



# **INFORMATION SECURITY POLICY AND GUIDELINES**

**ISSUE-I**

**Year 2022**

---

**DIRECTORATE GENERAL OF AERONAUTICAL QUALITY  
ASSURANCE (DGAQA)  
GOVERNMENT OF INDIA, MINISTRY OF DEFENCE  
DEFENCE OFFICE COMPLEX, K G MARG,  
New Delhi-110001**

**INFORMATION SECURITY POLICY  
AND  
GUIDELINES  
FOR PROTECTION OF INFORMATION  
IN CYBERSPACE**

**IN**

**Directorate General of Aeronautical Quality  
Assurance (DGAQA)**

---

**Information Technology Group  
DGAQA  
Ministry of Defence  
New Delhi**

## FORWARD

The Directorate General of Aeronautical Quality Assurance (DGAQA), under Department of Defence Production, Ministry of Defence, Govt of India is the regulatory authority for Quality Assurance and final acceptance of Military Aircraft, Unmanned Aerial Vehicles (UAVs), Aero Engines, Airborne Systems, Avionics, Armaments, Consumables (FOL Stores), Allied Ground Systems and Missiles during Design & Development, Production, Repair, Modification and Overhaul at various Defence PSUs, Ordnance Factories and Private Firms. The field establishments are spread all over in our great nation in Defence Public Sector Undertakings, Ordnance Factories, DRDO Labs and various Private Firms. With regards to Information Security, the role of Headquarters assumes more importance and as such we need to be better equipped to meet the modern day challenges. With the fast changing world due to rapid technological innovations, it is needed to facilitate our personnel in terms of information and resources.

Cyber-attackers use malicious code and software to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes such as information and identity theft or system infiltration.

Cyber-crime is unlikely to slow down, despite government efforts and input from specialists. Its growth is being driven by the expanding number of services available online, and the increasing evolution of online criminals who are engaged in a continuous game with security experts. With constant technical innovation, new dangers are constantly coming to the surface. For example, the migration of data to third-party cloud providers has created an epicenter of data and therefore, more opportunities to misappropriate critical information from a single target. Similarly, mobile phones are now targets, expanding the opportunities to penetrate security measures.


The Information Security Policy and Guidelines (ISPG) has been prepared by the HQ-DGAQA (with help of documents issued by MHA), based on the experience of the existing security standards and frameworks and the global best practices and experience of implementation in the wake of expanding information security threat scenario. This policy document will supplement the existing guidelines issued by DeitY, NIC, IB and NTRO for the security of ICT infrastructure, assets, networks, applications, user management, email etc.

This ISPG document along with Standard operating procedures (SOPs) for IT (Information Technology) documents created to explain various procedures within an information systems environment at HQ. These documents primarily prepared by HQ DGAQA IT Group for in-house use and provide IT department personal the required guidelines that can be used for reference and training purposes. Further, FEs to follow by preparing their own SOP document/ the instructions as per their requirement by taking guidance from SOP issued by HQ DGAQA.

Further, separate Cyber Security documents are already issued by HQ-DGAQA for strict compliance by all FEs and HQ (viz Cyber Security Policy, Cyber Crises Management Plan (CCMP), Cyber Security Framework, National Cyber Security Policy 2013 and Role and Responsibilities of Chief Information Security Officer).

The Information Security Policy and Guidelines (ISPG) and Standard operating procedures (SOPs) for IT (Information Technology) are being released today on 31<sup>st</sup> Aug 2022 during 69<sup>th</sup> DGAQA Foundation day. I am sure that, these documents will be useful to all officers, IT & Cyber Security personnel, who are handling the IT activities for their better understanding and guidance while performing their duties with utmost Cyber Security care, dedication and professionalism in achieving excellence with our commitment in taking DGAQA to further heights by following Govt of India's Digital India Initiative.

Date : 31 Aug 2022  
Place: New Delhi

  
(S CHAWLA)  
DIRECTOR GENERAL

**The followings have been covered as part of this document.**

These are:

1. Network and Infrastructure security
2. Identity, access and privilege management
3. Physical security
4. Application security
5. Data security
6. Personnel security
7. Threat and vulnerability management and
8. Security and incident management

Further, guidelines have been provided for technology specific ICT deployment and trends:

1. Cloud computing
2. Virtualization
3. Social media

Additionally, guidelines for essential security practices have been provided:

1. Security testing
2. Security auditing
3. Open source technology

[illegible]

## ABBREVIATIONS

CERT-In	Indian Computer Emergency Response Team
CISO	Chief Information Security Officer
CSO	Chief Security Officer
DDoS	Distributed Denial of Service
DeiTY	Department of Electronics and Information Technology
DLP	Data Loss Prevention
DoS	Denial of Service
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISO	Information Security Officer
ISPG	Information Security Policy and Guidelines
ISSP	Information Systems Security Policy
NCIIPC	National Critical Information Infrastructure Protection Centre
NIC	National Informatics Centre
NISPG	National Information Security Policy and Guidelines
NSA	Network Security Administrator
NTRO	National Technical Research Organisation

RBAC	Role Based Access Control
SA	System Administrator
SIEM	Security Information and Event Management
SSDLC	Secure Software Development Lifecycle
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TVM	Threat and Vulnerability Management
VOIP	Voice Over Internet Protocol



## Table of Contents

1.0	Introduction .....	1
2.0	Purpose .....	3
2.1	Purpose of Information Security Policy and Guidelines .....	3
2.2	The ISPG aims to provide:.....	4
3.0	Approach.....	4
3.1	Security of classified information .....	4
3.2	Security risk assessment.....	4
3.3	Principles for establishing organization wide security framework.....	5
3.4	Security Audit .....	6
3.5	Exception to implementation of recommended guidelines and controls .....	6
3.6	Limitations: .....	7
4.0	Information Classification Guidelines: .....	8
4.1	Information Classification.....	8
4.2	Information Handling .....	8
5.0	Information Security Organization Overview .....	8
5.1	Security Division .....	8
5.2	Information security division & roles .....	9
6.0	Framework .....	10
6.1	Standard for information security management.....	10
6.2	Introduction to globally accepted Information security management standards.....	10
7.0	Domains impacting information security.....	10
7.1	Overview.....	10
7.2	Information security domains .....	11
8.0	Network and infrastructure security .....	13
8.1	Background.....	13
8.2	Relevance of domain to Information Security.....	13
8.3	Network and infrastructure security management guidelines .....	14
8.4	Network and infrastructure security controls .....	16
8.5	Network and Infrastructure security implementation guidelines .....	18
9.0	Identity, access and privilege management .....	22
9.1	Background.....	22
9.2	Relevance of domain to information security .....	23
9.3	Identity, access and privilege management guidelines .....	23
9.4	Identity, access and privilege management controls .....	25
9.5	Identity, access and privilege implementation guidelines .....	27
10.0	Physical and environmental security .....	31
10.1	Background.....	31
10.2	Relevance of domain to information security .....	32
10.3	Physical and environmental security guidelines.....	32
10.4	Physical and environmental security controls .....	33
10.5	Physical security implementation guidelines .....	35

11.0	Application security .....	39
11.1	Background.....	39
11.2	Relevance of discipline to information security .....	39
11.3	Application security guidelines.....	40
11.4	Application security controls .....	41
11.5	Application security implementation guidelines .....	42
12.0	Data security .....	47
12.1	Background.....	47
12.2	Relevance of domain to information security .....	48
12.3	Data security guidelines .....	48
12.4	Data Security Controls .....	49
12.5	Data security implementation guidelines.....	51
13.0	Personnel security.....	56
13.1	Background.....	56
13.2	Relevance of domain to information security .....	57
13.3	Personnel security guidelines .....	57
13.4	Personnel security controls .....	58
13.5	Personnel security implementation guidelines .....	59
14.0	Threat and vulnerability management .....	62
14.1	Background.....	62
14.2	Relevance of domain to information security .....	63
14.3	Threat and vulnerability management guidelines.....	63
14.4	Threat and vulnerability management controls .....	64
14.5	Threat and vulnerability management implementation guidelines .....	65
15.0	Security monitoring and incident management .....	69
15.1	Background.....	69
15.2	Relevance of domain to information security .....	69
15.3	Security monitoring & incident management guidelines .....	69
15.4	Security monitoring & incident management controls .....	70
15.5	Security monitoring and incident management implementation guidelines.....	72
	Guidelines for technology specific ICT deployment.....	78
16.0	Cloud computing.....	78
16.1	Background.....	78
16.2	Cloud computing management guidelines.....	78
16.3	Cloud computing implementation guidelines: .....	79
16.4	Data security in cloud .....	80
16.5	Use of authorized cloud services .....	80
17.0	Mobility & BYOD .....	80
18.0	Virtualization.....	80
19.0	Social media .....	80
19.1	Background.....	80
19.2	Social media management guidelines .....	81
19.3	Social media implementation guidelines.....	81

20.0	Open source technology .....	82
20.1	Background.....	82
20.2	Open source technology management guidelines .....	82
20.3	Open source technology implementation guidelines.....	82
	Guidelines for essential security practices.....	83
21.0	Security testing .....	83
21.1	Background.....	83
21.2	Security testing management guidelines .....	84
21.3	Security testing implementation guidelines.....	84
22.0	Security Auditing.....	85
22.1	Background.....	85
22.2	Security audit management guidelines .....	85
22.3	Security audit implementation guidelines.....	87
23.0	Annexure.....	89

## List of Figures

Figure 1:- Information Systems Security Policy.....	2
Figure 2:- Each area encompasses information which has ramifications towards National Security.....	7
Figure 3:- Information Security Domains .....	12

## List of Annexure

### Annexure 1

**1A** -List of government advisories on information security

**1B** – List of information security frameworks

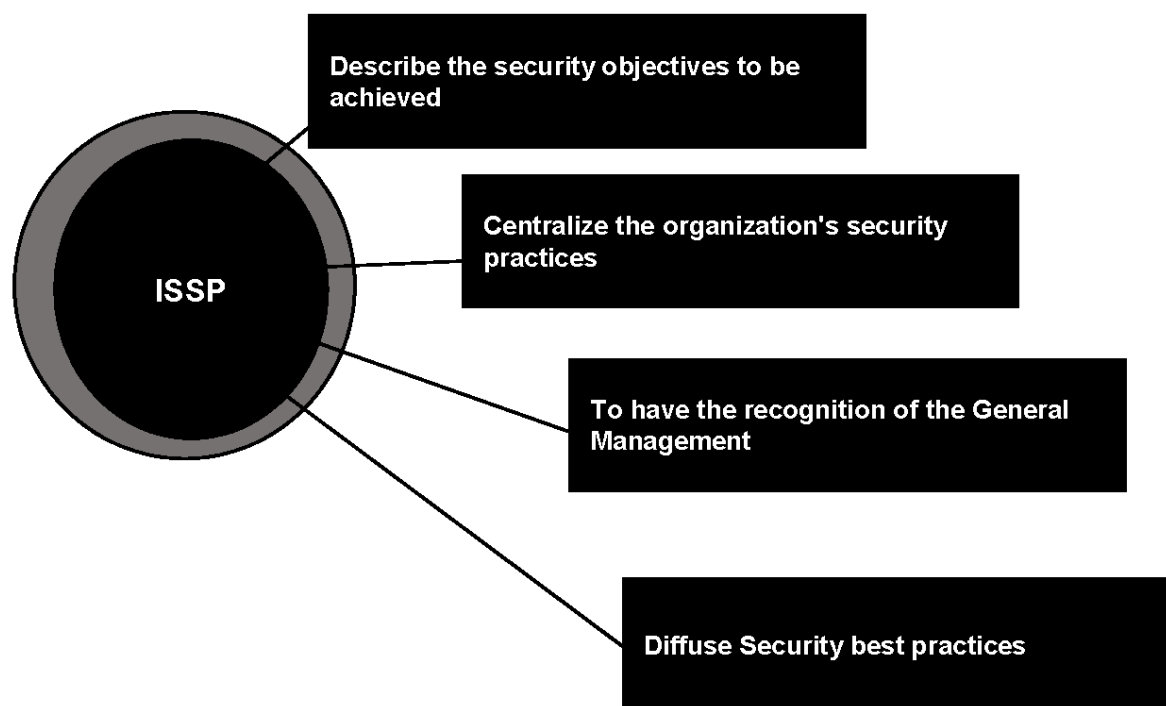
**Annexure 2**– Guidelines and controls mentioned in “Cyber Security Policy for Government of India

**Annexure 3**- Glossary

**Annexure 4** –Additional references

## 1.0 Introduction

- 1.1 The digital world is a reality today in all aspects of our lives. Digital infrastructure is the backbone for smooth functioning of the Organization .Therefore improving and securing this digital infrastructure in all its dimensions including increased availability of next generation broadband connectivity, security of information, is critical to the organizations like DGAQA.
- 1.2 Information Systems (IS) are today an integral part of the functioning of administrations and activities of the DGAQA Organization. The security of these information systems has become a major issue at the present scenario. Information security policy is the general term used to describe any document that transmits an element of the security program in order to ensure compliance with the organization's security goals and objectives. Information is a valuable asset that must be protected from unauthorized disclosure, modification, use or destruction. Prudent steps must be taken to ensure that its confidentiality, integrity and availability are not compromised. The Information Systems Security Policy (ISSP) reflects the expectations and requirements of the Executive Management with regard to the Information System It must take into account at least the needs in terms of availability, confidentiality and integrity of applications and data used and transiting on networks and systems. The ISSP is the counterpart of the Information Systems Master Plan for security. In addition to defining roles and responsibilities, information security policies increase users' awareness of the potential risks associated with access to and use of technology resources. Employee awareness through dissemination of these polices helps accelerate the development of new application systems and ensure the consistent implementation of controls for information systems. It can lead to an ISSP action plan that prioritizes projects to meet ISSP objectives. The objectives of the Information Systems Security Policy (ISSP) are described in figure 1.



**Figure 1:- Information Systems Security Policy**

- 1.3 Traditionally, information available with the government has been safely managed by keeping it in paper records throughout its lifecycle i.e. creation, storage, access, modification, distribution, and destruction. However, to make organization more effective, along with transparency & reliability, the department has steadily graduated towards using electronic formats of information. Now, several forms of information have been converted to the electronic format by DGAQA which includes On line APAR, Uploading of Circulars and other Data, Updating of Reports in the form of electronics Data, implementation of e-office, On-line clearance of MEMO etc. The classification, storage and protection of such information in electronic format have always remained an area of concern. The challenge, as with the information contained in paper format, remains the same, namely the ability to categorize, protect, archive, discover, and attribute information during its useful life and eventual destruction. Even though the lifecycle of information remains the same in electronic documents and online transactions, the methods to secure information in electronic environment are different.
- 1.4 Information security is one of the important components of cyber security and is gradually taking center stage in the national security deliberations and discussions. In fact, it has become a key component of national security design and is shaping international strategies of nations globally. Threats to information are increasingly organized and targeted, helping criminals, state actors and hacktivists to reap immense benefits out of information compromise, theft or espionage.

- 1.5 Cyber criminals can carry out identity theft and financial fraud; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals or disrupt critical infrastructures by exploiting the vulnerabilities in any system connected to the Internet. The cybercriminals could be located anywhere in the world and they can target a particular user, system or a particular service in a country or a region. Worse still, the cybercriminals can cover their tracks so that they cannot be traced. It is extremely difficult to prove whether the cyber criminal is an individual, a gang, a group of state actors or a nation-state.

## **2.0 Purpose**

### **2.1 Purpose of Information Security Policy and Guidelines**

- 2.1.1 Information Security Policy and Guidelines will help to classify and protect the classified information possessed by DGAQA & all Fes. Breach of such classified information may have an impact on national security, or may cause unfavorable impact on internal security.
- 2.1.2 This document elaborates baseline information security & highlight relevant security concepts and best practices to protect DGAQA & all FEs classified information.
- 2.1.3 These guidelines will help DGAQA & FEs to establish minimum security processes and controls and devise appropriate information security programs. DGAQA & FEs need to apply enhanced security measures commensurate with risks identified with specific operating environment and the information being handled.
- 2.1.4 These guidelines will help organizations to focus on security objectives and strategy to protect their classified information, during every stage of information lifecycle such as creation, acquiring, storing, accessing, processing, transacting, retaining or disposal. These guidelines will help drive organizations towards designing, implementing and operating focused information security initiatives.

## 2.2 The ISPG aims to provide:

- 2.2.1 Guidance to prioritize and focus attention and efforts in classification of information and securing such classified information
- 2.2.2 Guidance for deriving security measures and controls commensurate with the criticality and sensitivity of classified information.
- 2.2.3 Guidance to drive security implementation.

## 3.0 Approach

### 3.1 Security of classified information

- 3.1.1 **Securing classified information in government sector processes life cycle:** DGAQA and all FE's should ensure that they establish appropriate processes and capabilities to secure information throughout its life cycle i.e. as information is created, accessed, modified, stored, processed, transacted, transmitted, deleted, disposed of or destroyed. Information can be classified based on its category or type, sensitivity, value and the context throughout its life cycle.

### 3.2 Security risk assessment

- 3.2.1 **Conducting periodic risk assessment:** Security risk assessments should be conducted periodically to evaluate risks and associated threats leading to loss of confidentiality, integrity and availability of information. Threat and vulnerabilities associated with the information must also be evaluated for their potential impact, including impact on internal and national security.
- 3.2.2 **Risk assessment framework:** Due to the diverse nature of operations of different organizations there can be no single approach recommended for risk assessment. However, to develop a risk based methodology which helps develop resilience to changing threat environment, ministries, departments, agencies and their subordinate organizations need to integrate information security risk assessment with the broader risk management framework for operations. For details Cyber Security Frame work issued by DGAQA can be referred.

**3.2.3 Periodicity of risk assessments:** Information security risk assessment should be an on-going activity, triggered early into the life cycle of system design and development. It should be conducted at least once every year or when changes are made to existing information assets or when threat perception over information and information systems changes. For systems containing classified data, a thorough risk assessment should be conducted at-least once every quarterly.

**3.2.4 Additional insights:** A comprehensive information security risk assessment will also provide insights in to expected ICT security expenditure, thereby helping formulate budgets and estimate costs and help strategic decision making.

### **3.3 Principles for establishing organization wide security framework**

**3.3.1 Core security goals:** Information security frameworks should be designed to ensure confidentiality, integrity, availability of information to authenticated and authorized users, while establishing accountability over transactions conducted over the lifecycle of information and establishing non-repudiation of information, across layers of people, process and technology.

**3.3.1.1 Architecture:** Adequate steps must be taken for integrating information security measure switch the IT architecture of organizations to address contemporary security threats. Capability to respond to new issues or threats through integrating internal and external intelligence measures, deployment of tools, techniques and methods in identifying threats, which generate timely and desired response from other security & IT management processes, must be established

**3.3.2 Security division structure:** DGAQA and All FEs must establish accountability and ownership structure for information security, where tasks are clearly distributed with respect to administrative and technical arrangements required for information security. The head of security must report directly to the head of the departments or organizations and not to the IT head.

**3.3.3 Deployment of professionals and skill development:** DGAQA and All FEs must ensure that trained professionals in the field of Information Security are deployed to address their Information Security initiatives, at appropriate levels. Further, adequate measures to train existing users, human resources, to acquaint them with best practices for securing information and align them with the overall objectives of the organization for protection of information and information assets must be undertaken at periodic intervals. Every new employee should go through the information security awareness program which could be organized in-house. Also every employee should be given training in information security at least once every two years.



### 3.4 Security Audit

- 3.4.1 Security audits:** DGAQA and All FE's must conduct appropriate evaluation, testing and audits of all organizational structures, mechanisms, policies, procedures, technologies and controls to ensure their alignment with the implementation objectives of the information security policy and guidelines at regular intervals. Areas of improvement should be identified and a mechanism to improve the overall deployment of such structures, mechanisms, policies, procedures, technologies and controls should be undertaken.
- 3.4.2 Identification and response to data breach:** DGAQA and All FEs should develop the ability to identify, alert, evoke responses & resolve a data breach in timely manner
- 3.4.3 Coordination with Agencies:** DGAQA and All FEs should interact with relevant agencies in the domain of information security to gather and share intelligence about threats and vulnerabilities. CISO of HQ DGAQA is the nodal officer for Design, implement, monitor and govern an organization-wide information security program.

### 3.5 Exception to implementation of recommended guidelines and controls

- 3.5.1 DGAQA and All FEs expected to conduct a thorough risk assessment and use the practices outlined in this document to help implement a framework within the organization.
- 3.4.2 DGAQA and All FE's must exercise its own discretion in customizing and adapting the guidelines mentioned in this document..
- 3.5.2 The Cyber Security Group, DDP, CIRA, MoD or any designated agency may seek compliance in the form of audit reports to demonstrate adherence to controls and guidelines specified in DGAQA.
- 3.5.3 In case some guidelines and controls are not adhered to, FE's should be able to substantiate their stance by reproduction of appropriate documentation specifying at a minimum, the following parameters:
- a) Reason for non-conformance to guidelines.
  - b) Risk evaluation reports detailing the risks due to non-conformance.

