.

Being a Ministry of Defence public sector, BEML LTD. has adopted and implemented the CYBER SECURITY POLICY at the end users level and network level covering all the IT infrastructure and required software of the organization. This also helps in protecting the IP(Intellectual property) of the organization from cyber attacks and threats.

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 Organizational level and also at the national level.

To accomplish these objectives, the policy details with numerous action items for the organization is as follows:

- To establish a link with national agencies like CERT-In and DDP Security group to coordinate all cyber security matters.
- To designate a Chief Information Security Officer responsible for cyber security.
- Developing a dynamic legal framework to address cyber security challenges in the areas of cloud computing, mobile computing and social media.

- Enhancing global cooperation in combating cyber security threats.
- Fostering education and training programs in cyber security for all the inmates.

The key considerations for securing the cyber space include:-

- 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.
- 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.
- 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.
- 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.
- 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.

- Use of adequately trained and qualified manpower for effective results in a highly specialized field of cyber security.

- 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.

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 BEML LTD..

The current IT environment in BEML LTD. has both networked and stand alone systems. Though the network is not isolated for air gap purpose the same is achieved in the form of logical separation at router level and firewall level. As per the guide lines of cyber security group BEML LTD. is establishing the air gap network.

A major reason for loss or theft of classified information in any organization 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.

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. Encryption is not applied on data level as the same is used by more than one end user for analysis and statistics purpose.

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. Regular updates of IT infrastructure is being done with respect to IT equipments which includes Desktops and Laptops along with N/w Components as per BEML IT Policy 2016..

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 at BEML Ltd. will adhere to the guidelines given in this policy.

2. Scope

The following are the scope.

- Framing of cyber security policy by referring to MOD Guide lines and other authorities like CERT-In and DDP Security Group issued from time to time.
- Implementation of cyber security policy pan BEML as per the organizational requirement and MOD compliance.
- Audit reports shall to be considered while adopting this policy and improving the security posture of the organization.

3. Standards and Review

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

- National Cyber Security Policy 2013
- National Information Security Policy and Guidelines (NISPG) ver 5.0
- Gazette of Govt. of India dated 18.02.2015 on usage of IT resources in GOI and Email Policy for officers of GOI.
- Information Technology (IT) Security Guidelines given by Department of IT, Ministry of Communications & IT, Govt of India.
- National Cyber Security Crises Management Plan 2015
- ISO/IEC 27001 (ISMS)
- Cyber Security Framework issued by DDP
- BEML IT Policy 2016

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 BEML LTD. by laying down cyber security policy for establishing, implementing, monitoring, review and management of information infrastructure.

5. Objectives

The objectives of this policy are:-

- To ensure availability of networks and information systems and ensure highest assurance levels for al IT devices.
- To prevent loss, damage, modification or misuse of information by preventing unauthorized access, damage and interference to information infrastructure.
- To create a secure cyber ecosystem for maintaining integrity of ICT products and services, including embedded software in devices weapons, platforms and munitions.
- To create and enhance infrastructure for response, resolution and crisis management.
- 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.
- To prevent unauthorized access, damage and interference to information infrastructure.
- To lay down guidelines for incident response within the BEML LTD.

6. Organization Structure of Cyber Security Group – BEML LTD.

Cyber Security Group – DDP The Organization structure of Cyber Security Group at BEML Ltd. shall have the following structure along with DDP organization structure.

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

Corporate and Divisional Cyber Security Cell

- The organization Structure of Cyber Security Group- BEML LTD. is given in Annexure B.

The CYBER SECURITY Group at BEML LTD. shall be formed as follows.

1. BEML Chief Information Security Officer (BCISO)
2. BEML Corporate Cyber Security Group (BCCSG)
3. BEML Divisional Cyber Security Group(BDSCG)

- **BEML Corporate Cyber Security Group (BCCSG)** : This Cyber Security Group familiarly called as 'Sectoral cyber security cell' by DDP. This Cyber Security Group under Chief Information Security Officer of BEML will act as a nodal agency for coordinating activities in relation to computer security incident management for incident reporting and coordination with other Cyber Security Agencies.
- **BEML Divisional Cyber Security Group(BDSCG)**: This Cyber Security Group familiarly called as 'local cyber security cell' by DDP. This group under the Chief Information Security Officer of BEML will act as a nodal agency to maintain the Cyber Security in various divisions of BEML LTD.
- The Higher Management / board of the organization shall constitute the Divisional Cyber Security cell which will operate as an apex body in the respective organization and shall be responsible for enforcing the Cyber Security at organization level. The Local Cyber Security Cells are responsible for implementation of guidelines and practices at the unit level.

- **CISO and Cyber Security Officer**: The CISO of the organization shall brief the board about the Cyber Security progress once every quarter. The

CISO shall also brief the CISO –DDP on quarterly basis on all cyber security related issues pertaining to their organizations. The CSO shall assist in all the cyber security related matters.

- BEML Ltd. has nominated a CISO in the rank of director. CISO has a team in the form of corporate(BCCSG) and divisional Cyber Security Cells(BDSCG).

7. Responsibilities of Stake Holders & Assurance Level

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 organization.

Following needs to be ensured:-

- Adequate funds are provisioned for cyber security activities.
- Cyber security audits are conducted at planned intervals as per policy and framework guidelines.
- 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.
- Periodic cyber security audits are carried out by the division Cyber Security Cells to monitor the implementation and effectiveness of cyber security measures. Division wise cross auditing of IT infrastructure is to be carried out once in six months.
- The ownership of IT asset and overall responsibility for protection of all information assets will be defined. Division wise IT infrastructure list is maintained and circulated to all concerned.
- 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 organization as per the

information security needs of that organization.

Responsibilities of System & Network Administrator

- 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.

Employees Responsibility

- The responsibility and usage of IT assets by the employees is defined in BEML IT Policy 2016.
- Users have the responsibility and accountability towards usage of unauthorized 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. **The violations to the cyber security policy will attract disciplinary action listed under BEML IT Policy 2016**.

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.
- **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. Each asset shall be recognized by a physical number called asset number which will go into books of accounts and form plant ledger of the organization. This shall be used to depreciate the IT assets before salvaging them.
- **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.
- **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.
- **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

Physical Security

- **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 authorized personnel are allowed access.

- **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.
- **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.

Equipment Security

- **Support Utilities** Equipment will be protected from power failures and other disruptions by having adequate standby arrangements. BEML LTD. shall provide all its IT equipment with UPS power with a backup from DG power supply in all its locations.

- **Network Cabling** All network cabling and test points will be protected from unauthorized interception and damage. Physical check of cables to detect tampering will be carried out as part of the existing security checks at all levels. BEML LTD. shall provide suitable network racks placing them at an height of not easily reachable by general public.

- **Equipment Maintenance** Equipment will be correctly maintained to ensure its continued availability and integrity. Before sending out 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.

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

12. Network Security

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.

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 organizations under DDP 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.

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

- 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.
- 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.
- 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 unauthorized access.
- 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

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.

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.

File Integrity

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

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.

Authorized Software

Only authorized, licensed software will be used.

Outsourced Software Development

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

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 organization 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.

- The cloud services are hired preferably from Government/ PSU agencies.
- Ensure that cloud provider is using strong encryption methods.
- Data backup may be managed by the organization/ enterprise itself.
- There must be barriers to keep critical information separate from other information and organizations.
- Cloud-Organization and Cloud-Cloud inter linkages must be secured.
- It should be ensured that the information data is accessible to authorized users only.
- Logs at provider's end should be maintained and stored in encrypted from. Access to logs must be limited to minimum persons.
- Security related issues/ aspects may be covered under Service Level Agreements (SLA).
- 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.

- There should be adequate authentication mechanism to avoid any chances where an attacker can pose as a cloud subscriber.
- Threat/ Risk management and mitigation strategy on cloud security should be part of IS Policy.
- 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.
- Client side and server side systems must be protected by timely updating, patching etc.
- Access to information, network services, operation system, application and system should be controlled.