### 3.6 Limitations:

The figure below summarizes the overall security eco system by explaining the relationship between national security, cyber security, organization security and information security. The policy focuses on protection of classified information and hence intends to only provide guidance, procedures and controls which are relevant to this specific area. While it is beyond the scope of this document to detail every single practice involved in the design, implementation, configuration, management and security enforcement, an effort has been made to capture information security measures through security domains.

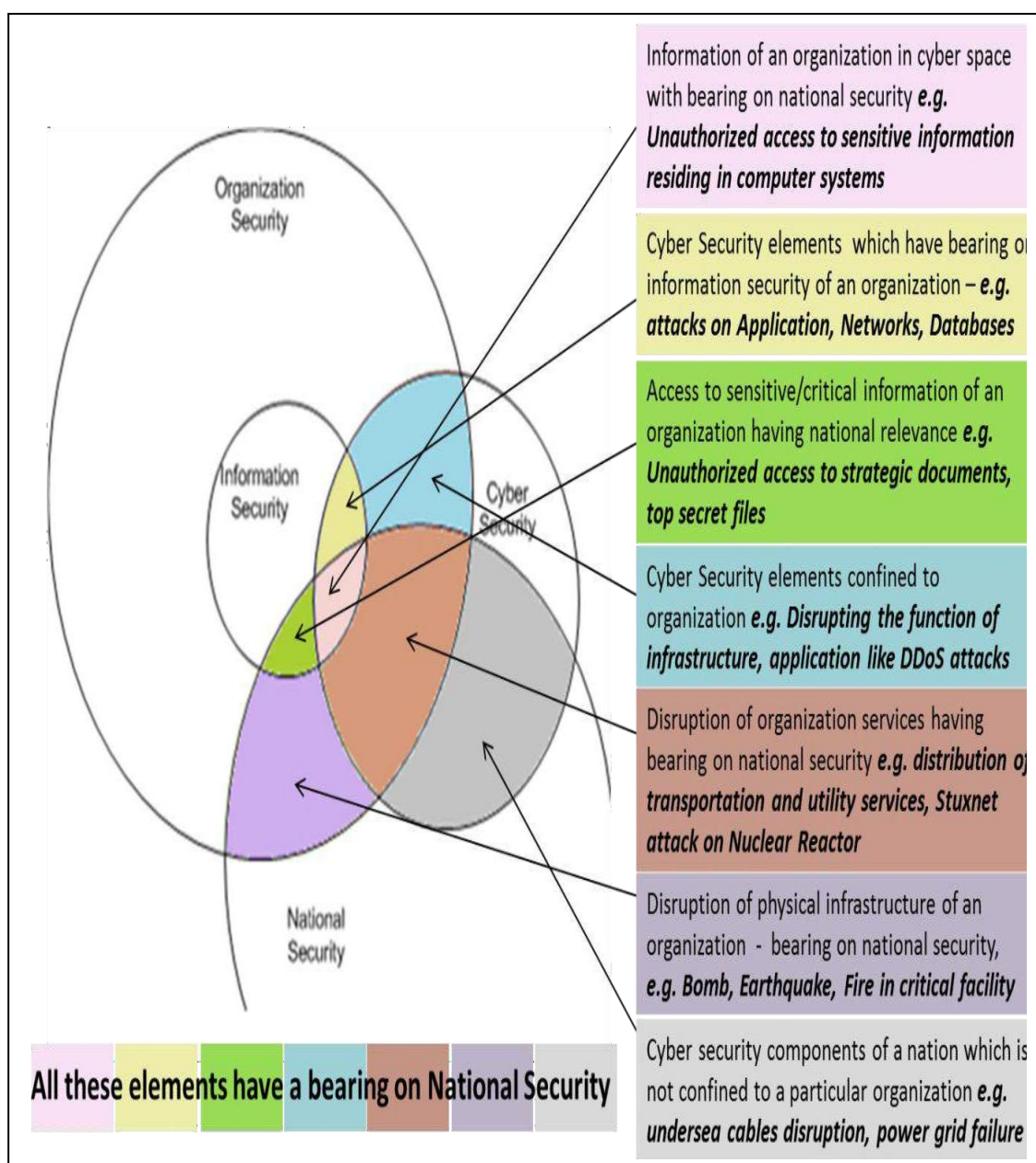


Figure 2:- Each area encompasses information which has ramifications towards National Security

## 4.0 Information Classification Guidelines:

### 4.1 Information Classification

All information available with organizations should be classified into one of the following categories

- 4.1.1 **Top Secret:** Information, unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for nation's closest secrets and is to be used with great reserve.
- 4.1.2 **Secret:** Information, unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.
- 4.1.3 **Confidential:** Information, unauthorized disclosure of which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization, or could affect the organization in its functioning. Most information, on proper analysis, will be classified no higher than confidential.
- 4.1.4 **Restricted:** Information, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.
- 4.1.5 **Unclassified:** Information that requires no protection against disclosure .e.g. Public releases
- 4.2 **Information Handling:** Appropriate information handling procedures must be developed, commensurate with the level of classification.

## 5.0 Information Security Organization Overview

### 5.1 Security Division

- 5.1.1 **Role of Chief Information Security Officer (CISO):** The responsibility of security management should be entrusted to the "Security Division" under the charge of the Chief Information Security Officer (CISO). Its role cuts across the traditionally defined boundaries of IT and covers all the horizontal and vertical functions of an organization. CISO's role is detailed below:

- 5.1.1.1 Design, implement, monitor and govern an organization-wide information security program.

- 5.1.1.2 Ensure information security risk assessments and audits are performed as necessary. Oversee risk assessment exercise to understand the threats to key information assets, analyze risks with the concerned divisions of the organization.
- 5.1.1.3 Design information security related policies, procedures and processes to ensure confidentiality, integrity, availability of classified information while establishing accountability, authorization and non-repudiation of actions over information.
- 5.1.1.4 Review policies, procedures and standard operating procedures.
- 5.1.1.5 Work on positioning of security division, so as to make it more effective.
- 5.1.1.6 Devise programs for capacity building and oversee information security training and development of personnel .Additionally, the CISO should establishing mechanisms for information security awareness in the organization.
- 5.1.1.7 Liaison with relevant agencies to gather intelligence about prevailing threats and best practices.

## 5.2 Information security division & roles

(Refer “Cyber Security Policy for Government of India” ver2.0 released 30<sup>th</sup> August, 2010)

- 5.2.1 The following roles are required based on the fact that each Ministry/ Department / Organization is located in one of more location / Bhawan and each location / Bhawan has one or more Ministries / Departments / Organizations.
  - 5.2.1.1 **Chief Information Security Officer (CISO):** Responsible for cyber security in the organization. This role is to be designated by the respective Ministry / Department.
  - 5.2.1.2 **Cyber Security officer (CSO):** Responsible for technical functions, related to cyber security for the respective Zone.
  - 5.2.1.3 **Information Security Officer (ISO):** Responsible for administrative functions related to security for every location of the HQ DGAQA or FEs. This role is to be designated by the Ministry / Department for each location of the Ministry /Department.
  - 5.2.1.4 **System Administrator (SA):** Responsible for performing functions, that requires system administration privileges of the user systems, for each location of the Department.
  - 5.2.1.5 **Network Security Administrator (NSA):** Responsible for managing the security of the networks per location. This role will be performed by the service provider.

## 6.0 Framework

### 6.1 Standard for information security management

- 6.1.1 DGAQA should ensure enforcement of a globally accepted standard of information security management and governance. Reference to the standard used, should be documented in the ministry / department's security policy, or in some other high level document, developed by the Chief Information Security Officer (CISO).
- 6.1.2 The implementation of information security and its governance requires coordinated effort between designated personnel and well defined framework for governance. The governance process and the personnel tasked with governance of information security should be stated in the security policy.

### 6.2 Introduction to globally accepted Information security management standards

- 6.2.1 There are several standards accepted globally which help an organization conduct risk assessment, gap analysis and govern security implementation at different levels such as network access points, user authentication, applications etc. across the people, process, and technology (PPT) layers. There are several information security management standards which are adopted by organizations worldwide. DGAQA follows ISO 27001-2013 standard.

## 7.0 Domains impacting information security

### 7.1 Overview

- 7.1.1 **Alignment with security framework:** DGAQA has identified eight core domains namely, network and infrastructure security, identity and access management, physical security, application security, data security, personnel security, threat & vulnerability management, security monitoring & incident management. Additionally, the areas of security audit, security testing and business continuity, which cut across all domains, have been covered as part of the guidelines. Further, guidelines for technology specific areas such as virtualization, cloud computing, mobility and social media are provided in a separate section.
- 7.1.2 **Achieving maturity in security domains:** Domains mentioned above need to be understood critically for security of classified information. Strategies for each of them, along with tactical guidelines for implementation, and security controls are essential for making security robust. The ministries, departments, agencies and their subordinate organizations should organize, allocate and drive resources towards each of these security domains and strive to achieve maturity over time to counter the increasing threats and attacks.

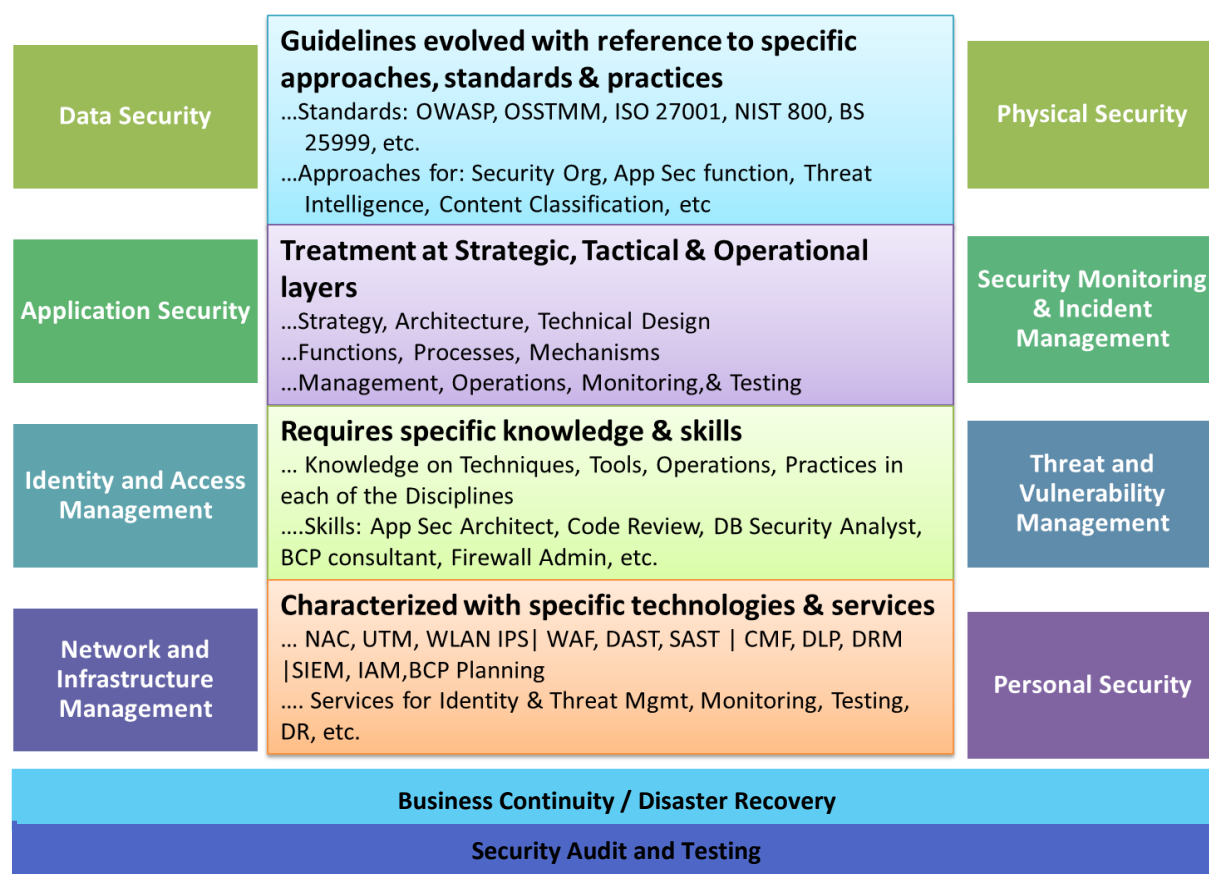
## 7.2 Information security domains

- 7.2.1 **Network and infrastructure security:** The architectural plan of locating information in a network arrangement and other infrastructure security arrangements such as internal and external connections to information, protocols that are used to transfer information, preparedness to withstand attacks etc. require specific consideration and treatment from the perspective of securing information.
- 7.2.2 **Identity and access management:** Sensitivity and criticality of information specifies the requirements with respect to ability of an individual or group of users to access and perform a set of operations on the said information. The increasing reliance on third parties and external SME's makes it imperative for the organization to secure itself against risk arising from misuse of identities or additional or illegitimate access provided to the users.
- 7.2.3 **Physical security:** Organizations generally have multiple touch points from where information can be accessed physically. To add that, technology enables easy availability of portable devices. This can defeat traditional physical screenings of individuals. With more solutions and techniques becoming available in the market, physical security concepts are also evolving, establishing it as an important discipline for protecting information security. While it focuses more on restriction to physical intrusion, technological solutions provide means to raise alarms by detecting anomalies and patterns of information being accessed which help in detection and containment of information security incidents.
- 7.2.4 **Application security:** The primary objective of application security is to secure information as it is processed, transferred or stored during the life cycle of an application. The characteristics of applications vary from basic versions, to context aware, and Internet rich usage of apps. These variations at various fronts expose the information processed, stored, accessed, transacted through these applications to a larger threat landscape.
- 7.2.5 **Data security:** Each data item collected, stored, processed, transmitted and accessed by an organization has to be protected against cyber-attacks especially that are sensitive or critical for internal and national security as stated in classification of information. The entire focus and effort is to secure data. It is this which has led to the evolution of the discipline of data security -the ultimate goal of an organization's security.
- 7.2.6 **Personnel security:** Risks due to insider threat and internal security breach undermines all security measures taken to fortify information systems and data from the outside world. The personnel security focuses on both the aspects of employee as well as third party security and focuses on sourcing patterns of an organization which requires specifics checks from a security view point.
- 7.2.7 **Threat & vulnerability management:** There is an ever increasing rise of security threats with enhanced capabilities, varieties and scales; exploring new ways to find vulnerabilities and exploits in an organization's infrastructure to cause maximum possible damage. Threat and Vulnerability Management (TVM)



ensures that an organization's resources are protected against the perennial as well as evolving threats, and provides assurance over the management of its resources in a way that the relevance of new vulnerabilities, exploits or malware is immediately tested and that the organization responds swiftly to them. TVM adds critical value to an organization's security initiatives, which not only delivers protection capabilities but also provides means to manage IT infrastructure securely.

- 7.2.8 Security monitoring & incident management:** Security Monitoring and incident response management is a key component of an organization's information security program, as it demonstrates its ability to respond to an information breach which might emanate from external or internal sources.
- 7.2.9 Security audit and testing:** Security audit, testing and reviews should be conducted on a continuous basis to check for conformance of security measures deployed by the organization with security policies, standards and requirements. Specific requirements are implicit in all disciplines. Moreover, general best practices have been provided as part of this document.
- 7.2.10 Business continuity:** Business continuity of the operations has to be planned by the respective government departments and is kept outside the scope of this policy. However, this document covers areas which are important from the perspective of ensuring availability of critical operations and classified information.



**Figure 3:- Information Security Domains**

## **8.0 Network and infrastructure security**

### **8.1 Background**

- 8.1.1 The increased adoption of information technologies has created immense opportunities to connect, expand and integrate different entities. This led to the expansion of the network capabilities and adoption of emerging connectivity techniques.
- 8.1.2 The network infrastructure itself has evolved with various options of network topologies, types of routing and switching devices and different connectivity options. Networks are playing important role in providing access to information and information systems; providing new ways for executing transactions and helping organizations leverage fruits of globalization and hyper specialization. The diversity of these topologies, devices and connections contributes to creating immense possibilities, however; it also introduces several new security issues and concerns.
- 8.1.3 The organizational ecosystem is undergoing transformation, extending its boundaries by increasingly providing access to third parties and vendors, integrating external interfaces, adopting innovations in endpoint, mobility and wireless technologies, while relaxing norms of standardization and ownership of connecting devices. Enterprise architectures are becoming more complex, multiple new system components are under deployment, and their capabilities are extensively utilized through virtualization. This provides multiple opportunities by which security can be compromised.

### **8.2 Relevance of domain to Information Security**

- 8.2.1 Network plays an important role as it binds all the information assets together and provides a means for operational transaction where different entities can participate, exchange information and carry operations over the information by making use of specific ports, protocols and services provided by the network. This may create the possibilities of exposure of information.
- 8.2.2 Network plays a role in provisioning users and devices access to data as it is the first point of connects. Users seek flexibility in accessing data across different devices and access paths. This may expose organization's information through these devices and the way user's access information.
- 8.2.3 Network infrastructure typically spreads across geographies, providing access, facilitating exchange of information and executing a variety of transactions. A combination of network solutions and devices are required in order for these transactions to be successful. They may create possibilities of compromising security of information at various levels



- 8.2.4 Traffic flow, connections, devices and traffic patterns introduce significant vulnerabilities and weaknesses. These vulnerabilities and weaknesses may lead to serious security threats to information.
- 8.2.5 Insiders have easy access information and IT systems. Network aids their access to the information and IT systems. They may be source or reason for compromise of security of information.
- 8.2.6 The new components and architectural elements incorporated as a part of the plan for infrastructure transition may introduce serious security issues. Adoption of trends such as mobility and usage of personally owned devices exposes the network to a new set of threats.

### 8.3 Network and infrastructure security management guidelines

- 8.3.1 **Inventory of assets and infrastructure:** The organization should ensure that a network diagram illustrating all network devices and other significant devices is available. Since this contains classified information, such documentation should be appropriately protected and its distribution should be limited. The organization must maintain and update a map/inventory of authorized devices such as:
- a) **Infrastructure components** spread across the organization and connected to the network endpoints, server systems, applications, databases and data files, and messaging systems.
  - b) **Connectivity and access** to users, endpoints, devices, server systems, applications, databases and messaging systems should be recorded and maintained.
  - c) **The spread of the organizational assets** across the operational functions and geographies and their access requirements should also be recorded.
- 8.3.2 **Security testing of network & infrastructure devices:** All infrastructure and network hardware may be procured, from manufacturers or resellers who are authorized by manufacturers, with reasonable demonstration of compliance with global security best practices.
- 8.3.3 **Network perimeter security:** The government organization must secure the Network perimeter by deploying competent security solutions
- 8.3.4 **Network zones:** The organization must divide their networks into multiple functional zones according to the sensitivity or criticality of information or services in that zone. Wherever possible, physical isolation must be performed
- a) **Access from external environment:** Sensitive IT assets must not be directly accessible from the external environment

- b) **Network segmentation technologies:** The organization must ensure that appropriate network segmentation technologies are enforced to logically and physically isolate the network and protect classified information and critical services (such as user authentication and user directory information)
  - c) **Operating zones for users:** Environment that allows internal user's access to information assets and systems should be separated from the environment created for external users.
- 8.3.5 **LAN security:** The organization must develop, document and periodically update security policies and procedures related to Local Area Networks (LAN).
- a) The organization must evaluate risks associated with transmission of classified information over LAN on a periodic basis.
  - b) The organization must clearly define roles and responsibility of personnel for supporting planning and implementing of LAN security, through appropriate job functions.
  - c) The organization must ensure that appropriate security measures, tools and methodologies are implemented to protect transmission of classified information over LAN. Traffic over LAN should be protected with use of appropriate encryption methodologies
- 8.3.6 **Wireless architecture:** The organization must ensure that Wireless LAN (WLAN) planning and implementation incorporates security best practices. However in DGAQA wireless configuration is to be disabled.
- a) **Confidentiality and integrity:** The organization must implement appropriate encryption for transmission of classified information over WLAN.
  - b) **Administration of access points:** The access to WLAN key distribution program should be controlled and limited to the administrators only.
  - c) **Logging of device activities and audit trails:** Network traffic and access to the WLAN should be logged by using suitable methodologies.
- 8.3.7 **Network security management:** Network security management processes should be created and documented. These processes should define the governing procedures for any security mechanism, changes or modification to the network configuration, the approval matrix, backup mechanisms, guidelines for testing and failover switching amongst others. The organization should ensure that all network security management tasks are approved and performed under the aegis of a single authority or team.
- 8.3.8 **Unauthorized device connection:** Organizations should implement stringent measures to minimize the risk of unauthorized devices from accessing the network. The necessary countermeasures must be deployed to deter the attempts of unauthorized access.
- 8.3.9 **Extending connectivity to third parties:** The government organizations must integrate the infrastructure security with other security solutions such as identity & access management, security monitoring & incident management for integrated defense and response against the threats.

## 8.4 Network and infrastructure security controls

- 8.4.1 **Identification & classification:** The organization must ensure that all infrastructure devices are grouped and classified in accordance to the criticality of the information that they contain/ process.
- 8.4.2 **Network diagram:** The organization must ensure that the network diagram is updated as changes are made to the network. The date of last modification should be clearly stated
- 8.4.3 **Network configuration:** The organization should regularly review their network configuration to ensure that it conforms to the documented network configuration.
- 8.4.4 **Testing and certification of network & infrastructure device:** Network and infrastructure devices should be tested basis globally accepted security standards, in appropriate test labs prior to their purchase. A secure and stable configuration of the device and product may only be procured for deployment.
- 8.4.5 **Network security measures:** The organization must ensure the competent Security counter measures for network security are established, such as:
- a) Perimeter defense.
  - b) Traffic inspection and detection of anomalies and threats
  - c) Detection and prevention of intrusion.
  - d) Filter, block and prevent the malicious traffic.
  - e) Restrict insecure ports, protocols and services
  - f) Protection against the denial of service and distributed denial of service attacks.
  - g) Restriction on connections to the external world and the internet.
  - h) Malicious code detection and filtering
  - i) Restrict, change and segment users access.
- 8.4.6 **Security of IPv6 device:** The organization must ensure that all dual-stack network devices, equipment and operating systems that support IPv6 must disable the functionality unless it is being used and appropriate security measure have been deployed for their protection. All future networks should be IPv6 compatible
- 8.4.7 **Segmentation:** The organization must create appropriate network Segmentation and maintain updated network access control lists.
- 8.4.8 **Security zones:** The organization must create separate zones for and apply additional security protections to network zones that contain classified information from the environment where their users access the Internet and external email.
- 8.4.9 **Network traffic segregation:** The organization must implement network access controls to limit traffic within and between network segments to only those that are required for operations.

- 8.4.10 **LAN security:** The organization must implement relevant controls to ensure security of information traversing the organizations Local Area Network (LAN).
- 8.4.11 **Wireless LAN security:** It should be disabled as wireless system is not authorized in DGAQA.
- 8.4.12 **Disabling unused ports:** The organization must disable unused physical ports on network devices such as switches, routers and wireless access points.
- 8.4.13 **Personal devices usage policy:** The organization must ensure that incase personally owned devices are permitted to be connected to the organizations network, a prior security validation must be performed on such devices a teach log-in instance to check for basic system health requirements. Devices which are non-compliant with health requirements should be quarantined.
- 8.4.14 **Restricting access to public network:** The organization must ensure that devices are prevented from simultaneously connecting to an organization controlled network and to a public data network.
- 8.4.15 **Network access control:** The organization must implement network access controls on all networks.
- 8.4.16 **Firmware upgrade:** The organization must ensure that firmware for network devices is kept up to date.
- 8.4.17 **Network change management:** All changes to the network configuration, in the form of upgrades of software and firmware or in the form of addition or removal of hardware devices and systems should be undertaken post approval from competent authority. All changes to the network configuration should be documented and approved through a formal change control process.
- 8.4.18 **Securing transmission media:** All cables and encompassing cabinets must be secured from unauthorized access, physical damage and tampering.
- 8.4.19 **Default device credentials:** The organization must ensure that default user names and passwords are changed before network devices are deployed.
- 8.4.20 **Connecting devices:** The organization must deploy appropriate monitoring and network scanning methodologies to detect systems connecting to the network and portable devices connected to work stations via USB ports
- 8.4.21 **Audit and review:** The organization must conduct periodic audits of network devices which are being added or removed from networks and create an inventory of authorized network devices.
- a) **Network logs:** The organization must set up logging of access and activity of network devices. Depending on the scale of the network components, organization may be also evolving to have automated alert systems wherever there is a deviation in the acceptable log parameters.
- 8.4.22 **Extending connectivity to third parties:** The connectivity to third party must be restricted.

## 8.5 Network and Infrastructure security implementation guidelines

- 8.5.1 **Identification and classification:** The organization must ensure that classified information is mapped with the infrastructure elements through which it will be transmitted, processed or stored.
- b) All infrastructure devices should be categorized as per classification of information that they manage
- 8.5.2 **Network diagram:** The organization must develop an accurate mapping of the core components, connections and information of the network to build organization's network diagram including network components such as routers, switches, firewall and computer systems, IP addresses, data flow routes, blacklisted or white listed systems/IP addresses, open/entry ports, subnet mask, administrative interface, zones, access control lists, network name amongst others.
- a) All amendments to network diagram should be documented with reason of change, nature of change, person responsible.
  - b) All previous configuration diagrams must also be retained for reference.
- 8.5.3 **Network configuration:** Organization must review network configuration periodically by using configuration audit and configuration comparison tools.
- a) The organization must establish a mechanism that compares the running configuration of network devices against the documented configuration.
  - b) There must be documented standards/procedures for configuring network devices (e.g. routers, hubs, bridges, concentrators, switches, firewalls, IPS,IDS etc.), which cover - security architecture, device configuration, access control to network devices, vulnerability and patch management, changes to routing tables and settings in network devices and regular review of network device configuration and set-up.
  - c) Security controls applied to network devices must incorporate security architecture principles (e.g. 'secure by design', 'defense in depth', 'secure by default', 'default deny', 'fail secure', 'secure in deployment' and 'usability and manageability').
- 8.5.4 **Testing and certification of network & infrastructure device:** Devices deployed must be tested and certified prior to their implementation in the organization's environment
- a) Network and infrastructure devices must be self-certified by the manufacturer.
  - b) Network and infrastructure devices must be tested and certified Cert –in empanelled /recognized lab.
  - c) The organization must ensure comprehensive network and infrastructure device testing from established testing labs of STQC, DRDO or other designated government test labs
- 8.5.5 **Network security measures:** For perimeter defense, organization must use appropriate security capability, such as
- a) For traffic inspection and detection of anomalies and threats organization should implement Security Information and Event Management (SIEM) capability.

- b) Organization should deploy Intrusion Detection System (IDS) capabilities to monitor network or system activities for malicious activities or policy violations.
- c) Organization should deploy Intrusion Prevention System (IPS) capabilities to identify malicious activities in the network, log information and attempts to block them.
- d) For protection against the distributed denial of service (DDoS) and denial of service (DoS) attacks appropriate protection must be incorporated in-house such as on premise traffic filtering equipment or from service providers for services such as traffic-routing service through Border Gateway Protocol, DNS change to traffic snubbing centers, cloud based mitigation etc.
- e) The organization should conduct or participate in mock drill exercises to test network security measure

**8.5.6 Security of IPv6 device:** The organization should have security measure specific to IPv6 security

- a) Disable IPv6 functionality at the gateway level until and unless required for use by organization with additional DoS security measures. Block all IPv6 traffic on IPv4- only networks
- b) Use standard, non-obvious static addresses for critical systems.
- c) Firewall, IDS/IPS must be able to scan IPv6 traffic and enforce policies on the same.
- d) The event and transaction logging mechanism must be capable of capturing activity of IPv6 devices.
- e) All future networks should be IPv6 compatible.

**8.5.7 Segmentation:** To restrict, segment and modify user access, organization should deploy tools such as Active Directory to limit or grant permissions to a user

- a) The organizations must ensure segmentation of the network to create security zones for isolating sensitive traffic and secure critical IT systems. This is typically done by using means such as establishing Demilitarized Zone (DMZ) and configuring virtual LANs
- b) Organization should limit and segment user rights for access by implementing proper Access Control Lists in the network. Access controllistsshouldbeconfiguredondevicessuchasroutersand/orswitches

**8.5.8 Security zones:** Virtual LAN should be used by an organization to logically separate zones which deal with confidential information from the rest of the network.

- a) VLANs should not be used between classified networks and any other sensitive networks
- b) VLANs between classified networks and any other network of a lower classification must not be used.
- c) VLANs between a sensitive or classified network and public network infrastructure must not be used.
- d) VLAN trunking must not be used on network devices managing VLANs of differing security classifications
- e) Administrative access for network devices using VLANs must only be permitted from the most trusted network.



- 8.5.9 **Network traffic segregation:** Organization should enforce rule set to minimize methods and level of access to classified information in order to limit access to authorized personnel.
- a) Implementation of traffic flow filters, VLANs, network and host based fire walls,
  - b) Implementation of application level filtering, proxies, content-based filtering etc.
  - c) Wherever possible physical segregation must be preferred over logical segregation
- 8.5.10 **LAN security:** The organization must implement the following to ensure LAN security:
- a) **Securing LAN devices:** Ensure that all default passwords of routers and switches are changed prior to deployment.
  - b) **Strong device passwords:** Use strong passwordssuchusingaminimumof12 characters or more (combination of alphanumeric and special characters)
  - c) **Using secure protocols:** Disable all non-IP-based access protocols such as TELNET, and use secure protocols such as SSH, SSL, or IP Security (IPSec) encryption for all remote connections to the router/switch/server
  - d) **Traffic monitoring:** Deploy traffic management capabilities which continuously monitors and controls IP network
  - e) **Allocating IP address:** Ensure that IP addresses allocated to each network appliance/system/server is associated with their respective MAC address and is not user modifiable.
- 8.5.11 **Wireless LAN security:** DGAQA does not implement Wireless LAN. Hence all the devices must be disabling for wireless connectivity.
- 8.5.12 **Disabling unused ports:** The organization must identify ports, protocols and services required to carry out daily operations and block all others, including all non-IP based and unencrypted protocols, by establishing policies in routers and wireless access points
- 8.5.13 **Personal devices usage policy:** Use of personal devices must be authorized by concerned personnel of the organization, with documented forms maintained to reflect approvals and rejections. This documentation should include fields such as employee name, employee ID, device approved/rejected status, date and time, device id entity and type etc. (refer section 20.2)
- a) The organization must perform security check of the personal device prior to authorization for use in official premises. A comprehensive security evaluation of the device must be performed to ensure no security loop hole is induced in the network due to introduction of such devices. These checks should include at a minimum checking for malwares, open ports, installed firewall, antivirus, latest system patches installed amongst others.
- 8.5.14 **Restricting access to public network:** The organization must disable unused network adapters in systems and restrict internet connection sharing and ad hoc network creation.
- a) Organization owned information assets should be configured to connect to organization owned / operated networks only

- b) Organization must disable Internet connection sharing, Ad hoc networks, Routing between virtual private network interfaces and other network interfaces on all organization owned devices

8.5.15 **Network access control:** The organization must implement network access control mechanism across the network

- a) Verify identity of device upon request to connect to the network
- b) Perform health scan of device post access to network resources
- c) Authorize access to information sources post validation of policy implementation and update in device
- d) There must be documented standards/procedures for managing external network access to the organization's information systems and networks, which specify: List of external connections must be maintained, access control must be implemented, allow only authorized remote device, external connection must be removed when no longer required
- e) Information systems and networks accessible by external connections must restrict external network traffic to only specified parts of information systems and networks as per the business requirements, provide access to defined entry points, verify the source of external connections, log all security-related activity, record details relating to external connections established
- f) Access to the network must be restricted to devices that meet minimum security configuration requirements, which includes verifying that devices which are authorized, are running up-to-date malware protection, have the latest systems and software patches installed, are connecting over an encrypted network
- g) There should be policy for use of firewalls, remote access, VOIP and Telephony and Conferencing

8.5.16 **Firmware upgrade:** Organization must regularly check for updated firmware for network appliances. All upgrades must be installed post appropriate validation and testing.

8.5.17 **Network change management:** Organization must test/simulate the changes required for the network in the network simulator tools before implementing in live environment.

- a) Ensure that appropriate test and simulation facility/ lab is available
- b) Select and download appropriate patches/ upgrades and prepare them for test and simulation in facility/lab.
- c) Examine test results to ensure there are no conflicts with existing patches /upgrades
- d) Appropriate permissions should be obtained from the concerned department
- e) Significant changes to network configuration must be approved by the ISSC



**8.5.18 Securing transmission media:** All cables and encompassing cabinets must be secured from unauthorized access, physical damage and tampering.

- a) Ensure proper mapping and labeling of transmission media.
- b) Physical access to cables must be restricted.
- c) All connectivity points must be secured inside a cabinet.

**8.5.19 Default Device Credentials:** The organization must ensure that default credentials of network devices and information systems such as username, passwords, tokens are changed prior to their deployment or first use.

**8.5.20 Connecting Devices:** The organization must identify active hosts connected to its network using tools and techniques such as IP scanners, network security scanners etc.

- a) Deploy client side digital certificates for devices to authorize access to network or information resources.

**8.5.21 Extending connectivity to third parties:**

- a) The organization must restrict the use of ports, service, protocol etc. used for extending access of organization network to third parties.
- b) The organization must limit the access granted to third parties to the purpose of granting such access and to the time duration specified for completion of defined tasks.
- c) The organization must ensure that network documentation provided to a third party, such as to a commercial provider, must only contain information necessary for them to undertake their contractual services and functions. Detailed network configuration information must not be published in documentation
- d) All traffic emanating from third parties must be monitored

## **9.0 Identity, access and privilege management**

### **9.1 Background**

**9.1.1** Users have a diverse set of access requirements based on their roles and privileges that lead to complex authentication, access, role & privilege management scenarios in respect of access to information and information systems.

**9.1.2** The access requirements vary widely from providing access to endpoints to network, server systems, applications, data and databases, messaging systems, and so on. Organization's information is stored, processed and shared over these components of infrastructure. Access to these systems may expose the users to the information.

- 9.1.3 Further, users and user groups, with their respective operational roles, seek access to different information assets for diverse purposes and through various platforms and means. Changing operational ecosystem introduces significant level of dynamism in access requirements in the life cycle of information and information systems

## 9.2 Relevance of domain to information security

- 9.2.1 Identity breach is one of the most common threats for organization: intruders try and defeat the organizations authentication scheme; or might steal a critical element of their identity; or might misuse an attribute of their identity to engage in fraud.
- 9.2.2 As there is significant complexity of users identities, privileges and access patterns, the organization may struggle to comprehend the exposure of information and exposure of information to unintended person may get unnoticed.
- 9.2.3 Without specific attention on identification, access and privilege management of employees of external service providers and vendors, information may be exposed outside the boundaries of an organization.

## 9.3 Identity, access and privilege management guidelines

- 9.3.1 **Governance procedures for access rights, identity & privileges:** The organization must establish appropriate procedures to govern access rights to information systems and assets; establish a process for creation of identities; establish a process for defining user privileges and a devise a mechanism to understand how access to information is provided.
- a) Each information assets must have an appointed custodian or owner, who should be responsible for classification of data and approving access to the same.
  - b) Information about the user identities, privileges, access patterns must be managed in secure manner.
  - c) The management oversight must be enforced through the process of approval, monitoring and review to manage identity, users and privileges through their life cycles- identity request, creation, assignment, operations and revocation.
  - d) The changes should be approved by a designated authority
  - e) The changes should be recorded for any future analysis.

**9.3.2 Authentication & authorization for access:** The organizations must establish processes for authenticating each user accessing information systems or assets. The access requests should be authorized based on predetermined rules that consider type of information, access types, access requirements, user's roles and security requirements (Refer section 7.2)

- a) Instances that authenticate users and authorize their access to critical information must be recorded.
- b) Inactive accounts must be disabled as per the organization's policy

**9.3.3 Password management:** The organizations must have standardized, reliable and secure way of managing passwords of users.

- a) A standard for password must be defined length, type of characters permitted.
- b) Password history, password change duration etc. should be determined depending on the sensitivity of information and transactions.
- c) Password reset requests must be handled carefully and securely.
- d) Password of privileged user accounts should be handled with additional care.
- e) Shared passwords with vendors must be changed regularly

**9.3.4 Credential monitoring:** The organization must ensure that instances of user access provisioning, identification, authentication, access authorization, credential changes and deprovisioning are logged.

- a) The access instances should be monitored and reviewed for identifying discrepancies.
- b) Malicious attempts of authentication should be prevented, recorded and reviewed.

**9.3.5 Provisioning personal devices and remote access:** The organizations must ensure that provisioning of access to employees of external service providers and vendors is managed in a standardized and secure manner

**9.3.6 Segregation of duties:** The organization must ensure that user roles are appropriately segregated for performing operations. It should be ensured that user levels and their designated actions are segregated based on the criticality of information and transactions.

- a) Each user action must be distinguished from other users. Any discrepancies must be identified, reviewed and corrected.

**9.3.7 Access record documentation:** The organization must ensure that it maintains an updated record of all personnel granted access to a system, reason for access, duration for which access was granted.

9.3.8 **Linkage of logical and physical access:** The organizations must correlate logical access instances with physical access rules for areas where sensitive information is processed and stored.

9.3.9 **Disciplinary actions:** The organizations must incorporate provisions for managing discrepancies and non-conformance in the disciplinary processes.

## 9.4 Identity, access and privilege management controls

9.4.1 **Operational requirement mapping:** The organization must ensure that operational requirements are carefully studied to translate them into access requirements.

9.4.2 **Unique identity of each user:** The organization must ensure that each user identity (User-ID) is uniquely attributable to only one unique user.

9.4.3 **User access management:** The organization must document procedures for approving, granting and managing user access including user registration/de-registration, password delivery and password reset. The procedures must be updated in a periodic manner as per policy

- a) **Authorization for access:** The organization must not allow access to information unless authorized by the relevant information or information system owners.

9.4.4 **Access control policies:** The organization must define access control policies which are integrate-able with existing architecture and technological, administrative and physical controls.

9.4.5 **Need – to – know access:** Access rights to information and information systems must only be granted to users based on a need-to-know basis.

9.4.6 **Review of user privileges:** The organization must enforce a process to review user privileges periodically.

9.4.7 **Special privileges:** The organization must ensure that the use of special Privileges shall be restricted, controlled and monitored as per organization's policy.

9.4.8 **Authentication mechanism for access:** The organization must enforce appropriate authentication mechanism to allow access to information and information systems which is commensurate with the sensitivity of the information being accessed.

9.4.9 **Inactive accounts:** Inactive accounts must be disabled as per organizations policy.

9.4.10 **Acceptable usage of Information assets & systems:** The organization must define an acceptable usage policy and procedures specifying the security requirements and user responsibility for ensuring only organization mandated.

9.4.11 **Password policy:** The organization must define a password policy.

- a) Password standards- such as minimum password length, restricted words and format, password life cycle, and include guidelines on user password selection.
- b) Password reset process must be set in order to secure the credential in the process.

9.4.12 **Monitoring and retention of logs:** The organization must monitor and retain records for all activity related to granting access to users.

9.4.13 **Unsuccessful log-in attempts:** The organization must monitor all log-in attempts to information systems and block access to users with consecutive unsuccessful log-in attempts.

- a) The organization must ensure appropriate monitoring mechanism is available to identify fraudulent or malicious activity. The authorization credentials of user accounts suspected of being compromised must be reset immediately

9.4.14 **Ad-hoc access to systems:** The organization must ensure that prior approval from the head of the department is obtained in-case it is required to connect a departmental information system with another information system under the control of another organization. The security level of the information system being connected shall not be downgraded upon any such interconnect of systems

- a) Under any circumstances the authorization level should not allow vendors to access sensitive information / database of the organization. If needed proper supervision mechanism may be evolved to watch the activities of the vendors

9.4.15 **Remote access:** The organization must ensure that security measures are in place to govern the remote access to information systems.

- a) Appropriate security technologies must be implemented to protect information or information systems being accessed via remote access. These may include use of protocols such as SSL, TLS, SSH and IP sec.

9.4.16 **Provisioning of personal devices:** The organization must govern provisioning of access to personal computing devices such as smart phones, tablets, and memory devices to its internal network as per its security policy.

9.4.17 **Segregation of duties:** The organization must ensure that duties, roles, responsibilities and functions of individual users are segregated, considering Factors such as conflict of privileges.

9.4.18 **User awareness & liability:** The organization must ensure that all users are made aware of their responsibilities towards secure access to and usage of the organizations information and information systems. All users shall beaccountableandresponsibleforallactivitiesperformedwiththeirUser-IDs

## 9.5 Identity, access and privilege implementation guidelines

**9.5.1 Operational requirement mapping:** The organization must develop a formal procedure to govern allocation of user identification and access mechanism. All privileges associated with a user-ID must also be governed as per standard procedure.

- a) Operational roles must be mapped to corresponding IT roles.
- b) IT roles must be grouped for performing particular operations.
- c) Credential requirements of the roles must be mapped carefully.
- d) Operational rules for granting and revoking access must be studied and an inventory should be created of the same.

**9.5.2 Unique identity of each user:** All employees including temporary and contract workers must be allotted a unique ID. The system for managing user IDs must function directly under the head of the department or his authorized representative.