15. Secure Configuration and Access Control

Logical Access Control

- **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 unauthorized access to systems and devices based on the classification of info/data being handled.
- **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:-
- **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.
- **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 unauthorized access will have allocation of privileges controlled through a formal authorization process.

- **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.
- **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. User authentication shall be created by the Administrator only with initial password. Password policy has been framed under BEML IT Policy 2016.
- **Password Use** Users will be required to follow best security practices in the selection and use of passwords.- Password policy is framed under BEML IT Policy 2016.
- **Unattended User Equipment** Users will ensure that unattended equipment has appropriate physical and logical protection.
- **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.

Network Access Control

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

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.

- **User Authentication for External Connections** Appropriate identification, authentication and authorization methods will be used to control access by remote users.- Organization shall use VPN Client facility.

- **Equipment Identification in Networks** Equipment identification will be implemented to authenticate connections from specific locations and devices.
- **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.
- **Segregation in Networks** Groups of information services, users, and information systems will be segregated by deploying secure gateway appliances.
- **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.
- **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. Organization shall enable VLAN in switch level.

Operating System Access Control

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

- **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. The organization shall adopt dual authentication for all its business applications.

Application and Information Access Control

- **Information Access Restriction** Logical access to application software and information will be restricted to authorized users only.
- **Classified System Isolation** Classified systems above CONFIDENTIAL will have a dedicated and isolated computing environment.

16. Monitoring

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.

Audit Logging

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

Monitoring System Use

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

Protection of Log Information

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

Administrator Logs

Administrator activities will be logged.

Fault Logging

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

Clock Synchronization

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

17. Cryptographic Controls

Information Classification

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

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.

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.

Secure Storage

Storing SECRET and TOP SECRET Information in Electronic Form

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

- 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.
- 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 residue in the originating computer including page files, swap areas, slack areas, RAM etc.
- 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.
- To safeguard against loss/theft of classified data in storage media, encryption techniques will be used to ensure confidentiality of data at rest.

- 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.
- 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

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:-

- Responsibility for security.
- Internal security audit.
- User access management.
- Network access control.
- Patch and virus management.
- Handling of removable media and portable computing devices.
- Incident reporting and handling.
- Backup and recovery for business continuity.
- Repair and maintenance.
- Installation of software.
- Starting and stopping of classified applications and security solutions.
- Key Management.
- Change Management.
- Crisis Management
- Third Party Services

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.

Segregation of Duties

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

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.

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.

Back-Up

- Back-up of information and software will be taken and tested regularly in accordance with the backup policy as defined in BEML IT Policy 2016 of the establishment and criticality of information.

19. Handling of Storage and Removable Media

Management of Removable Storage Media

All secondary mass storage devices such as CD/DVD Writers, removable hard drives, etc when authorized 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 authorization of a nominated controlling officer and records of the same maintained. Transfer of data between networked computers will be done through the network only.

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 authorized 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. 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.

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.

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.

Security and Storage of System Documentation

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

20. Electronic Messaging

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.

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

21. Internet

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.

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 organizational 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.

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

An authorization 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.

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:-

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.

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

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

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

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

Compliance with Security Policies and Standards

- 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.

- Frequency of Audit To ensure compliance of cyber security policy each establishment will carry out audits as per the periodicity laid down by DDP viz. once in two years by CERT-In empanalled auditors and once in a year by DDP security auditors.

25. Cyber Crisis and Incident Management

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.

Incident Prevention, Reporting and Handling

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

- 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.

- **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

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.

Cyber Security Awareness

- To promote and launch a comprehensive Cyber Security Awareness Program in relation to national awareness program on security of cyberspace.
- To sustain security literacy awareness and publicity campaign through electronic media to help the staff of organization to be aware of the challenges of cyber security.
- To conduct, support and enable cyber security workshops/ seminars and certifications.

27. Information Sharing and Co-operation

- To develop bilateral and multi-lateral relationships in the area of cyber security with other cyber entities in the country.
- To enhance National cooperation among security agencies, Law Enforcement Agencies and judicial systems.
- 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

- 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.

- To encourage Research & Development to counter a wider range of cyber security challenges prevailing in cyber field.
- To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.
- To set up Centers of Excellence and Security Operational Centers (SOCs) in areas of strategic importance for the point of security of cyber space.
- To collaborate in joint Research & Development projects with industry and other research organizations 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 organization. This to be achieved by:

- Develop the continuity planning policy statement
- Conduct the Business Impact Analysis (BIA)
- Identify preventive controls
- Develop recovery strategies
- Develop contingency plan
- Test the plan and conduct training and exercises
- Maintain the plan.
- DR DRILLS

Business continuity should be a part of the security program taking into consideration the threats to the organization. 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 organization 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 organization in a negative way and having an action plan for each threat with applicable probability and severity is to be put in place. If 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

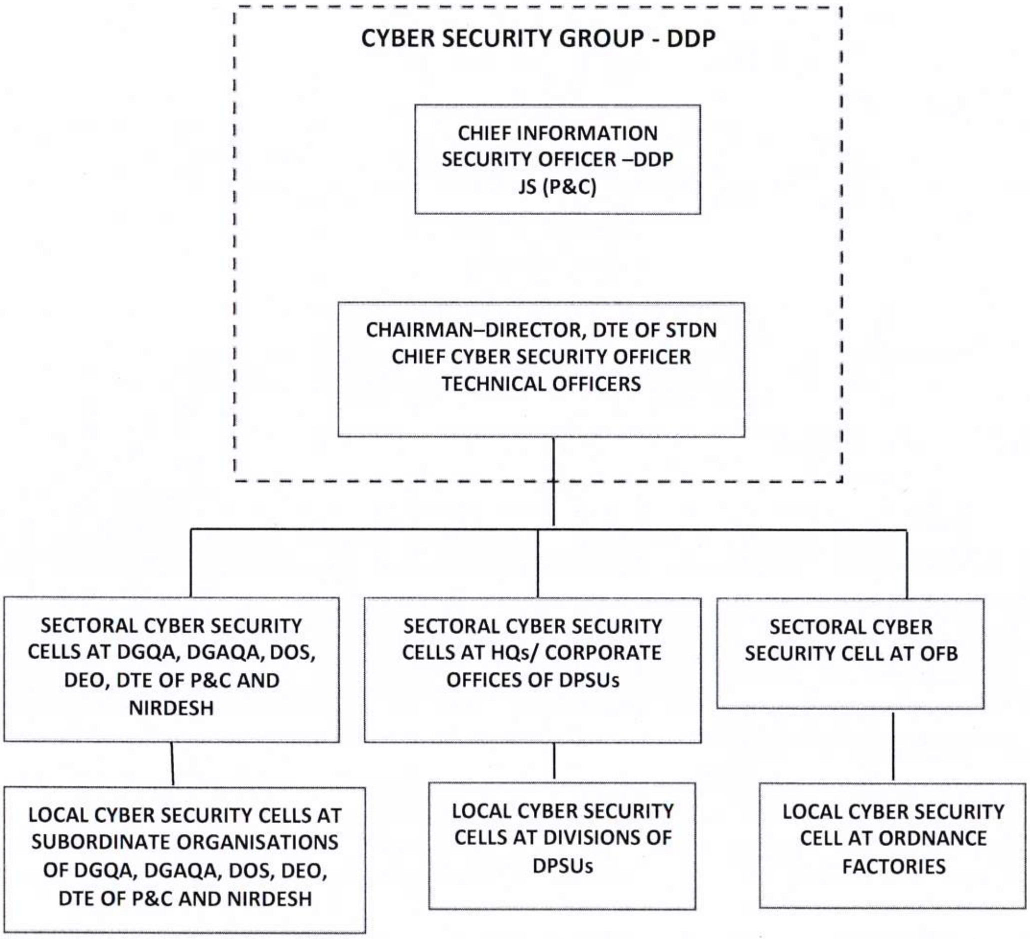
31. Summary

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 Department of Defence Production DDP).