- a) User identity schemes must be defined and enforced.
- b) Identity provisioning workflow must be defined with proper checks and balances
- c) Identity provisioning process must be audited at periodic interval
- d) Any sharing of user ID's should be restricted to special instances, which are duly approved by the information or information system owner.
- e) The shared ID's passwords must be changed promptly when the need no longer exists and should be changed frequently if sharing is required on a regular basis.
- f) There must be clear ownership established for shared accounts.
- g) There must be a log maintained as to whom the shared ID was assigned at any given point of time. Multiple parallel sessions of the same ID must be strictly prohibited.

**9.5.3 User access management:** The organization must establish a process to manage user access across the lifecycle of the user from the initial registration of new users, password delivery, password reset to the final de-registration of users who no longer require access to information systems and services in the organization

- a) Details of users authorized by the head of the department to access information systems and devices must be communicated as per standard user access request form containing details such as name of person, location, designation, department, and access level authorization, access requirement for applications, databases, files, and information repositories etc.

- b) Any changes or update to user access level must be made only post approval from head of department.
- c) User access deactivation request must be submitted immediately upon termination of employment, instances of non-compliance, suspicious activity and in case required as part of disciplinary action etc.
- d) The organization must ensure that all user access requests are well documented with details including, but not restricted to, reason for access, user details, type or user – admin, super user, contractor, visitor etc., period of access, HOD approval, information as set/ system owner approval

9.5.4 **Access control policies:** The organization must enforce, govern and measure compliance with access control policy.

- a) **Enforcement of access control policies:** Access control policies must be defined to be enforced on ICT infrastructure components such as network, endpoints, servers systems, applications, messaging, databases and security devices.
- b) **Governance of access control policies:** Access to the systems, network resources and information must be governed as per organization's policies.
- c) **Compliance with access control policies:** Non-conformance to policy must be monitored and dealt with as per standard practice defined by organization.
- d) **Correlation of logical and physical access:** The organization must implement a mechanism to correlate instances of physical access and logical access using IP enabled physical security devices, collection and correlation of logs and rules written to correlate physical and logical instances.

9.5.5 **Need – to – know access:** Access privileges to users must be based on operational role and requirements

- a) Access to higher category of classified information must not be granted unless authorized by information owner.
- b) Access to systems containing higher category of classified information must be restricted by logical access control.
- c) Access security matrix must be prepared which contains the access rights mapped to different roles. This must be done to achieve the objective of role based access control (RBAC).
- d) Access to system must be granted based on access security matrix.

9.5.6 **Review of user privileges:** All user accounts must be reviewed periodically by concerned authority by use of system activity logs, log-in attempts to access non-authorized resources, abuse of system privileges, frequent deletion of data by user etc.



9.5.7 **Special privileges:** The organization must ensure that the use of special privileges for users to access additional information systems, resources, devices are granted only post documented approval from information owner

- a) All such additional privileges must be issued for a pre-notified duration and should lapse post the specified period.
- b) Allocation of special privileges must be strictly controlled and restricted to urgent operational cases.
- c) All activity conducted with the use of special privileges must be monitored and logged as per organization's policy.

9.5.8 **Authentication mechanism for access:** The organization must have various levels of authentication mechanisms.

- a) Depending on the sensitivity of information and transactions, authentication type must vary
- b) For access to sensitive information system, authentication such as 2-factor authentication should be implemented. Authentication levels must be defined to include a combination of any two of the following authentication mechanisms:

Level 1: PIN number or password authentication against a user-ID

Level 2: Smart card or USB token or One-time password

Level 3: Biometric identification

- c) Credential sharing must be performed on an encrypted channel which is separate from the message relay channel.

9.5.9 **Inactive accounts:** The organization must ensure the following:

- a) All user accounts which are inactive for 45 days should be disabled.
- b) The authentication credentials of all disabled accounts must also be reset upon deactivation.
- c) All disabled accounts must be reactivated only post verification of the user by concerned security administrator
- d) All accounts in disabled state for 30 days must be deleted.

9.5.10 **Acceptable usage of Information assets & systems:** The organization must ensure that users are made aware of their responsibility to use their account privileges only for organization mandated use

- a) The organization must clearly state that it provides computer devices, networks, and other electronic information systems to meet its missions, goals, and initiatives and users must manage them responsibly to maintain the confidentiality, integrity, and availability of the organizations information.



- b) This needs to be elaborate across areas such as email, internet, desktops, information, clear desk policy, password policy etc.
- c) The organization must obtain user sign-off on acceptable usage policy.

9.5.11 **Password policy:** The organization must define its password policy, with specific focus on password issuance and activation methods along with standard process for governance and communicate the same to user upon creation of user account

- a) All active sessions of a user must be terminated post 15 minutes of inactivity and must be activated only post re-authentication by specified mechanism such as re-entering password etc.
- b) Passwords must be encrypted when transmitting over an un-trusted communication network
- c) Issue guidelines to end user to help in selection of strong alphanumeric password comprising of a minimum of 12 characters
- d) Prevent users from using passwords shorter than a pre-defined length, or re-using previously used passwords
- e) Passwords must be automatically reset if user accounts are revoked or disabled upon inactivity beyond 30 days of inactivity
- f) Password communication must on verified alternate channel such as SMS, email, etc.

9.5.12 **Default device credentials:** The organization must ensure that default login credentials of devices such as routers, firewall, storage equipment etc, are changed prior to the deployment of such devices in the operational environment

9.5.13 **Monitoring and retention of logs:** The organization must retain information pertaining to requests for user ID creation, user rights allocation, user rights modification, user password reset request and other instances of change or modification to user profile, as per audit and governance requirements

9.5.14 **Unsuccessful login attempts:** The organization must monitor unsuccessful log-in attempts from each of the authentication mechanisms, to track for consecutive unsuccessful log-in attempts

- a) The user account must be disabled for a pre-defined limit post five unsuccessful log-in attempts.
- b) A random alpha numeric text CAPTCHA should be introduced post second unsuccessful log-in attempt

**9.5.15 Ad-hoc access to systems:** The organization must ensure that authentication credentials of information systems which are disclosed to vendors for maintenance and support are reset on a periodic basis or upon termination of maintenance activity, as defined under the organization's policy.

**9.5.16 Remote access:** Appropriate device configuration must be maintained and security capability must be deployed, to prevent remote access to information systems and data from outside the organizations boundary, unless approved by the head of the department.

- a) Implement appropriate security technologies to protect information or information systems being accessed via remote access, such as using VPN based on SSL/TLS, SSTP or IP sec.
- b) Enable capture of logs of all activity conducted via remote access
- c) Audit logs of all activity conducted via remote access

**9.5.17 Provisioning of personal devices:** Refer section 20.3

**9.5.18 Segregation of duties:** The organization must ensure the following:

- a) Separate duties of individuals as necessary, to prevent malevolent activity without collusion
- b) Documents separation of duties
- c) Implements separation of duties through assigned information system access authorizations.
- d) Restricts mission functions and creates distinct information system support functions are divided among different individuals/roles.
- e) Prevent different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security).
- f) Separate security personnel who administer access control functions from performing administer audit functions
- g) Create different administrator accounts for different roles

## **10.0 Physical and environmental security**

### **10.1 Background**

**10.1.1** Organizations generally have multiple touch points, which may be spread across different geographic regions, from where information can be accessed physically. Thus geographies, locations and facilities play an important role in the security posture of information and information systems.

- 10.1.2 Physical aspects have a role in determining how information and information systems are housed in a facility, who can possibly reach physical systems, which way one can enter or exit from the facility, what can human elements physically do with the system housed in a facility and what will be impact of regional physical events on the particular facilities.
- 10.1.3 Physical security is an important component of information security and requires a care full attention in planning, selecting countermeasures, deploying controls, ensuring secure operations and respond in case of an event.
- 10.1.4 Physical security is not only restricted to barriers or locks but have evolved with the use of access control measures, risk based or multifactor authentications, monitoring cameras, alarms, intrusion detectors, etc.

## 10.2 Relevance of domain to information security

- 10.2.1 Lack of due consideration to the area and to the choice of the building may expose information and IT systems to threats. Choice of the area, building architecture and plan have a significant impact on security posture of information and information systems
- 10.2.2 Insufficient entry controls may give access to unintended persons. It may allow entry of unauthorized assets or easy passage of sensitive assets from premises.
- 10.2.3 Without adequate interior physical control, unauthorized personnel may gain access to sensitive areas. Instances such as theft of information may remain undetected
- 10.2.4 Without processes for physical access provisioning and deprovisioning, governing access to the sensitive physical locations will remain a challenging task. This will have serious impact on security of information and information during their life cycle in a particular physical facility.

## 10.3 Physical and environmental security guidelines

- 10.3.1 **Map and characteristics of physical facilities:** The organization must create an map of access point and information assets and systems housed within
- 10.3.2 **Protection from hazard:** The organization must ensure that all facilities housing information systems and assets are provided with adequate physical security measures, which include protection from natural and man-made hazard
- 10.3.3 **Physical boundary protection:** The organization must deploy an adequate level of perimeter security measures such as barriers, fencing, protective lighting, etc.
- 10.3.4 **Restricting entry:** The organization must deploy an adequate level of counter measures for restricting the entry to the facilities only to authorized persons.

- 10.3.5 **Interior security:** The organization must ensure that all information systems and assets are accessed by only authorized staff and protected by adequate interior security measures
- 10.3.6 **Security zones:** The organization must ensure that appropriate zones are created to separate areas accessed by visitors from areas housing classified information assets and systems.
- a) **Basis information classification:** Appropriate security zones must be created inside the premises/ building based on the location of information assets and systems, commensurate with the classification of information
  - b) **Marking of zones:** Zones must be clearly marked to indicate type of personnel allowed access to the said zone with in the premise
  - c) **Security and monitoring of zones:** Strict security measures in addition to round the clock monitoring of such areas must be done.
- 10.3.7 **Access to restricted area:** Access of people and equipment movement and disposal from the restricted area should be regulated and governed. A special care must be taken for wearable devices. Such clearances should be done by the concerned head of the department. The organization must establish a methodology to ensure coordination between internal functions and staff for the same
- 10.3.8 **Physical activity monitoring and review:** All physical access to information assets and systems should be monitored and tracked. User should not be allowed to carry external devices such as laptops; USB drives etc. without prior approval and authorization, into areas which house critical information infrastructure such as data centers etc.

## 10.4 Physical and environmental security controls

- 10.4.1 **Map and characteristics of physical facilities:** The organization must obtain visibility over physical facilities and information systems housed within
- a) A list of persons who are authorized to gain access to information assets and systems housed in data centers or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and should be reviewed periodically.
- 10.4.2 **Hazard assessment:** The facility housing information assets and systems must be protected from natural hazard and man-made hazard. All facilities located in geographically vulnerable areas must undergo annual assessment to check structural strength.
- 10.4.3 **Hazard protection:** All facilities must be equipped with adequate equipment to counter man-made disasters or accidents such as fire. The facility should have a combination of hazard detection and control measures such as smoke sensors, sprinklers, fire extinguishers etc. Other sensors and alarms should also be installed for early warning.

- 10.4.4 **Securing gateways:** All entry and exit points to facilities housing information assets and systems must be secured by deploying manpower and appropriate technological solutions.
- 10.4.5 **Identity badges:** The entry to a facility is restricted to only those users who provide proof of their organizational identity. Users must be aware of the importance of carrying their identity proof with them
- 10.4.6 **Entry of visitors & external service providers:** the organization must define process for allowing and revoking access to visitors, partners, third-party service providers and support services
- 10.4.7 **Visitor verification:** All visitors to the facility must only be permitted to enter post validation from concerned employee. Visitor must be instructed to record their identity credentials into the visitor register prior to permitting them inside the facility.
- 10.4.8 **Infrastructure protection:** Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.
- 10.4.9 **Guarding facility:** The organization must ensure that an adequate number of security guards are deployed at the facilities.
- 10.4.10 **Vehicle entry:** Ensure that an adequate level of security measures are implemented for vehicle entry & exit, vehicle parking areas, loading/unloading docks, storage areas, manholes, and any other area that may provide passage for physical intrusion
- 10.4.11 **Correlation between physical and logical security:** The instances of physical access should be analyzed with logical access instances. Restrictions should be imposed for on premise access of information systems to unauthorized personnel.
- 10.4.12 **Monitoring & surveillance:** All entry and exit points should be under surveillance round the clock to look for suspicious activity. Further, all security zones inside the facility/ building must be secured by deploying manpower and appropriate security technologies.
- 10.4.13 **Disposal of equipment:** Physical disposal of computer or electronic office equipment containing non-volatile data storage capabilities must be checked and examined to ensure all information has been removed. Destruction, overwriting or reformatting of media must be approved and performed with appropriate facilities or techniques such as degaussing of hard drives, secure delete technologies etc.(ReferAnnexure7.2)
- 10.4.14 **Protection of information assets and systems:** All information assets and systems must be protected with appropriate access control methodologies such as authorized log-in and password control, smart cards or biometric access.
- 10.4.15 **Authorization for change:** Ensure that security authorization is performed for all changes pertaining to physical security, instances that may introduce security vulnerabilities and exception to the policy.

- 10.4.16 **Inactivity time out:** All information systems must be configured to time-out a user's activity post inactivity for a designated period of time.
- 10.4.17 **Protection of access keys and methodology:** All access keys, cards, passwords, etc. for entry to any of the information systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures
- 10.4.18 **Shoulder surfing:** The display screen of an information system on which classified information can be viewed shall be carefully positioned so that unauthorized persons cannot readily view it.
- 10.4.19 **Categorization of zones:** The facilities in the organization must be categorized based on parameters such as the sensitivity of information in the facility, roles of employees in facilities, operational nature of facility, influx of visitors etc.
- 10.4.20 **Access to restricted areas:** Visitors requiring access to restricted areas, in – order to perform maintenance tasks or activities must be accompanied by authorized personnel from the concerned department at all times. A record of all equipment being carried inside the facility must be maintained along with equipment identification details. Similarly a record of all equipment being carried outside the facility must be recorded and allowed post validation and written consent from employee concerned
- 10.4.21 **Visitor device management:** Visitors must be instructed to avoid carrying any personal computing devices or storage devices inside facilities housing classified information, unless written permission is obtained from the head of the department.
- 10.4.22 **Physical access auditing and review:** All attempts of physical access must be audited on a periodic basis.

## 10.5 Physical security implementation guidelines

- 10.5.1 **Map and characteristics of physical facilities:** The organization must appropriately position security and monitoring measures commensurate with criticality of Physical facilities, information and IT systems housed within these facilities.
- a) Create map of facilities, their entry & exit points, deployment of IT systems and people.
  - b) Create list of authorized personnel, permitted to access areas/ facility housing sensitive information systems/ devices, and should be maintained at all entry points.
  - c) Physical access to such areas/ facility must be granted only post verification of person as well as by user authentication by use of smart cards, etc.

- 10.5.2 **Hazard assessment:** The organization must undergo hazard assessment at regular intervals to counter disasters or accidents such as fire safety risk assessment, seismic safety assessment, and flood control assessment and other natural calamities amongst others
- 10.5.3 **Hazard protection:** The organization must deploy sufficient tools, techniques, equipment etc., to deal with hazard. Capability for detection, prevention and control measures such as fire alarms, sprinklers, fire extinguishers, safety evacuation plans, clear exit markings must be available in each facility housing classified information.
- 10.5.4 **Securing gateways:** All entry and exit points to facilities/areas housing classified information in an organization must have biometric access controls such as fingerprint scanners or other similar gateway access control mechanisms.
- 10.5.5 **Identity badges:** The organization must issue photo identity cards with additional security features such as smart chips to employees for identification and entry to facilities.
- a) Appropriate measures must be undertaken to prevent tailgating inside the organizations facility.
- 10.5.6 **Entry of visitors & external service providers:** The organization should maintain records for visitor entry such as name of visitor, time of visit, concerned person for visit, purpose of visit, address of the visitor, phone number of the visitor, ID proof presented, devices on-person etc.
- a) Entry by visitors such as vendor support staff, maintenance staff, project teams or other external parties, must not be allowed unless accompanied by authorized staff.
  - b) Authorized personnel permitted to enter the data center or computer room must display their identification cards at all instances.
  - c) Visitor access record shall be kept and properly maintained for audit purpose. The access records may include details such as name and organization of the person visiting, signature of the visitor, date of access, time of entry and departure, purpose of visit, etc.
  - d) The passage between the data center/computer room and the data control office, if any, should not be publicly accessible in order to avoid the taking away of material from the data center/computer room without being noticed.
- 10.5.7 **Visitor verification:** Visitor entry must be permitted only if prior notification has been shared via email from the concerned personnel.
- a) Visitors must present a valid photo identification card, preferably issued by the Government of India at the reception, for verification
  - b) Visitors must always be escorted by the concerned person into the designated meeting area in the facility.



- c) Visitors should be issued a temporary identity card that identifies them as a visitor and must be returned to issuing authority while leaving the premises after marking out time in the visitor's record.

#### 10.5.8 **Infra structure protection:**

- a) Power and telecommunication lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.
- b) Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.
- c) Power cables and switching centers should be segregated from communication cables to prevent interference.

#### 10.5.9 **Guarding facility:** Background checks of all private guards manning the facility should be conducted prior to employment/ deployment. Details such as address verification, criminal records, past experience, references, family details, and medical records must be maintained as a minimum.

- a) Ensure that background checks and credibility is established prior to recruitment of guards. In- case guards are hired from a third party organization a stringent process to verify and establish credibility of the third-party organization must also be undertaken.
- b) The organization must conduct regular trainings for security guards to handle routine security operations as well as security incidents, physical intrusions, awareness about news to rage devices, etc.

#### 10.5.10 **Vehicle entry:** Adequate security measures should be adopted at vehicle entry, exit and parking areas such as deploying physical barriers, manual inspection of vehicles, security lighting, video surveillance, deploying adequate security guards etc.

#### 10.5.11 **Correlation between physical and logical security:** Physical security and logical security link ages must be created.

- a) Only approved personnel should have physical access to facility housing systems or devices which enable physical or logical access to sensitive data and systems. This includes areas within the facility which house backup tapes, servers, cables and communication systems etc.
- b) Access controls should encompass areas containing system hardware, network wiring, backup media, and any other elements required for the system's operation.

#### 10.5.12 **Monitoring & surveillance:** The organization must establish mechanism for surveillance of all areas inside the physical perimeter by use of technology such as security cameras (or closed-circuit TV).

- a) The organization must monitor the areas such as hosting critical/sensitive systems and have video images recorded. There cording of the camera should be retained for at least a month for future review.

- b) Intruder detection systems can be considered to be installed for areas hosting critical/sensitive systems

10.5.13      **Disposal of equipment:** Destruction and disposal of hard drives/ memory devices should be performed by techniques such as removing magnets, hammering, burning, degaussing, shredding, secure deletion etc.

- a) Any equipment, being carried out of the facility for disposal, must be authorized by the head of the department, under whom the equipment was deployed as well as the concerned representative of the information security team.

10.5.14      **Protection of information assets and systems:** Physical access to information assets and systems must be governed by employing techniques such as biometric access, smartcards, passwords etc.

10.5.15      **Authorization for change:** Any modification or changes to the physical security layout/ established procedure must be done post documented approval of concerned authority in the security team/Head of the department.

10.5.16      **Inactivity timeout:** All information systems should be configured to automatically lock the computer system after 10 minutes of inactivity

10.5.17      **Protection of access keys:** All access keys, cards, passwords, etc. for entry to any of the information systems and networks shall be physically secured or subject to well- defined and strictly enforced security procedures.

- a) Maintain a record of all physical access keys by capturing details such as serial number, card ID.
- b) Create a mapping of physical cards issued with details of person authorized to use the same.
- c) Establish governance and audit procedures to manage issue of all physical access cards and eventual return to concerned authority on employee departure or revocation of access rights of individual authorized to access using physical cards.

10.5.18      **Shoulder surfing:** Information systems containing classified information should be secured, to avoid shoulder surfing, by deploying privacy filter, positioning the systems to reduce chances of unauthorized viewing.

10.5.19      **Visitor device management:** Visitors must not be allowed to carry personal computing or storage devices such as USB, laptop, hard drive, CD/DVD etc. unless written permission is obtained from head of department.

- a) Wearable devices: Visitors must be prohibited from carrying any wearable computing and processing devices such as smart watch's, glass or similar equipment.
- b) All visitors and Third parties authorized to carry information processing equipment (like Laptops, Ultra books, PDAs) or Media (like Mobile phones with cameras, DVD/CDs, Tapes, Removable storage), shall be asked to declare such as sets. They will be issued a returnable gate pass containing the date, time of entry

and departure along the type of equipment and its serial number, if applicable. The same shall also be recorded in a register at the security gate.

- c) Equipment like laptops, hard disks, tape drives, camera mobile phones, etc. shall not be allowed inside the restricted areas, shared services area, etc. unless authorized by the concerned authority.

**10.5.19 Physical access auditing and review:** All attempts of physical access must be captured in logs and audited for illegal access attempts, number of access attempts, period of access, facilities visited etc. The following steps should be undertaken.

- a) Enabling and collecting logs physical devices.
- b) Writing rules to correlate logs to identify physical security incidents.
- c) Integrating physical security logs with logical security logs.
- d) Integrating physical security with SIEM solutions.
- e) Real time monitoring of physical security logs for classified information.

## **11.0 Application security**

### **11.1 Background**

11.1.1 Application portfolios of organizations are becoming increasingly complex with a mix of legacy applications, addition of new applications, deployment of enterprise packaged applications and adoption of externally provisioned applications. Each of these applications and their modules provide means of achieving a certain set of organizations objectives. These variations at various fronts expose information to a larger threat landscape.

11.1.2 Protecting applications against attacks simply by defending the perimeter with firewalls and network traffic encryption has proven to be insufficient. To address the risks at application layer, several technology and tactical measures have emerged that have helped the evolution of 'application security' as an important discipline in itself. The application itself should build in additional security measures, depending on the vulnerability of the system and the sensitivity of the data it is dealing with.

### **11.2 Relevance of discipline to information security**

11.2.1 As most information, both for operational and governance operations, is processed and transacted through applications, it becomes important to secure applications throughout their lifecycle.

11.2.2 Information of the organization may be compromised or exposed if applications are not securely designed, developed, tested, configured and deployed.

11.2.3 Inadequate visibility over how applications handle information; inadequate effort and resources deployed for application security; and lack of key application security capabilities endanger security of information.

11.2.4 Applications liberate access to information and information systems, providing multiple avenues for internal as well as external users to connect and perform their respective tasks. However, they provide opportunities to attackers or introduce security threats which may help attackers penetrate into information systems.

11.2.5 Applications are undergoing continuous innovation, several architectural ideas and platforms are under evolution and numerous have already been deployed. New ways of managing and setting up sessions are being implemented and transaction processing is undergoing change with respect to the way information is handled. This makes applications vulnerable to many new types of attacks.

### 11.3 Application security guidelines

**11.3.1 Application security process:** The organization must establish application security processes to ensure all tasks performed for securing applications are done in a standardized manner.

**11.3.2 Application design:** The organization must ensure that the system specification and design phase should incorporate necessary and relevant practices for application security.

**11.3.3 Application threat management:** The organization must ensure a threat model is built, and threat mitigation measures are present in all design and functional specifications by analyzing high-risk entry points and data in the application

**11.3.4 Application security testing:** The organization must have a plan for testing applications for identifying vulnerabilities and weaknesses.

**11.3.5 Data management:** Information owners must evaluate the sensitivity of their data and define associated parameters for securing information.

**11.3.6 Application lifecycle management:** The organization must ensure that appropriate security measures such as version control mechanism and separation of environments for development, system testing, acceptance testing, and live operation are adhered with

**11.3.7 Application vulnerability intelligence:** The organization must ensure that it compiles information around application vulnerabilities, exposures and weaknesses. The information should be compiled from both internal and external sources.

**11.3.8 Application security governance:** The organization must deploy a governance mechanism to ensure that the security issues of applications are timely identified, analyzed and remediated.

## 11.4 Application security controls

**11.4.1 Application security process:** The organization must ensure that documentation and listing of applications is properly maintained and relevant personnel are tasked with dedicated responsibilities for application security.

**11.4.2 Application security architecture:** The organization must ensure that application security is considered during the design of application.

- a) Application security controls should be planned in early stages of the development rather than post deployment.

**11.4.3 Application user authentication:** User authentication by the application must be managed in a standardized manner.

**11.4.4 Secure configuration:** Ensure that the application and system are properly and securely configured, including turning off all unused services and setting security configurations as per policy.

- a) Installation audit and control: The organization must audit and control the installation of all computer equipment and software.

**11.4.5 Ports & services:** Ensure that unused or less commonly used services, protocols, ports, and functions are disabled to reduce the surface area of attack

**11.4.6 Session management:** The organization must ensure that applications have proper and secure session management to protect the sessions from unauthorized access, modification or hijacking

**11.4.7 Input validation:** The organization must ensure that strict validation is applied to all input of the application such that any unexpected input, e.g. overly long input, incorrect data type are handled properly and would not introduce a exploitable vulnerability in to the application.

- a) Ensure that security mechanisms are designed to reject further code execution if application failure occurs.

**11.4.8 Error handling:** The organization must ensure that error handling by applications should not provide system information or become reason for denying service, impairing system or leading to a system crash

**11.4.9 Application security testing:** The organization must test applications to know their strength against contemporary security threats.

- a) Security testing schedule for the applications must be defined considering their criticality and sensitivity.
- b) Testing requirements, testing types, and frequency of testing should be defined for the applications.<sup>1</sup>

**11.4.10 Code review:** For sensitive applications, the source code must be reviewed for evaluating vulnerabilities. Code review should be done while new application is being developed or any significant changes are under progress.

**11.4.11 Black box testing:** Application security testing, vulnerability assessment and penetration testing, should be performed at a frequency determined by sensitivity of the information handled by applications.

**11.4.12 Data handling:** The organization must ensure that applications handle data in a secure manner.

**11.4.13 Least privileges:** The organization must ensure that applications are designed to run with least amount of system privileges necessary to perform their tasks.

**11.4.14 Segregation of duties:** The organization must ensure that the practice of segregation of duties is followed in such a way that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process.

**11.4.15 Secure Software Development Life-Cycle (SDLC) processes:** The organization must ensure that security is considered at different stages of application development, deployment and maintenance such as application conceptualization, requirement definition, architecture planning, development, testing, deployment, operation and continuous improvement.

**11.4.16 Application change control:** The organization must develop a change control procedure for requesting and approving application/system changes. All change activity must be documented.

**11.4.17 Application vulnerability intelligence:** Ensure that application threat management incorporates knowledge about vulnerabilities from both internal as well as external intelligence sources.

**11.4.18 Application logs & monitoring:** Ensure that applications have the capability of generating logs of exceptions, error or other instances which impact security.

## 11.5 Application security implementation guidelines

**11.5.1 Application security process:** The organization must maintain an updated document containing the list of authorized applications, their usage, custodian(s) assigned to each application, level of criticality, version implemented, Number of installed instances, application license details etc.

- a) Specific personnel must be entrusted with the task of application security, who should be accountable for defining and enforcing enterprise level standards and guidelines for application security.
- b) The application security process should specify tasks and activities required to be performed for application security.

- c) The process should drive and guide other organizational functions such as operations, application development and maintenance and infrastructure management for the purpose of application security.

**11.5.2 Application security architecture:** For applications developed in-house or sourced from a third party vendor, the organization must ensure that secure coding principles are adhered to.

- a) The web software applications must be developed as per secure coding guidelines such as the Open Web Application Security Project (OWASP) guidelines.
- b) Methods such as threat modeling, data flow, risk assessment etc. should be deployed to understand the threat exposure of an application.
- c) Application interactions, data handling, session management, processing of transactions, authentication, authorizations, etc. should be planned in early stages.
- d) The applications must not have hardcoded passwords to connect to other databases and start services.
- e) There must be application security standards developed and all applications must be subjected to those during the time of induction or during any major change release.

**11.5.3 Application user authentication:** Ensure applications integrate with central authentication systems to authenticate users.

- a) Authorization of users should be based on centralized system rather than at an individual application level. Application may be integrated with central authentication system such as active directory.
- b) Authorization and access to resources should be based role, affiliation and membership of group rather than individual basis.
- c) Periodic review of authorization should be performed.

**11.5.4 Secure configuration:** Ensure that applications are securely configured through use of secure protocols and services and measures such as implementing encrypted storage of data, using strong password for administrative access of application amongst others.

- a) Perform installation security audit prior to production launch and post major changes to the system.

**11.5.5 Ports & services:** The organization must identify ports, protocols and services required to carry out daily operations of application and restrict or block all others, including all non-IP based and unencrypted protocols, in addition to removing



unnecessary content such as server banners, help databases, online software manuals, defaulter sample files etc

**11.5.6 Session management:** Ensure that applications have secure session management to protect the sessions from unauthorized access, modification or hijacking.

- a) Protection measures include generating unpredictable session identifiers, limiting the session lifetime, applying appropriate logout function and idle session timeout, and filtering invalid sessions.
- b) Ensure that sessions established by applications are secured by using appropriate encryption technologies, especially when sensitive information is transferred using HTTPS/TLS protocols.
- c) Ensuring encrypting sensitive session contents using protocols such as S/MIME.

**11.5.7 Input validation:** Ensure applications validate input properly and restrictively, allowing only those types of input that are known to be correct. Examples include, but are not limited to, cross-site scripting, buffer overflow errors, and injection flaws amongst others.

- a) Organization should ensure that applications validate the data on the server-side and not on client-side.

**11.5.8 Error handling:** Ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system.

- a) Ensure that the application will provide meaningful error message that is helpful to the user or the support staff.
- b) Ensure that errors are detected, reported, and handled properly.
- c) Error messages shouldn't reveal much information.
- d) No debug message for errors, no debugging in application itself.
- e) Application safe mode for occurrence of unexpected instance.

**11.5.9 Application security testing:** Ensure comprehensive security testing of applications in its lifecycle. The testing may be performed either in-house or in government approved labs.

- a) Applications should be subjected to rigorous application security testing and risk assessment since the beginning of design phase.
- b) Application security testing process must be coordinated with and approved by authorized individuals in an organization.
- c) Vulnerability scans should be performed whenever there are developer changes to application code or configuration.
- d) Daily vulnerability scanning for sensitive applications.

- e) All security flaws should be prioritized, and fixed prior to the release of the application.
- f) Flaws discovered in applications that are already released must be assessed to determine whether there is a low/medium/high level of exposure due to the following factors:
  - i. The likelihood that the security flaw would be exposed.
  - ii. The impact on information security, integrity and application availability.
  - iii. The level of access that would be required to exploit the security flaw.
- g) Automated escalation workflow of resolving application security flaws.
- h) Emergency procedures for addressing security flaws must be defined and documented prior to production deployment. Methods such as limiting application use, blocking access, temporarily blocking some parts of applications must be used amongst others.

**11.5.10 Code review:** The organization must conduct code-level security reviews with professionally trained personnel for all applications along with document details of actions performed

- a) Perform source code review to identify security bugs overlooked during development stage. It may focus on input validation, information leakage, improper error handling, object reference, resource usages, and weak session management.
- b) Organization should consider reviewing the source code of the application for vulnerabilities with the help of government approved labs or organizations such as DRDO.
- c) Code review by automated code review tools.
- d) Combination of automated tool and manual skills for code review.

**11.5.11 Black-Box Testing:** Ensure specification based testing is performed, to assure that defined input will produce actual results that agree with required results documented in the application development specifications.

- a) Periodic application penetration testing must be performed.
- b) Quarterly for sensitive application.
- c) Vulnerabilities identified should be resolved on priority based on the criticality of the underlying information impacted.
- d) For sensitive applications, critical vulnerability must be resolved within 3 days of detection.

**11.5.12 Data handling:** The organization must ensure that applications handle data securely, by use of:

- a) Security measures based on classification of data.
- b) AES128 bit encryption for the classification level of secret.

- c) AES256 bit encryption for storage for the classification level of top secret.
- d) Auditing of each instance of data access.

**11.5.13 Least privileges:** User privileges and rights to use an application must be configured using the principle of least functionality with all unnecessary services or components removed or restricted.

- a) Ensure that end-user account only has the least privilege to access those functions that they are authorized, and the account has restricted access to back end database, or to run SQL or other OS commands.
- b) Restrict access to application and web server system or configuration files.

**11.5.14 Segregation of duties:** The organization must ensure that no employee handles more than one critical function and avoid execution of all security functions of an information system by a single individual. Functions such as custody of assets, record keeping, authorization, reconciliation etc. should be allocated to different individuals.

- a) The access rights shall be kept to the minimum and authorized by the application owner.
- b) Ensure that proper access control is implemented to enforce the privileges and access rights of the users.

**11.5.15 Secure Software Development Life-Cycle (SDLC) processes:** The organization must incorporate security at each level of software development lifecycle such as during development, deployment and maintenance of application etc. to limit inclusion of threats or vulnerabilities.

- a) SDLC processes such as change management, release management, test management, back log management should incorporate security.
- b) Security responsibility of SDLC roles such as change manager, release management, engineering support, platform manager must be defined.
- c) SDLC infrastructure such as development, test, build, integration and pilot environments must be segregated.
- d) Security testing must be incorporated in each stage of SDLC.

**11.5.16 Application change control:** The organizations must implement and maintain a change management process to track and monitor activity related with changes to existing software applications.

- a) Activity such as application maintenance, installation of critical changes, review of changes and post testing, responsibility of changes, documenting change requests amongst others must be documented with relevant details.
- b) Each significant change in application must be approved ISSC.

**11.5.17 Application vulnerability intelligence:** Ensure that a mechanism exists to manage the application security specific information.

- a) Sources of information
  - i. **Internal sources:** historical vulnerability trend of application, vulnerability scans and penetration testing results.
  - ii. **External sources:** vulnerability databases exploit & threat databases, vendor alerts and third party penetration testers.
- b) Diligent integration of intelligence in application threat management process.

**11.5.18 Application logs & monitoring:** Exceptions which are thrown by the application such as a warning or as a validation error should be logged for monitoring and incident management.

- a) The log generation should adhere to the standard process so that it can be integrated with monitoring and incident management mechanism.
- b) Enable web server log and transactions log.
- c) Ensure implementation of web application firewalls.
- d) Log monitoring at periodic interval.
- e) Daily log monitoring for application processing secret information.
- f) Real time monitoring for application processing top secret information.
- g) Integration of application log monitoring with SIEM solution.
- h) Application security dashboard.

## 12.0 Data security

### 12.1 Background

12.1.1 Increasing complexity of data access due to multiplicity of platforms leads to multiple leakage scenarios while data is being created, accessed and utilized.

12.1.2 Network, server systems, endpoints, applications, physical environments, and communication channels are involved in the execution of a data transaction. These elements contribute to the security posture of data.

12.1.3 Value associated with data collected by an organization is increasing phenomenally, attracting attention of adversaries and attackers.

12.1.4 Security threats are becoming more organized and targeted, reaping immense benefits out of data compromises. This has led to the increasing concentration of these threats at the data layer.

## 12.2 Relevance of domain to information security

12.2.1 Without classification of information, it will be difficult to sensitize services, processes and functions towards importance of information.

12.2.2 Secondly, it will misalign measures planned for security. Critical information may not get the desired level of protection.

12.2.3 Without labeling of information, criticality of information may not be recognized and may not invoke the corresponding actions for protection.

12.2.4 Lack of prior knowledge about potential data leakage scenarios will lead to inadequate threat mitigation measures.

12.2.5 There have been increasing instances of cyber espionage, where there have been concentrated and targeted efforts on attacking the data resulting in data breaches, which attracts a high level of media attentions. Organization should ensure that the weaknesses leading to data leakages are addressed in a timely manner.

## 12.3 Data security guidelines

**12.3.1 Information discovery, identification & classification:** The organization must continually ascertain the information being created, accessed, received, processed, stored and shared.

**Identification & classification:** Prior to determining security measures, the information to be protected needs to be identified and classified. For information classification norms, refer section 7.1

**12.3.2 Cryptography & encryption:** Ensure that proportionate encryption protection is applied to protect sensitive information.

**12.3.3 Key management:** The organization must retain control over the encryption keys while allowing efficient and effective encryption operations.

**12.3.4 Information leakage prevention:** The organization must establish procedures to protect classified information from unauthorized access or unintended disclosure, by identifying possibilities of data breach. Appropriated at a backup and data leakage prevention methodologies, to monitor and protect classified information while at rest in storage, in use at endpoint, or in transit with external communications must be implemented.

**12.3.5 Information access rights:** The organization must establish appropriate procedures to govern access rights of users to access information systems and assets; establish process for creation of identities; establish process for defining user privileges and devise mechanisms to understand how access to information is provided.

**12.3.6 Third party access:** The organizations must set up norms for third parties, which will be involved in the processing of information and seek the desired level of assurance from third-parties, for security of information available with them.

**12.3.7 Monitoring & review:** The organizations must monitor the instances of access of information. Activity logs must be enabled to help in review of information usage and handling.

**12.3.8 Breach management & corrective action:** The organizations must have proactive measures to identify, notify, remediate and manage breach of information (refer section 19).

- a) Any breach of classified information should be reported to relevant agencies such as CERT-In, NCIIPC and any such agency duly notified by the Government of India.

## 12.4 Data Security Controls

**12.4.1 Data discovery:** The organization must establish a process of discovering information that is created, received, accessed and shared.

**12.4.2 Data classification:** The organization must enforce the information classification across all processes, functions and operations.

- a) Establish easily accessible data classification guidelines, with proactive contextual help to bring data consciousness in the organization's operations.
- b) Information labeling should be strictly adhered.
- c) Integrate information identification and classification in the organization's Operational lifecycle.
- d) Automated tool for classification and labeling information.

**12.4.3 Cryptography & encryption:** The organization must use encryption techniques to protect the data and enforce confidentiality during transmission and storage. Several methods exist for encryption of files such as encryption feature on external hardware device, secret key encryption, and public key encryption.

- a) SAG (Scientific Analysis Group) approved encryption should be used for secret and top secret classification levels.

**12.4.4 Key management:** Encryption key must be managed securely and governed by a documented key management process. For sensitive networks, Cryptographic keys for the systems must be obtained from Joint Cipher Bureau (JCB).

**12.4.5 Data-at-rest:** The organization must implement appropriate capability to protect all data storage including back up files.

**12.4.6 Data-masking:** The organization must use data masking techniques while provisioning access to application interfaces and providing data for testing.

**12.4.7 Database management:** The organization must incorporate security considerations in database management and administration. Access to database management should be governed as per organizations policy.

**12.4.8 Public mail and collaboration tools:** The organization must ensure that access to public mail and collaboration tools such as instant messaging should be restricted.

**12.4.9 External media and printing devices:** The organization should prohibit use of external media such as USB memory, external HD, mobile storage where classified information is handled.

- a) The organization must enable security feature on printing devices.

**12.4.10 Preventing loss of information:** The organization must ensure that the loss of information is prevented.

**12.4.11 Backup:** The organization must ensure that backup copies should be maintained for all operational data to enable reconstruction should they be in advertently destroyed or lost.

**12.4.12 Data retention and disposal:** The organization must implement data retention and disposal policy, considering laws, regulations and guidelines regarding the storage of data:

- a) Limit data storage for the time required as per applicable policy, law or regulation etc.
- b) Deploy/ devise system to delete and purge data beyond that its storage date.
- c) Classified and personal data must be erased before any ICT asset such as media, computer system and electronic office equipment etc. are to be transferred or disposed.
- d) Standard Operating Procedure (SOP) regarding transfer and disposal of Information media should be maintained.
- e) Encryption modules / memory modules / chips having cipher related data in the embedded device, if any, should be removed and destroyed beyond recovery.

**12.4.13 Third party access:** Access to third parties systems and persons must be granted and governed by predestinated policies and procedures.

**12.4.14 Monitoring & review:** The organization must have mechanism to monitor and review access, use and share of information at the predetermined level.

**12.4.15 Breach management:** The organization must respond to security compromises, incidents and breaches in predicable and responsive manner.



## 12.5 Data security implementation guidelines

**12.5.1 Data discovery:** The organization must deploy a process and techniques for discovering data generated, received, accessed and shared.

- a) Scanning all projects, processes and functions.
- b) Scanning all applications, endpoint systems, servers and network storages.
- c) Scanning connections, emails, and collaboration tools.
- d) Deployment of data discovery tools.

**12.5.2 Data classification:** Ensure classification of data based on its level of criticality and the impact to the organization and on internal and national security of the nation, should that data be disclosed, altered or destroyed without authorization. The organization must enforce the information classification as per Section 7, across all processes, functions and operations.

- a) Implement a mechanism that helps identify the information, classify and report it.
- b) Information without any security classification should also be protected at-least on par with restricted information.
- c)

**12.5.3 Cryptography and encryption:** The organization must use encryption techniques to protect the data and enforce confidentiality during transmission and storage.

- a) For data at rest, the organization should use secure encryption methodologies such as AES (128 bits or higher).
- b) To avoid data tampering during transmission and to establish authenticity of source or origin of data, cryptographic and hashing algorithms such as SHA -2 should be applied while using digital signature. Passwords that are used for authentication or administration should be hashed or encrypted in storage.
- c) Passwords that are used for authentication or administration should be hashed or encrypted in storage.
- d) In cases where the information asset or system is reachable via web interface, web traffic must be transmitted over Secure Sockets Layer (SSL), using only strong security protocols, such as SSLv3, Transport Layer Security (TLS1.2 or higher).
- e) SAG (Scientific Analysis Group) approved encryption algorithms must be used for secret and top secret classification.

**12.5.4 Key management:** Ensure key management process is documented and includes key distribution plan which must describe circumstances under which key management components are encrypted or decrypted, their physical form such as electronic, optical disk, paper etc.