Annexure A

(Refers to paragraph 06 of DDP Cyber Security Policy Template – 2018)

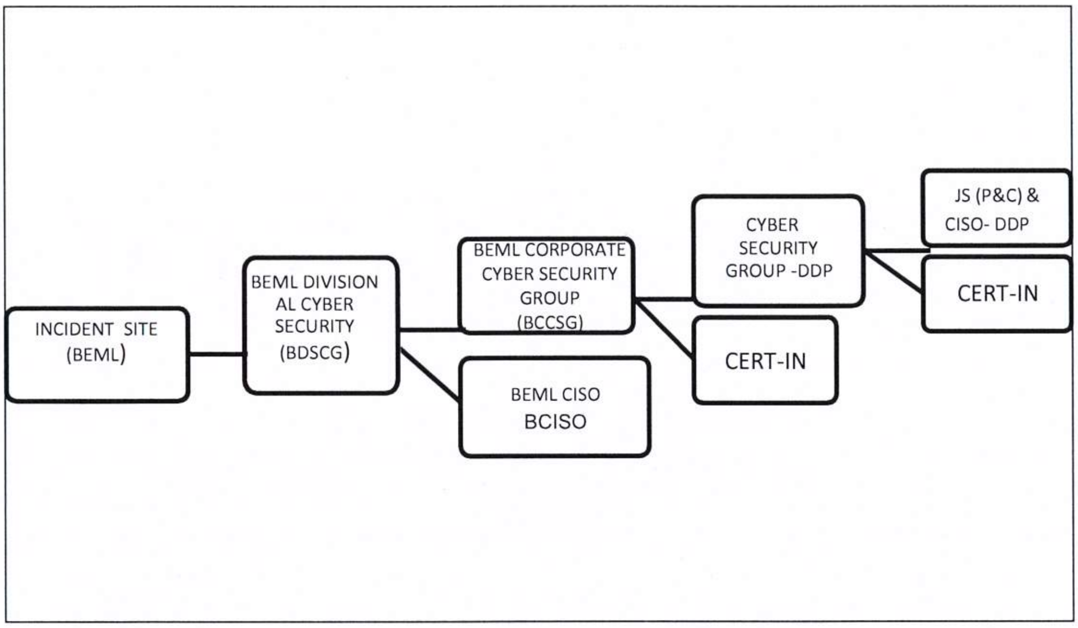
ORGANIZATION STRUCTURE


CYBER SECURITY GROUP - DDP
CHIEF INFORMATION SECURITY OFFICER –DDP JS (P&C)
CHAIRMAN–DIRECTOR, DTE OF STDN CHIEF CYBER SECURITY OFFICER TECHNICAL OFFICERS
SECTORAL CYBER SECURITY CELLS AT DGQA, DGAQA, DOS, DEO, DTE OF P&C AND NIRDESH
SECTORAL CYBER SECURITY CELLS AT HQs/ CORPORATE OFFICES OF DPSUs
SECTORAL CYBER SECURITY CELL AT OFB
LOCAL CYBER SECURITY CELLS AT SUBORDINATE ORGANISATIONS OF DGQA, DGAQA, DOS, DEO, DTE OF P&C AND NIRDESH
LOCAL CYBER SECURITY CELLS AT DIVISIONS OF DPSUs
LOCAL CYBER SECURITY CELL AT ORDNANCE FACTORIES

Annexure B

(Refers to paragraph 25 of DDP Cyber Security Policy Template – 2018)

CHANNEL OF REPORTING


INCIDENT SITE (BEML)
BEML DIVISION AL CYBER SECURITY (BDSCG)
BEML CORPORATE CYBER SECURITY GROUP (BCCSG)
BEML CISO BCISO
CYBER SECURITY GROUP -DDP
CERT-IN
JS (P&C) & CISO- DDP
CERT-IN