- a) Central key management function, however the execution should be distributed to ensure to avoid single point of failure.
- b) It should support multiple encryption standards.
- c) Centralize user profiles for authentication and access keys. Users must be assigned and issued credentials to provide access to encryption resources.
- d) Ensure extensive logging of operational instances of key management function Restrict access to cryptographic keys to the fewest number of custodians.
- e) Keys should be distributed securely.
- f) Periodic key changes should be implemented at the end of their crypto-period.
- g) Ensure one key management solution for field, file and database management.
- h) For sensitive networks, Cryptographic keys for the systems must be obtained from Joint Cipher Bureau (JCB).
- i) Ensure to support to third party integration should be restricted for Secret and Top Secret unless it is required.
- j) Ensure that keys must be stored securely inside cryptographic hardware and encrypted using master key etc.
- k) Proper SOP must be placed for outlining Key Management during:
  - i. Day-to-day operations
  - ii. Emergency circumstance
- l) In the event of key compromise.

**12.5.5 Data-at-rest:** The organization must:

- a) Implement segmentation to secure access paths to storage containing classified data.
- b) Enforce strict access control on the file systems of the storage devices in the storage network.
- c) Data should be protected as it is in active use as well as when it is archived to external storage devices/media by use of encrypted storage.
- d) For sensitive data, a suitable a full-disk encryption may be deployed.

**12.5.6 Data masking:** Ensure use of data masking techniques such as randomization, blurring, nulling, shuffling, substitution amongst others while provisioning access to data.

**12.5.7 Database Management:** The following must be implemented for database management.

- a) Access to database must be restricted to authorized users.
- b) Sensitive fields must be encrypted in databases.
- c) Instances of database accesses must be logged and activities of database administrator must be recorded.
- d) Database administration credentials must be protected from unauthorized access.
- e) A mechanism for real time monitoring of databases.

**12.5.8 Public mail and collaboration tools:** The following must be implemented for securing public mail and collaboration tools.

- a) Information systems containing classified information marked top secret should not be connected with the Internet.
- b) Public mail such as Gmail, yahoo etc. should strictly not be used for official purposes or official communication. Access to public mails from official systems should be prohibited, unless approved the head of the department, for limited personal use.
- c) Files and messages transferred from public mails should be monitored using capabilities such as Data Loss Prevention (DLP).
- d) Official collaboration tools such as inter office chat facility should prohibit transfer of classified files and data, using such services. Public chat applications/ web portals should be strictly prohibited on official information systems or assets.

**12.5.9 External media & printing devices:**

- a) External storage media (e.g., USB memory devices/readers, removable hard drives, SD, Compact Flash, flash drives, key drives, rewritable DVDs, and floppy disks) should not be allowed to be connected with official information systems or assets.
- b) The organization must implement appropriate detection capability and take necessary corrective action to thwart instances of unauthorized attempts to use such media.
- c) All endpoint devices allocated to users must have their USB ports disabled, unless authorized for use by head of department due to operational requirements.
- d) User authentication such as PIN, smart card, user password for printing information.

- e) The printing devices must be configured to remove spooled files and other temporary data using a secure overwrite, or device storage for data processing must be encrypted.
- f) All printing devices must be allocated a static IP address.
- g) Enable secure network protocols and services (e.g. IP sec or Secure Internet Printing Protocol (IPP)) to prevent unauthorized network interception.

**12.5.10 Preventing loss of information:** External storage media used for official purposes should be encrypted prior to use.

- a) Classified information shall not be stored in privately-owned information processing equipment, mobile devices or removable media, unless authorized by head of department. Top secret or secret information must not be processed in privately-owned computers or mobile devices in any case.
- b) External connections from information systems and assets should be restricted for information exchange and transmission.
- c) External connections from information systems and assets should be restricted & monitored for information exchange and transmission.
- d) Email exchanges should be evaluated to build visibility over what information is leaving the organization.
- e) Activity on information systems should be monitored for information exchange and transmission.
- f) Classified information meant for internal use only, should be prevented from transmission.

**12.5.11 Back up:** The backup copies should be taken at regular intervals such that recovery to the most up-to-date state is possible.

- a) Backup activities must be reviewed and tested for integrity on a periodic basis. Hash signature of the backup data must be maintained to verify the integrity of data at the time of restoration.
- b) Backup should be properly labeled as per the classification of data stored. Backup labels should also indicate the exact date and time of backup creation as well as the name/type of system from which backup has been created.
- c) Copies of backup media and records should be stored at safe and secure location where they may be recovered/ reconstructed in case of disaster at the original location.
- d) Adequate and strong encryption methodology such as AES (256 bit) must be deployed for backup of data at the operations and recovery center.
- e) Backup media disposal should be in accordance with asset destruction controls.

- f) Backup may be extracted as per daily schedule, weekly schedule, monthly schedule, quarterly schedule etc. Backup data of at least the last 5 cycles should be maintained at a minimum.

**12.5.12 Data retention & disposal:** Data erasure from storage devices must be done prior to its transfer or destruction from storage devices using secure technologies such as degaussing or overwriting disks and tapes etc. obsolete storage devices must be physically destroyed.

- a) All media must be checked to ensure secure deletion of information and data prior to transfer or destruction.
- b) The organizations must ensure that all ICT assets are securely disposed of by authorized users when they are no longer required by physically destroying the ICT assets, to ensure that no information can be retrieved.
- c) Asset transfer or destruction decisions, and the reasons for taking them, must be documented. Record of all ICT assets transferred or destroyed must be maintained with an officer of appropriate level of authority.
- d) Periodic audit should be in place to verify the storage media disposal process.
- e) Obsolete ICT equipment such as laptops, desktops and other computing devices must only be allowed outside the organizations premises post secure deletion of data.
- f) 2 years retention of data from the levels of top secret to restricted after active use. The retention period is subject to respective regulatory requirements.

**12.5.13 Third party access:** Ensure that third party access to information is restricted and governed.

- a) Block access to third party systems and persona unless it is required.
- b) Ensure the security provisions are incorporated into the contract.
- c) Ensure background verification and security clearance of external people before providing the access.
- d) Establish a mechanism for seeking assurance from third party organizations.
- e) Restrict access to public emails, writing material and mobile phone in the premises of third party accessing information.

**12.5.14 Monitoring & review:** The organization must deploy a process for monitoring use and access of information.

- a) Each instance of access to information is logged.
- b) Access of fields, files and databases is recorded and logged.
- c) Activity of data base monitored.

- d) Behavior of people and systems access data is closely tracked.
- e) Logs are reviewed frequently.
- f) Logs of reviewed on real time basis for sensitive information.
- g) Integration with SIEM solution.
- h) Dashboard of data security.

12.5.15 **Breach management:** The organization must ensure that each security, incident or breach generates desired level of attention to resolve in a timely manner.

- a) Mechanism to identify or recognize security incident.
- b) Define type of incidents and their respective severity.
- c) Escalation matrix for each type of incident.
- d) Establish remediation workflow.
- e) Automated tool and technology for incident management like SIEM.
- f) Process to notify the breaches to authorities like CERT-In, NCIIPC, etc.

## 13.0 Personnel security

### 13.1 Background

13.1.1 Insider threat has been a large contributor towards a number of security incidents faced by organizations. Additionally, the sourcing patterns of an organization are increasingly dependent on external service providers, for bridging gaps in their skills and competence, saving costs, augmenting capabilities to improve scalability and for making operations lean and efficient.

13.1.2 However, granting access to organizations information assets and systems to third-party service providers (TPSP's) increases the security risk. As employees and third parties have access to confidential information during their tenure of employment it is crucial that greater emphasis be given to securing threats originating from human resources.

13.1.3 The organization may have robust security framework; however, the third party may not have a similar framework, thus placing the information at risk of compromise or theft. The third party may become the weakest link in the security ecosystem of the organization.

## 13.2 Relevance of domain to information security

13.2.1 Personnel are owners, custodian or users of information assets and systems. Lack of data about these personnel, who may be either employees or third parties, will lead to inadequate protection of these assets and systems from a security standpoint.

13.2.2 As processes and sub processes continue to be outsourced or managed by third party personnel, it is important to keep track of information and data they have access to. All vendors, third parties, consultants etc. should be contractually liable to implement and follow security best practices for personnel security, understanding the applicable legal and regulatory compliances, assessment of the sensitivity of information and formulation of robust contractual agreements.

13.2.3 Without the knowledge over how and what employees access, it will be difficult to assess risk posed to information and IT systems by employee actions.

13.2.4 Without training and awareness, employees may not be aware of the security implications of their actions, resulting in unintentional loss.

13.2.5 Third party environment and employees may not be sensitive to the specific security requirements of the organization. If coverage of the personnel security does not extend to them, it will be difficult to get the desired level of assurance.

## 13.3 Personnel security guidelines

**13.3.1 Awareness & training:** The organization must develop an appropriate information security awareness and training program for all personnel. All adequate tools and systems to support such training programs should be made available by the organization.

**13.3.2 Employee verification:** The organization must conduct background checks or security clearance as part of its employee hiring process.

**13.3.3 Authorizing access to third parties:** The organization must develop and document a process for authorizing physical and logical access to third parties for organization owned information assets and systems.

**13.3.4 Record of authorized users:** The organization should maintain an updated record of all users granted access to each information as set and system.

**13.3.5 Acceptable usage policy:** The organization must develop an acceptable usage policy for all information assets and systems including Web and email resources provided to employees, amongst others.

**13.3.6 Monitoring and review:** The organization must implement appropriate monitoring tools and technology to track compliance of personnel with organization's policies.



**13.3.7 Limiting exposure of information:** The organizations must ensure that coverage of personnel security program limits the exposure of information to unintended recipients, parties or organizations.

## 13.4 Personnel security controls

**13.4.1 Training and Awareness:** The organization must ensure that role based training is provided to all personnel within the organization to familiarize them with their roles and responsibilities in order to support security requirements. The organization must ensure that information security awareness and training includes the following:

- a) Purpose of the training or awareness program.
- b) Reporting any suspected compromises or anomalies.
- c) Escalation matrix for reporting security incidents.
- d) Fair usage policy for organizations as sets and systems.
- e) Best practices for the security of accounts.
- f) Authorization requirements for applications, databases and data.
- g) Classifying, marking, controlling, storing and sanitizing media.
- h) Best practices and regulations governing the secure operation and authorized use of systems.

**13.4.2 Employee verification:** The organization must ensure appropriate verification such as background checks are performed for employees and personnel of TPSP(s) before providing access to classified information.

- a) The organization must conduct pre-employment verification through authorized/competent agency.

**13.4.3 Authorizing access to third parties:** The organization must identify individuals representing third party organizations such as consultants, contractors, or any other individuals who require authorized access to the organizational information and information system.

- a) Access to information and information systems by employees of external /Third Party Service Provider(s) (TPSP) should only be allowed after due verification (which should be repeated after specific intervals), and such access should occur under supervision of relevant authority.
- b) Under no circumstances shall third party vendors or partner be allowed unmonitored access to the organizations information or information systems.

**13.4.4 Acceptable use policies:** Ensure that the policies for acceptable use are established for secure usage of organization's resources such as email, internet, systems, networks, applications and files amongst others.

**13.4.5 Disciplinary processes:** Ensure that a mechanism and supporting disciplinary processes are established to resolve non-compliance issues and other variances in a timely manner.

**13.4.6 Record of authorized users:** The organization must prepare and continuously update records of access granted to all users such as employees and third party personnel.

The record management must be performed in an automated manner to ensure access authorizations granted by different functions are maintained in a central repository/system.

**13.4.7 Monitoring and review:** The organization must define processes to monitor and review access granted to personnel including temporary or emergency access to any information asset or system.

**13.4.8 Non-disclosure agreements:** The organization must incorporate considerations such as signing non-disclosure contracts and agreements in the HR process, both for employees and third parties allowed to access information assets and systems.

**13.4.9 Legal and contractual obligations:** The organization must ensure that employees and third parties are aware of legal and contractual obligations with respect to security of information.

- a) The organization must ensure that users are aware of policies, procedures and guidelines issued with respect to Information Security.

**13.4.10 Communication practices:** The organization must prohibit its employees and external parties from disseminating/ communicating classified information for any other purpose except its authorized and intended use.

- a) Information regarding security incidents must only be communicated by designated personnel.

## **13.5 Personnel security implementation guidelines**

**13.5.1 Training and awareness:** Organization must undertake the development, implementation and evaluation of role-based training for all personnel.

- a) Impart role-based training to all personnel through specially designed training courses or modules, on a regular basis.
- b) Emphasize on role of the employees towards information security while designing training courses or modules.
- c) Organization should work with an IT/cyber security subject matter expert when developing role-based training material and courses.
- d) Organization must measure effectiveness of role-based training material by means of internal evaluation of attendees.

- e) Organization must ensure that role-based training material is reviewed periodically and updated when necessary.
- f) Organization should provide an effective mechanism for feedback on role-based training security material and its presentation.
- g) Employee awareness on information security: Organization must provide information security awareness training as part of the employee induction process and at regular intervals during the employee's tenure. This must be extended to all third party employees working from the organizations facility.
- h) Awareness training program should aim to increase user understanding and sensitivity to threats, vulnerabilities.
- i) Awareness training should focus on the need to protect organization's and personal information.
- j) Awareness training must cover topics such as security procedures, security policies, and incident reporting amongst others.

**13.5.2 Employee verification:** Organization must conduct employee verification by using methods such as:

- a) Perform identity verification through authorized/competent agency.
- b) Conduct background checks of all personnel including third party personnel, prior to allowing access to classified information.
- c) Background verification check should include details such as address verification, criminal records, past experience, medical records, and family details amongst others.

**13.5.3 Authorizing access to third parties:** The organization must restrict the level of access provided to authorized individuals from third parties based on their role; function performed and associated need for access.

- a) Prior to granting physical and logical access to third party personnel, the organization must seek sufficient proof of identity of personnel from the third party employer such as recent background check and verification by competent authority.
- b) Authorization for access to third party personnel must be supported by documented request from head of department, where third party personnel will be deployed.
- c) Organization must strictly monitor all activity conducted by third party personnel.
- d) Organization must strictly monitor physical movement of third party personnel within its facility.

- e) Organization should permit authorized individuals to use an external information system to access or to process, store, or transmit organization-controlled information only post verification of the implementation of required security controls on the external system as specified in the organization's information security policy.
- f) Organization must limit the use of organization-controlled portable storage media by authorized individuals on external information systems.

**13.5.4 Acceptable use policies:** Organization must identify, document, and implement acceptable usage policy and incorporate the following:

- a) All users of information systems must take responsibility for, and accept the duty to actively protect organization's information and information systems.
- b) The acceptable usage policy must include information about usage of organization ICT resources such as computing equipment, email, optical drives, hard drives, internet, applications, printers, fax machine, storage media amongst others.
- c) Ensure all employees including third party vendors/consultants/personnel are signatory to the acceptable use policy.

**13.5.5 Disciplinary process:** Organization must establish disciplinary process to cater to instances of non-compliance to its security or acceptable usage policy.

- a) The organization must empower the security team to take disciplinary action whenever instances of non-compliance to the organization's security policy or procedures by any employee or third party personnel are encountered.

**13.5.6 Record of authorized users:** Organization must implement a centralized automated access request and authorization capability to establish clear visibility over clearance level granted to each user – including employees and third party personnel. Details about each user must be updated in a timely manner and should include:

- a) User details – personal details, contact details, role, function, status of employment.
- b) Details of background checks and verification.
- c) Details of HOD.
- d) List of authorized are as allowed to access.
- e) Registered / allocated devices and information systems.
- f) Category of classified information permitted to access.

**13.5.7 Monitoring and review:** Organization must implement monitoring mechanism to track user access activity and limit the access to explicitly allowed to Personnel by defining areas visited, time of access, activities conducted etc.

- a) The organization must periodically review the physical and logical access granted to personnel to detect instances of non-compliance.

13.5.8 Non-disclosure agreements: Organization should include signing of non-disclosure contracts and agreements in HR process during employment.

- a) Non-disclosure agreements should restrict employees and third parties from sharing organizational information publically.

13.5.9 Legal and contractual obligations: Organization must brief all personnel about their legal and contractual obligation to protect the organizations information and to follow all security advisories issued by competent authority so as to prevent disclosure of information, loss of sensitive data amongst and information compromise.

- a) The terms of employment must contain a copy of all relevant policies and guidelines.
- b) The organization must obtain a formal signoff from the employee on all such policies and guidelines such as end user policy, acceptable usage policy etc.

13.5.10 Communication practices: Organization must establish documented and implemented policies, procedures and controls to restrict personnel from unintended communication, both internally and with external entities such as media.

- a) Communication messages should be circulated to state security requirements or alert employees must be sent by designated personnel only.
- b) Only official spokesperson/ designated person from organization must be allowed to communicate with media Information / communication shared with internal or external personnel or entities must be approved by top management.

## **14.0 Threat and vulnerability management**

### **14.1 Background**

14.1.1 Organizations typically deploy security measures to guard against known threats. However, evolving threats add a different set of challenges, which require continuous vigil, monitoring and analysis. The discovery of a new vulnerability, disclosure of a new exploit or emergence of a new malware threat and the capability to incorporate protection from them on a real time basis fall under Threat and Vulnerability Management (TVM).

14.1.2 Keeping the infrastructure security posture up-to-date, scanning the infrastructure for identification of new issues or vulnerabilities that could potentially lead to a security compromise, taking corrective measures in case of a likely compromise, effectively managing infrastructure that inherently is risk prone and delivering a fast response in case of compromise are essential characteristics of the TVM function.

## 14.2 Relevance of domain to information security

14.2.1 ICT Assets (infrastructure and application) are used for creation, processing, transaction, and retention of information. These information assets are vulnerable to attacks because of issues such as configurations gaps or newer vulnerabilities with respect to the infrastructure or unpatched systems, etc.

14.2.2 Compromise of one element of ICT infrastructure may have catastrophic effect jeopardizing security of overall infrastructure and information.

14.2.3 ICT infrastructure is increasingly becoming diverse, introducing complexity of dealing with multiple entities and their independencies. This complexity makes managing threats and vulnerabilities a daunting challenge. Information that is stored, transmitted, accessed and processes by these entities will be compromised if their exposure to threats and vulnerabilities are managed effectively.

14.2.4 Threat and vulnerability information is diverse in nature reflecting diversity of infrastructure in an organization on the one hand. On the other hand, each element of ICT infrastructure is made up of components sourced from around the globe. Configuration and positioning of these elements and components also contribute to exposure to threats and vulnerabilities. Security of information may be compromised due to vulnerabilities identified in the components and elements of ICT infrastructure. Insecure configuration may lead to serious security breach.

## 14.3 Threat and vulnerability management guidelines

14.3.1 **Interdependence of systems:** The organization must create a high level map of interdependencies of ICT systems such as applications, servers, endpoints, databases, networks etc.

14.3.2 **Standardized operating environment:** The organization should attempt to achieve a standardized operating environment.

- a) The diversity in terms of hardware, application platforms, database types, operating environment and their versions must be minimized.

14.3.3 **Including TVM in change management.** The change management process for ICT infrastructure and systems should include a stringent threat assessment prior to deployment.

14.3.4 **Integration with external intelligence sources:** The organization must identify sources to gather threat and vulnerability intelligence for ICT infrastructure components including externally provisioned systems such as mobile and personally owned devices.

14.3.5 **Intelligence gathering:** The organization must develop capability correlate information about ICT infrastructure and systems.

- a) Capability to correlate logs capturing activity of users.

- b) Capability to monitor and analyze traffic.
- c) Capability to scan anomalous behaviors of applications and systems.
- d) Obtain information from other industry peers.
- e) Obtain information from security intelligence organizations.

**14.3.6 Technical policies:** The organization must define technical policies to guide configuration of ICT systems.

## **14.4 Threat and vulnerability management controls**

**14.4.1 Interdependence of systems:** Categorization of ICT systems should be based on lifecycle stages such as development, testing, staging, production and disaster recovery.

- a) Compatibility of various ICT systems must be analyzed, understood and documented

### **14.4.2 Standard operating environment:**

- a) The organization must aim to establish standard operating environments for server and endpoint systems.
- b) The organization must ensure that infrastructure is standardized and homogenous

**14.4.3 Threat assessment:** The organization must conduct periodic assessment of ICT infrastructure for identifying exposure to threats.

- a) All changes to ICT infrastructure and information systems must be made post thorough threat assessment.
- b) Changes to ICT infrastructure and information systems.

**14.4.4 Integration with external intelligence:** The organization must ensure that vulnerabilities and threat exposures are managed through appropriate agreements, obligations and service level requirements established with all vendors, TPSP(s) and partners.

**14.4.5 Vulnerabilities knowledge management:** The organization must ensure that it maintains record of vulnerabilities in existing configurations of systems by tracking and identifying vulnerabilities present in the Operating System (OS), applications, databases, network or endpoints and their impact on information leakage.

**14.4.6 Changing threat ecosystem:** The organization must evaluate all information systems continually to identify exposure to new and unknown vulnerabilities and threats.



**14.4.7 Threats emanated from third parties:** The organization must ensure that vendors, third party providers and partners adopt equivalent threat and vulnerability protection for information transacted, processed and stored on behalf of the organization.

**14.4.8 System hardening:** The organization must define standard operating procedures for system hardening.

**14.4.9 Patch management:** The organization must ensure that the security updates and patches are applied to the information systems as per schedule.

**14.4.10 Malware protection:** The organization must ensure that all information systems are protected with adequate measures to ward off threats from malware.

**14.4.11 Perimeter protection:** Ensure that perimeter security protects the organization from possible exploitation of vulnerabilities.

**14.4.12 Threat protection:** The organization must deploy appropriate capability to protect against attempts to penetrate into systems and traffic scanning.

**14.4.13 Configuration:** The organization must ensure that all the unnecessary services, ports and interfaces in systems, network equipment and endpoints are blocked.

**14.4.14 Remediation:** The organization must establish processes to ensure remediation of threats and vulnerabilities in the least possible time.

- a) Threat and vulnerability management system should integrate with ICT infrastructure management systems for triggering remediation tasks.

## **14.5 Threat and vulnerability management implementation guidelines**

### **14.5.1 Interdependence of systems:**

- a) Replacement of ICT assets with newer/upgraded version must be done keeping in view their backward and forward compatibility with existing infrastructure devices.
- b) Ensure that addition of ICT infrastructure components is made post compatibility analysis of the additional components with existing ICT infrastructure

**14.5.2 Standard operating environment:** The organization must ensure standardization of operating environment across the organization. This should include, but not limited to, the following:

- a) Operating systems.
- b) Servers and platforms.

- c) Limit diversity of endpoints.
- d) Uniform and homogenous network devices.
- e) Application platforms and installed versions.
- f) Database types should be uniform.
- g) Depending the size of the IT assets and to have standard, secure and smooth operating environment, organizations may create Network Operation Center (NOC) and Security Operations Center (SOC).

**14.5.3 Threat assessment:** The organization must identify the possible threat vectors' paths, exploitation points, tools and techniques which can compromise the security of the organization. The organization must also analyze the impact of compromise of security of a device or components to its operations:

- a) Perform vulnerability assessment to identify vulnerabilities and weaknesses as a result of specific way of configuring devices and systems; vulnerabilities and threats associated with the use of specific ports, protocols and services; vulnerabilities introduced due to changes in ICT infrastructure
- b) Vulnerabilities and threats associated with specific types of infrastructure components.
- c) Vulnerabilities associated with specific versions of infrastructure components.
- d) Whenever there is a change in ICT system, new configuration should take care of established identification, authorization and authentication policies.

**14.5.4 Integration with external intelligence:** The organization must establish a formal relationship with external entities for receiving timely notification.

- a) Relevant feeds, information about emerging threats, vulnerabilities, bugs and exploits must be obtained.
- b) Relevant sources should include a mix of different vendors, trusted third parties, product developers, open source communities, industry bodies and other relevant organizations.
- c) The organizations risk management function must incorporate inputs received from such external sources and entities.

**14.5.5 Vulnerabilities knowledge management:** The organization must document and maintain list of vulnerabilities present in installed instances of operating system, applications, databases, network device, end points.

- a) Specify the level of severity associated with each known vulnerability.
- b) Ensure availability of security capabilities to protect against all known threats and vulnerabilities.

- c) Maintain and update vulnerability information and integrate with change management process.
- d) Integrate information from external intelligence sources.

**14.5.6 Changing threat ecosystem:** The organization must evaluate all ICT systems and devices on regular basis to uncover new vulnerabilities.

- a) Conduct periodic security testing for all ICT systems and devices.
- b) Conduct ad-hoc security testing for all ICT systems and devices.

**14.5.7 Threats emanated from third parties:** The organization must ensure that all third party vendors, agencies, partners with access to the organizations information implement capability to counter emerging threats and address vulnerabilities, as per the organizations requirements.

**14.5.8 System hardening:** The organization must aim to establish standard operating environments covering hardware, software and the process of IT assets without comprising the security aspects of the IT assets. The organization must develop a standard procedure for system hardening which includes, but is not limited to the following:

- a) Developing standard hardened configuration for implementation across the organization by modification of default security controls, tailored to organizations requirements, eliminating known risks and vulnerabilities.
- b) Keeping security patches and hot fixes updated Implement encryption on all information systems.
- c) Establish hardening security policies, such as local policies relating to how often a password should be changed.
- d) Shut down unused physical interfaces on network devices.
- e) Use secure protocols when transmitting over the network.
- f) Implement access lists that allow only those protocols, ports and IP addresses that are required by network users and services, and then deny everything else.
- g) Restrict remote management connectivity to only controlled machines that are on a separate security domain with robust protection.
- h) Monitor security bulletins that are applicable to a system's operating system and applications
- i) Removal of unnecessary software.
- j) Enable system security scanning and activity and event logging mechanism.

**14.5.9 Patch management:** The organization must ensure that patch management is carried out at regular intervals or as soon as critical patches for ICT systems or software are available.

- a) Integrate patch management with operational cycle of ICT infrastructure management such as asset management, capacity management, change management, configuration management, problem management and service management
- b) The organization must regularly be in touch with vendors and service providers to ensure latest patches are installed on priority basis.

**14.5.10 Malware protection:** The organization must ensure that each information system is protected by installation of antivirus software and regular updates are made available to the same.

- a) Capabilities to protect against specific malware which attempt information theft should be available.

**14.5.11 Perimeter threat protection:** The organization must ensure perimeter threat protection of its network infrastructure through implementation of Capabilities such as a firewall.

**14.5.12 Protection from fraudulent activity:** The organization must deploy techniques for protection from fraudulent applications such as key loggers, phishing, and Identity theft and other rogue applications.

**14.5.13 Configuration of endpoints:** The organization must block all unnecessary services and system level administrator privileges through methods such as active directory, group policies on endpoint devices and systems.

**14.5.14 Remediation:** The organization must ensure that ICT systems and devices are updated with the latest security patches and virus signature to reduce the chance of being affected by, malicious code or vulnerabilities.

- a) The organization must prioritize the order of the vulnerabilities identified and treat them based on their impact and severity.
- b) The organization must pre-test the security updates and patches of the identified vulnerabilities. The organization must apply appropriate patches and perform post-test to confirm the return to desired secure state.
- c) The organization should deploy patches to the target machines and make sure that patches are only installed on machines where they are required.
- d) The organization must perform security risk assessment regularly by using capabilities such as vulnerability scanning tools (host-based or network-based) to identify patch inadequacy or potential system misconfiguration.

## 15.0 Security monitoring and incident management

### 15.1 Background

15.1.1 Organizations face significant risks of information loss through inappropriate account access and malicious transaction activity etc. which have implication such as information leakage resulting in misuse, financial loss and loss of reputation.

15.1.2 Security monitoring and incident response management is a key component of an organization's information security program as it helps build organizational capability to detect, analyze and respond appropriately to an information breach which might emanate from external or internal sources

### 15.2 Relevance of domain to information security

15.2.1 The success of a security program and the value being delivered by security initiatives lies in the organization's responsiveness to an external attack and its ability to sense and manage an internal data breach.

15.2.2 In the operating cycle of an organization, information is exchanged, processed, stored, accessed and shared. There are multiple ways through which the information may be exposed to unintended persons, it may be intentionally or unintentionally lost or external attackers may be able to steal information. This requires continuous monitoring of operations to identify likely instances of information loss.

15.2.3 Information loss instances lead to serious consequences. An organization has some window of opportunity to curb the losses and reduce the impact. This requires a predictable and responsive incident management.

15.2.4 The logs generated by information systems, servers, operating systems, security devices; networks and application systems provide useful information for detection of incidents pertaining to security of information.

15.2.5 Disruptive and destructive information security incidents demand a competent monitoring and incident management.

### 15.3 Security monitoring & incident management guidelines

15.3.1 **Incident response coverage:** The organization must develop the monitoring and incident response program such that it addresses the requirements of its extended ecosystem.

- a) The organization must ensure that the scope of security monitoring and incident management is extended to all information emerging from internal as well as external sources such as threats emerging from vendors, partner or third parties.

**15.3.2 Breach information:** The organization must build 'incident matrix', particular to its own threat environment, helping it identify possible breach scenarios that can expose or leak information whilst listing down appropriate response procedure.

- a) 14.3.2.1 The incident scenarios should be based on criticality and sensitivity of information, threat ecosystem around the organization.

**15.3.3 Security intelligence information:** The organization must establish capability to monitor and record specific information about vulnerabilities (existing and new) that could affect information, systems& assets.

**15.3.4 Enterprise log management:** The organization must ensure that logs are collected, stored, retained and analyzed for the purpose of identifying compromise or breach.

**15.3.5 Deployment of skilled resources:** The organization must deploy adequate resources and skills for investigation of information security incidents such as building competencies in digital forensics.

**15.3.6 Disciplinary action:** The organization must establish procedures in dealing with individuals involved in or being party to the incidents.

**15.3.7 Structure & responsibility:** The organizations should define and establish roles and responsibilities of all the stakeholders of incident management team, including reporting measures, escalation metrics, SLAs and their contact information.

**15.3.8 Incident management awareness and training:** The organization must conduct educational, awareness and training programs as well as establish mechanism by virtue of which users can play an active role in the discovery and reporting of information security breaches.

**15.3.9 Communication of incidents:** The organization must establish measures for effective communication of incidents along with its impact, steps taken for containment and response measures to all stakeholders including client's and regulators.

## 15.4 Security monitoring & incident management controls

**15.4.1 Security incident monitoring:** The organization must build capability to monitor activity over information assets and systems that are being used across its ecosystems.

**15.4.2 Incident management:** The organization must define an information security incident management plan which includes process elements such as incident reporting, incident identification and notification, incident metrics based on the type of incidents, procedural aspects and remediation measures, mechanisms for root cause analysis, communication procedures to internal as well as external stakeholders.

- a) The organization must deploy security measures for incident monitoring and protect the system during normal operation as well as to monitor potential security incidents. The level and extent of measures to be deployed should be commensurate with the sensitivity and criticality of the system and the information it contains or processes.

**15.4.3 Incident identification:** Ensure that a set of rules exists that helps to detect, identify, analyze and declare incidents from the information collected from different sources.

**15.4.4 Incident evaluation:** The organization must define policies and processes for logging, monitoring and auditing of all activity logs.

- a) The organization must deploy relevant forensic capability to aid in incident evaluation.

**15.4.5 Escalation process:** The organization must create and periodically update an escalation process to address different types of incidents and facilitate coordination amongst various functions and personnel during the lifecycle of the incident.

**15.4.6 Breach information:** Ensure that knowledge of incidents, and corrective action taken should be compiled in a structured manner. The organizations must record, at a minimum, the following information:

- a) The time information security incident was discovered.
- b) The time when incident occurred.
- c) A description of incident, including the information, asset & system, personnel and locations involved.
- d) Action taken, resolution imparted and corresponding update in knowledge base

**15.4.7 Configuring devices for logging:** The organization must configure the devices to generate log information required to identify security compromise or breach.

**15.4.8 Activity logging:** The organization must define a process for collection, management and retention of log information from all information sources.

- a) The scope of generating logs should be extended to all critical systems.

**15.4.9 Log information:** Logs must contain, at a minimum the following information: unauthorized update/access, starting/ending date and time of activity, user identification, sign-on and sign-off activity, connection session or terminal, file services such as file copying, search, log successful and unsuccessful log-in attempts, activities of privileged user-IDs, changes to user access rights, details of password changes, modification to software etc.

- a) The organization must ensure that time consistency is maintained between all log sources through mechanisms such as time stamping and synchronization of servers.

**15.4.10 Log information correlation:** Organization should ensure that a process is established for regular review and analysis of logs and log reports.

**15.4.11 Protecting log information:** Periodic validation of log records, especially on system / application where classified information is processed/stored, must be performed, to check for integrity and completeness of the log records.



- a) Any irregularities or system/application errors which are suspected to be triggered as a result of security breaches, shall be logged, reported and investigated.
- b) For sensitive network, all logs should be stored in encrypted form or place tamper proof mechanism for during creation/storing/processing logs.

**15.4.12 Deployment of skilled resources:** The organization must deploy personnel with requisite technical skills for timely addressing and managing incidents.

**15.4.13 Incident reporting:** The organization must ensure that a mechanism exists for employees, partners and other third parties to report incidents.

- a) Incident management should support information breach notification requirements as well as formal reporting mechanisms.
- b) Ensure that a significant level of efforts is dedicated towards spreading awareness about incident response process throughout the organization and to partners and other third parties.

**15.4.14 Sharing of log information with law enforcement agencies:** The organization must make provisions for sharing log information with law enforcement bodies in a secure manner, through a formal documented process.

**15.4.15 Communication of incidents:** The organization must ensure that timely communication is done to report the incident to relevant stakeholders such as the Information Security Steering Committee (ISSC), sectorial CERT teams and CERT- In etc.

## **15.5 Security monitoring and incident management implementation guidelines**

**15.5.1 Security incident monitoring:** The roles and responsibilities for incident management must be defined by the organization. Necessary tools and capability to enable monitoring must be made available. The following groups, entities form an essential part of the coverage of the organizations monitoring capability:

- a) Users – their roles, associations and activities over multiple systems and applications, disgruntled employee.
- b) Assets – ownerships, dependency on related applications or business processes and what information is accessed.
- c) Applications – usage of applications, transactions, access points, file systems which holds sensitive information.
- d) Networks – traffic patterns, sessions and protocol management which are used to access the information.
- e) Databases – access patterns, read & updates activity, database queries on information.

- f) Data – access and transactions on the amount of unstructured/structured data, sensitivity of data such as PII, PHI, financial Information etc.

**15.5.2 Incident management:** The organization must establish a security incident response procedure with necessary guidance on the security incident response and handling process. The procedure must be communicated to all employees, management and third party staff located at the organizations facility.

- a) Organization should establish guidelines for prioritization of information security incidents based on - criticality of information on affected resources (e.g. servers, networks, applications etc.) and potential technical effects of such incidents (e.g. denial of service, information stealing etc.) on usage and access to information.
- b) Organization should assign a category to each type of information security incident based on its sensitivity for prioritization of incidents, arranging proportionate resources, and defining SLAs for remediation services.
- c) Organization must define disciplinary action and consequences in-case employee or authorized third party personnel are responsible for breach or triggering security incident by deliberate action.
- d) Organization must define liability of third party entity in-case breach or incident originates due to deliberate action of such parties.

**15.5.3 Incident identification:** The organization must continuously monitor users, applications, access mechanisms, devices, physical perimeter, and other aspects of its operations to check for disruption in their normal functioning.

- a) Security capability should seek to detect and/or "prevent" attacks through monitoring activity.
- b) Establish processes to identify and report intruder's leveraging unauthorized access.
- c) Monitor downloading and installing activity.
- d) Monitor hosts, network traffic, logs, and access to sensitive data to identify abnormal behavior.
- e) Detect, seek establishment of unauthorized peer-to-peer networks, or intruder-operated botnet servers.
- f) The organization must develop guidelines to classify incident based on certain parameters such as identity theft, unauthorized access, and malicious code execution etc. This will aid in classification of incidents and help in identification of most frequent types of incidents.
- g) Direct all users to report suspicious activity or abnormal system performance.
- h) Conduct periodic training of all users to acquaint with incident reporting processes.

**15.5.4 Incident evaluation:** The organization must focus on developing procedures for incident evaluation such as type of incident, loss of information, access of information, IP address, time, and possible reason for incident, origin of threat etc.

- a) Obtain snapshot of the compromised system as soon as suspicious activity is detected. The snapshot of the system may include system log files such as server log, network log, firewall/router log, access log etc., information of active system login or network connection, and corresponding process status.
- b) Conduct impact assessment of the incident on data and information system involved.
- c) Segregate and isolate critical information to other media (or other systems) which are separated from the compromised system or network.
- d) Keep a record of all actions taken during this stage.
- e) Check any systems associated with the compromised system through shared network-based services or through any trust relationship.
- f) Isolate the compromised computer or system temporarily to prevent further damage to other interconnected systems, or to prevent the compromised system from being used to launch attack on other connected systems.
- g) Remove user access or login to the system.
- h) Ensure that incidents are reported in a timely manner so that the fastest possible remedial measures can be taken to reduce further damage to the IT assets.

**15.5.5 Escalation processes:** The organization must create and periodically update an escalation process to address different types of incidents and facilitate coordination amongst various functions and personnel during the lifecycle of the incident.

- a) The escalation procedure must identify and establish points of contact, at various levels of hierarchy, both within the organization and with vendors and third parties responsible for hardware/software.
- b) Maintain an updated list containing details of points of contacts from all concerned departments and functions such as technical, legal, operations and maintenance staff, supporting vendors, including the system's hardware or software vendors, application developers, and security consultants etc.
- c) Establish procedure for incident notification to be shared with the above identified personnel, based on the type and severity of impact caused by the incident, in a timely manner.
- d) Every system should have a specific escalation procedure and points of contact which meet their specific operational needs. Specific contact lists should be maintained to handle different kinds of incidents that involve different expertise or management decisions.
- e) Different persons may be notified at various stages, depending on the damage to or sensitivity of the system. Communication at each stage must be supported by details such as issue at hand, severity level, type of system under attack or

compromise, source of incident, estimated time to resolve, resources required amongst others.

**15.5.6 Breach information:** The organization must ensure adequate knowledge of incident/ breach is obtained through post incident analysis.

- a) Recommendations to thwart similar incidents in the future, possible method of attack, system vulnerabilities or exploits used amongst other information about incidents must be recorded.
- b) Details such as time of occurrence, affected devices/services, remediation etc. must also be documented.
- c) Save image of the compromised system for forensic investigation purpose and as evidence for subsequent action.

**15.5.7 Configuring devices for logging:** The organization must establish logging policies on all ICT systems and devices including security devices such as fire walls etc., by enabling sys log, event manager amongst others.

- a) The organization must capture and retain logs generated by activity on information assets and systems.
- b) The organization should subscribe to knowledge sources and correlate the information to generate intelligence out of various events and instances.

**15.5.8 Activity logging:** The organization must define a process for collection, management and retention of log information from all information sources.

- a) Logs should be securely managed in accordance to the organizations requirements and should focus on securing process for log generation, limiting access to log files, securing transfer of log information and securing logs in storage.
- b) Organization should integrate the log architecture with packaged applications or/and customized systems. There should be standardized log formats of unsupported event sources which may lead to information security incidents.
- c) Log archival, retention and disposal measures should be deployed as per the compliance requirements of the organization.

**15.5.9 Log Information:** Ensure that system logs contain information capture including all the key events, activity, transactions such as:

- a) Individual user accesses;
- b) Rejected systems, applications, file and data accesses;
- c) Attempts and other failed actions;
- d) Privileged, administrative or root accesses;
- e) Use of identification and authentication mechanisms;

- f) Remote and wireless accesses;
- g) Changes to system or application configurations;
- h) Changes to access rights;
- i) Use of system utilities;
- j) Activation or deactivation of security systems;
- k) Transfer of classified information.
- l) Deletion and modification of classified information.
- m) System crashes
- n) Unexpected large deviation on system clock.
- o) Unusual deviation from typical network traffic flows
- p) Creation or deletion of unexpected user accounts.
- q) Unusual time of usage.
- r) A suspicious last time login or usage of a user account.
- s) Unusual usage patterns (e.g. programs are being compiled in the account of a user who is not involved in programming).
- t) Computer system becomes inaccessible without explanation.
- u) Unexpected modification to file size or date, especially for system executable files.
- v) All log generation sources such as information systems and critical devices must be synchronized with a trusted time server periodically (at least once per month).

**15.5.10 Log information correlation:** The organization must schedule a periodic log review process for examination of any attempted system breaches, failed login attempts amongst others.

- a) The organization must undertake regular review of log records on systems/ applications where classified information is stored or processed to identify unauthorized access, modification of records, unauthorized use of information, system errors and security events, unauthorized execution of applications and programs, in addition to review of changes to standard configuration of systems storing or processing classified information.
- b) Appropriate capabilities must be implemented to check for modification of information ownership and permission settings.
- c) Appropriate capabilities such as intrusion detection system (IDS) or intrusion prevention system (IPS) should be implemented to analyze log information to detect Intrusion, malicious or abusive activity inside the network, verification of integrity of classified information and important files.

**15.5.11 Protecting log information:** Periodic validation of log records, especially on system/application where classified information is processed/stored, must be performed, to check for integrity and completeness of the log records.

- a) Access to system and device logs must be restricted only to ICT personnel through administrative policies and other measures.
- b) Logs must be retained for adequate period of time considering organizational, regulatory and audit requirements.
- c) Log information must be securely archived and stored in secure devices and placed under the supervision of concerned Information security personnel.
- d) Log information, beyond its intended period of retention, must be disposed as per standard data disposal policy.
- e) Log information of all administrative and privilege accounts activity must also be maintained.
- f) Log information must be protected from modification or unauthorized access.

**15.5.12 Deployment of skilled resources:** The organization must define the resources and management support needed to effectively maintain and mature an incident response capability.

- a) Individuals conducting incident analyses must have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications.
- b) The organization must train personnel in their incident response roles and responsibilities with respect to the information system.
- c) The organization should incorporate simulated events in to incident response training to facilitate effective response by personnel in crisis situations.
- d) The organization should develop competencies in cyber forensics and investigations or seek support from authorized cyber investigation agencies.

**15.5.13 Incident reporting:** The organization must ensure that appropriate procedures are followed to enable reporting of incidents both by employees and partner agencies.

- a) The reporting procedure should have clearly identified point of contact, and should have easy to comprehend steps for personnel to follow.
- b) The reporting procedure should be published to all concerned staff for their information and reference.
- c) Ensure all employees and partner agencies are familiar with the reporting procedure and are capable of reporting security incident instantly.

- d) Prepare a standardized security incident reporting form to aid in collection of information.

**15.5.14 Sharing of log information with law enforcement agencies:** The organization must make provisions to share log information with law enforcement agencies such as police on receiving formal written notice or court orders.

**15.5.15 Communication of Incidents:** The organization must ensure that apart from addressing an incident, the information about its occurrence should be shared with relevant stakeholders such as the Information Security Steering committee (ISSC), sectorial CERT teams and CERT- In, service providers and partner vendors and agencies etc.

## Guidelines for technology specific ICT deployment

### 16.0 Cloud computing

#### 16.1 Background

16.1.1 Essentially, cloud computing offers a new way of delivering traditional ICT services to an organization, by combining platforms, operating systems, storage elements, databases and other ICT equipment.

16.1.2 While, the security guidelines and controls described above will be useful for the cloud service provider, to establish a security baseline, specific guidance has also been provided. Each organization has a different level of risk appetite

#### 16.2 Cloud computing management guidelines

**16.2.1 Security considerations in contract:** The organization must define a Service Level Agreement (SLA) with the cloud service provider incorporating aspects of data confidentiality, integrity, availability and privacy.

- a) In-case any part of the cloud service is further outsourced by the contracted cloud service provider, the organization must ensure that the agreed SLA is adhered to by such vendors.

**16.2.2 Alignment of security policies:** The organization must ensure that the security policy of the cloud service provider is aligned with the organizations evaluation and assessment of information security risks.

- a) The organization must ensure that the cloud service provider classifies information and associated virtualized assets based on the information classification guidelines used by the organization.
- b) The organization must ensure that access to information over the cloud environment is restricted in accordance with its access control policy.



**16.2.3 Data security in cloud environment:** The organization must ensure that security of applications in cloud environment is equivalent to or exceeds the security implemented for application in local environment.

**16.2.4 Authentication in cloud environment:** The organization should ensure that logical access authentication is performed using appropriate capabilities basis well defined authorization parameters.

**16.2.5 Continuity of operations:** The organization must ensure that disaster recovery plan and business contingency plan is developed in consultation with the cloud service provider.

**16.2.6 Definition of roles and responsibilities:** The organization must ensure that the cloud service provider clearly defines the roles and job duties of its employees, especially if the cloud service provider provides services to multiple organizations

**16.2.7 Security monitoring:** The organization must ensure that the cloud service provider develops appropriate mechanism to monitor; report and remediate security incidents. Security monitoring in the cloud should be integrated with existing security monitoring capabilities available with the organization.

**16.2.8 Availability of logs:** The organization must ensure that logs containing information about all operational activities, access events, modification of information, security events etc. are made available by the cloud services provider.

**16.2.9 Data security:** The organization should implement appropriate data masking and encryption based on classification of data transferred to the cloud.

- a) The organization should ensure that data is protected through appropriate encryption while in transit and at rest in cloud environment.
- b) The cryptographic keys must be managed in a secure manner and be available with only the least possible number of authorized personnel.
- c) The cryptographic keys must be stored at the least possible number of locations.

### **16.3 Cloud computing implementation guidelines:**

**16.3.1 Alignment of security policies:** The organization must ensure that security policy of cloud service provider is aligned with organization's security policies and procedures.

- a) The CSP must share updated process documentation, configuration standards, training records, incident response plans, etc. with the organization.
- b) Compliance certificates and reports should be requested from cloud service providers for verification of security practices of the cloud service provider.

**16.3.2 Data security in cloud environment:** The organization must conduct a comprehensive security assessment on applications in the cloud environment prior to production from the same.

- a) All changes in the form of upgrades, patches or enhancements must be followed by comprehensive security assessment, prior to live deployment.

**16.3.3 Authentication in cloud environment:** The organization must ensure that authentication and authorization on logical access control is clearly defined, such as who should be granted with the rights to access the data, what their access rights are, and under what conditions these access rights are provided.

**16.3.4 Security Monitoring:** The organization must ensure that cloud service provider performs security monitoring of the cloud environment on a continuous basis.

**16.3.5 Availability of logs:** The organization must define the type of activity and event logs that the CSP must provide. The organization must ensure that CSP continuously logs information about all maintenance activity, user and administrative access, critical system changes amongst others. CSP must also provide such logs to the organization as and when requested.

**16.4 Data security in cloud:** Classified data should be protected through encryption both at rest and in transit in a cloud environment. The cryptographic keys should be managed and protected securely.

**16.5 Use of authorized cloud services:** The organization must ensure that it procures services from authorized service providers such as those recognized by the Government of India.

## 17.0 Mobility & BYOD

DGAQA does not provide any Mobility and BYOD.

## 18.0 Virtualization

DGAQA does not provide any virtualization.

## 19.0 Social media

### 19.1 Background

19.1.1 Social media and networks offer users the opportunity to participate in discussions, create and follow blogs, share multimedia files etc.

19.1.2 However, such information on social media or social networks is often a source of compromise of sensitive information which may be detrimental to the Internal or national security of India.

19.1.3 Social media is often used by personnel to discuss professional issues or share information about their organization, nature of work, deployment etc. This not only leads to unnecessary disclosure of sensitive information but also exposes vital and strategic information.

19.1.4 Cyber-criminals use advanced techniques to gather intelligence from such public forums and communities. Such information enables them to mount cyber attacks by impersonation, spoofing or other social engineering attacks.

19.1.5 Additionally, attacks from malware, viruses or malicious script are easily spread across social media or social networks and similar applications

## 19.2 Social media management guidelines

**19.2.1 Limit exposure of official information:** All personnel including employees, contractual staff, consultants, partners, third party staff etc., who manage, operate or support information systems, facilities, communications networks and information created, accessed, stored and processed by or on behalf of the Government of India;

- a) Must be prohibited from accessing social media on all official devices, including personal devices with access to official information.
- b) Must be contractually bound against disclosure of official information on social media or social networking portals or applications.
- c) Must undergo mandatory training to educate them on perils and threats in the virtual world such as phishing emails, suspicious code in page etc. and for following best practices for practicing safe online behavior

**19.2.2 Permitted official use:** Only the designated function authorized to communicate unclassified information on public forums may be permitted the use of social media or social networking portals and applications.

## 19.3 Social media implementation guidelines

**19.3.1 Limit exposure of official information:** The organization must use methods to restrict access to social media websites in the organization environment and on organization's devices such as by enforcing policies through administrative directory, group policy tools etc.

**19.3.2 Permitted official use:** The organization must permit only authorized personnel in public communication function or similar in the organization to use social media through policy enforcement in administrative directory, group policy etc.

## 20.0 Open source technology

### 20.1 Background

20.1.1 Open source technology is available as source code under a license agreement. It imposes very few restrictions on the use, modification and redistribution of the source code. Using open standards can support greater interoperability between systems and devices.

20.1.2 The use of open source technology is particularly widespread in areas such as network infrastructure, computer servers, information security, Internet and intranet applications and network communications.

20.1.3 Open source technology rarely involves any up-front purchase costs and provides more flexibility compared with commercial software contractual agreements.

### 20.2 Open source technology management guidelines

20.2.1 **Integration:** The organization must ensure that open source technology selections are suitable for integration with existing infrastructure.

20.2.2 **Licensing:** Organization must ensure that open source technology has minimum licensing and binding requirements.

20.2.3 **Security testing:** Organization must conduct independent security review of open source technology in addition to gathering information about security of such technology from subject matter experts etc.

20.2.4 **Installation:** Organization must make sure that open source technology to be procured contains clearly defined and easy to understand installation procedure.

20.2.5 **Additional requirements:** The organization must ensure that additional system components required for procurement of open source technology are adequately handled.

20.2.6 **Availability of support:** Organization must ensure that Service-Provider providing open source technology is contractually bound to provide lifetime support towards patching and up-gradation of the technology.

### 20.3 Open source technology implementation guidelines

20.3.1 **Integration:** Organization should consider various factors which make open source technology suitable for integration with existing infrastructure such as operating system, processing power, storage space, connectivity, interoperability with other technologies amongst others.

**20.3.2 Licensing:** Organization should ensure that licensing agreements have minimum binding nature such as on the use of technology, time duration of use, number of systems allowed for use, permitted modifications amongst others.

**20.3.3 Installation:** Organization should ensure open source technology has clearly defined installation process which is understandable to ICT personnel.

**20.3.4 Additional requirements:** Organization should ensure that additional requirements of open source technology are adequately obtained such as system components, libraries or modules amongst others.

**20.3.5 Expertise:** Organization must ensure that it has expertise to handle installation, migration, maintenance, changes etc. in the open source technology either in-house or through external parties.

**20.3.6 Availability of support:**

- a) The organization must ensure that adequate support in the form of upgrades, patches etc. is part of contractual obligation of vendor providing open source technology.
- b) Organization should make sure of relevant support mechanism in case of any problems with the open source technology while in use such as availability of helpdesk, troubleshooting and bug-fix services amongst others.
- c) Organization should ensure that open source technology receives regular patching of newly introduced vulnerabilities.
- d) Organization should also ensure that open source technology receives relevant up-gradation to it from the vendor at regular intervals.

## Guidelines for essential security practices

### 21.0 Security testing

#### 21.1 Background

21.1.1 Security testing is the process of determining how effectively an entity being assessed meets specific security objectives. The process is intended to reveal flaws in the security mechanisms of an information system that protects data and maintain functionality as intended. Organizations conduct focused security testing with vulnerability assessment to discover and identify security vulnerabilities followed by penetration testing to simulate an attack by a malicious party and involves exploitation of found vulnerabilities to gain further access,

21.1.2 Security testing uncovers the current state of security in the organization to safeguard three main objectives of confidentiality, availability and integrity. It helps organizations to strengthen the security by mitigating and addressing all the vulnerabilities and weaknesses found as a result of the exercise. This further enhances organization's defenses against the exploitation of vulnerabilities by the attackers.

21.1.3 In the absence of appropriate security testing, present vulnerabilities may go unaddressed and exploitation by attackers may incur huge reputational and financial losses to the organization.

## 21.2 Security testing management guidelines

21.2.1 **Security evaluation:** Organization should deploy appropriate capabilities to evaluate all systems, applications, networks, policies, procedures and technology platforms such as cloud computing, mobility platforms, virtual environments etc. to identify vulnerabilities.

21.2.2 **Testing scenarios:** Organization should perform security evaluation by constructing scenarios combining internal and external threat agents.

21.2.3 **Overt and covert testing:** Organizations should perform both white hat and black hat testing to examine damage or estimate impact by an adversary.

21.2.4 **Vulnerability existence:** Organization should deploy appropriate techniques which corroborate the existence of vulnerabilities.

## 21.3 Security testing implementation guidelines

21.3.1 **Security evaluation:** The organization must ensure that relevant capabilities, tools and techniques are deployed for security evaluation such as use of network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security examination.

- a) **Security compliance evaluation:** Organization should deploy appropriate capabilities to evaluate all systems, applications, networks etc. and technology platforms such as cloud computing, mobility platforms, virtual environments etc. to check for compliance with security policies.

### 21.3.2 Testing Scenarios:

- a) **Internal testing:** The organization must conduct internal security testing assuming the identity of a trusted insider or an attacker who has penetrated the perimeter defenses.
- b) **External testing:** The organization must conduct external security testing from outside the organization's security perimeter with techniques such as reconnaissance, enumeration.

### 21.3.3 Overt and covert testing:

- a) **Black hat testing:** The organization must conduct black hat testing assuming an approach followed by an adversary, by performing testing without the knowledge of the organization's IT staff but with the full knowledge and permission of CISO/Senior management.
- b) **White hat testing:** The organization must perform white hat testing with the knowledge and consent of the organization's IT staff

**21.3.4 Vulnerability existence:** Security testing and assessment tools should be used to corroborate the existence of vulnerabilities which includes a list of products & affected version, technical details, typical consequences of exploitation, current exploitation status and overall measure of severity etc.

## 22.0 Security Auditing

### 22.1 Background

22.1.1 The ability of an organizations security architecture to provide assurance over its security coverage is important in order understand effectiveness of measures and capabilities implemented to counter threats and risks which may jeopardize the operations of an organization.

22.1.2 Security auditing is essential to test the effectiveness of design, implementation and operation of security counter measures and adherence to compliance requirements.

22.1.3 Security auditing is primarily conducted with the intent of checking conformance with established policies, procedures, standards guidelines and controls. It involves review of operational, technical, administrative, managerial controls implemented for information security.

22.1.4 Recommendations and corrective actions are derived out of security audits to improve the implementation of controls and reduce security risks to an acceptable level.

22.1.5 Security auditing is an on-going task and presents the overall state of existing protection at a given point in time and reveals status of implementation compared with defined security policies.

### 22.2 Security audit management guidelines

**22.2.1 Determine security auditing requirements:** The organization should define enterprise-wide mechanism to identify requirements and considerations for conducting security audits and scope definition. Parameters, such as the ones listed below, should be used by the organization to define scope of audits:



- a) Nature of operations, risk appetite of organization, criticality of processes and operational transactions.
- b) Exposure of organizations information to security threats
- c) Enterprise security policy, strategy and standards
- d) Legal and compliance requirements
- e) Historical information: previous audit reports, security incidents

**22.2.2 Periodicity and nature of audits:** The organization should conduct periodic audits of all information systems, infrastructure, facilities, and third parties etc. which handle classified information at any instance in its life cycle.

- a) Define nature of audit — internal/external, ongoing/project based, enterprise wide/limited to individual area.
- b) Define need for audit—compliance specific(NISPG, ISO standard, PCI- DSS etc.), security certification specific
- c) Allocate audit related tasks to dedicated and independent audit execution team—such as internal team, third-party audit etc.
- d) Define security audit types, schedule & timeline of audits, resource requirement audit —internal stakeholders and external partners efforts required
- e) Establish audit and assurance processes, and tactical mechanisms or tools to conduct the same.

**22.2.3 Audit management function:** The organization should formulate a dedicated audit management function.

- a) Roles& responsibilities of the function should be clearly defined
- b) Identification of resources required for security audit such as automated tools, manpower, down time etc.

**22.2.4 Evidence and artifacts:** The organization must define processes to manage audit sources or artifacts or evidences, such as below, in a secure manner.

- a) Policy documents
- b) Design/architecture
- c) Flow diagrams
- d) System documents
- e) Process documents
- f) Standards and procedures
- g) Operational guidelines

h) Systems reports

i) Test reports

**22.2.5 Management reporting and actions:** The organization must devise processes which ensure that all audit observations, issues and recommendations by the audit teams are reported to the head of respective department for necessary action and review.

## 22.3 Security audit implementation guidelines

**22.3.1 Determine security auditing requirements:** The organization must hold meetings with all stakeholders or heads of the department to chalk out the requirements for security audits such as:

- a) Examine the effectiveness of the existing policy, standards, guidelines and procedures.
- b) Compensating measures for existing vulnerabilities.
- c) Risks associated with category of classified information

**22.3.2 Periodicity and nature of audits:** Security audits must be conducted periodically to ensure compliance with security policy, guidelines, and procedures, and to determine the minimum set of controls required to address an organization's security. At a minimum security audit should be performed:

- a) Prior to implementation or installation or major enhancements in the organization.
- b) Periodically such as quarterly either manually or automatically using tools.
- c) Randomly between planned cycles of quarterly audit to reflect actual practice.

**22.3.3 Audit management function:** A dedicated management function must be formulated by organization to conduct security audits and associated tasks such as.

- a) Compiling audit requirements.
- b) Defining audit types.
- c) Identifying audit engagements.
- d) Planning and arranging audits.
- e) Overseeing audit execution.
- f) Managing engagement performance.
- g) Managing audit results.
- h) Reporting to the management.

**22.3.4 Evidence and artifacts:** The organization must define how much and what type of information should be captured, during each audit cycle.

- a) Organization should filter, store, access and review the audit data and logs such as log files including system start up and shut down information, logon and logout attempts, command execution, access violations amongst others; reports such as audit trails, summaries, statistics amongst others; storage media such as optical disks, USBs etc.

**22.3.5 Management reporting and actions:** Personnel associated with security audit should analyze auditing results to reflect current security status, severity level of the vulnerabilities or anomalies present after removing false-positives and report it to the concerned departments of the organization for remediation. The results of all security audits must be shared with the ISSC and senior management.

- a) Recommendations and corrective actions for improvements.

## 23.0 Annexure

### Annexure 1–References

#### 1A-List of government advisories on information security

S. No.	Name / Title	Issued by	Details
1	Manual of departmental security instructions	Ministry of Home Affairs	1994
2	Cyber Security Policy for Government of India	National Informatics Centre	V2.0, 30 <sup>th</sup> August, 2010
3	IT security policy	CERT- In	
4	Cyber security policy & procedures	Inter-Ministerial Task Force on Assessment of Indian Cyber Defence Strategies & Preparedness	V0.1, Draft under circulation
5	Guidelines for Protection of National Critical Information Infrastructure	National Technical Research Organization	V 1.0, June 2013
6	Information systems security guidelines for the banking and Financial sector	Reserve Bank of India	
7	Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism	CERT-In { Indian Computer Emergency Response Team }	March2012
8	National Cyber Security Policy	DeitY { Department of Electronics and Information Technology }	July2013
9	Computer Security Guidelines	IB { Intelligence Bureau }	2006
10	Guidelines for Sensitivity Assurance of Imported Equipment	Ministry of Science & Technology	

#### 1B – List of information security frameworks

S. No.	Name / Title	Issued by	Details
1	ISO27001:2005	International Organization for Standardization (ISO)	2005
2	ISO27001:2013	International Organization for Standardization (ISO)	2013
3	DSCI Security Framework	Data Security Council of India (DSCI)	2010
4	Common Security Framework (CSF)	Health Information Trust Alliance (HITRUST)	2012

5	COBIT5	Information Systems Audit and Control Association (ISACA)	2012
---	--------	---	------

## Annexure 2– Guidelines and controls mentioned in “Cyber Security Policy for Government of India” ver 2.0 released 30th August, 2010.

Note: The guidelines and controls mentioned in this policy document are bifurcated as per operational areas and contain general guidance spread across multiple domains.

S. No.	Areas	Guidelines and Controls
1.	Acceptable use of client systems	Virus and malicious code H/W, OS & Application software Email use Password security Portable storage media Network access policy Client system logs
2.	Security for system administrator	
3.	Security policy for network connected to Internet	Network access Client antivirus Gateway antivirus Network hardening Network Architecture Security Administration Monitoring & reporting Incident handling Security Audit Policy review Policy enforcement
4.	Security policy for department	Portable storage media Network access policy applicable for users Applications Audit trail and event log Security audit
5.	Application security guidelines	General guidelines Web application vulnerabilities Cross site scripting Malicious file execution Insecure direct object reference Cross site request forgery Information leakage and improper error handling Broken authentication and session management Insecure cryptographic storage Insecure communication Failure to restrict URL access
6.	Asset management guidelines	Asset management Nomenclature for asset ID Organization Location of bhawan Type of asset

		Sub type
		Numeric value
		Review and updation
7.	Client system security guidelines	
8.	Network device security guidelines	General
		Firewall guidelines
		Intrusion Prevention System (IPS) guidelines
		Switch configuration
		Router configuration
		Operating system up- gradation
		SNMP protocol
		Banner message
		Backup
		Log maintenance
9.	Password management guidelines	General
		Password complexity
		Password reset
		Password change
		Account lockout
		Password storage
10.	Security guidelines for user	Unattended client systems
		Internet usage
		Email usage
		Portable storage media
		Additional security measure for laptops
11.	Security policy dissemination guidelines	
12.	Time synchronization guidelines	
13.	Wireless network security guidelines	
14.	Change management process	
15.	Security incident management process	

## Annexure 2 –ISO 27001 list of controls

### A. ISO 27001: 2013

S. No.	Primary Security Domain	ISO 27001 Requirement (Reference)
1.	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.(A.5.1.1)
2.	Review of the information security policy	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.(A.5.1.2)
	<b>A.6.1 Internal organization</b>	
3.	Information security Roles and responsibilities	All information security responsibilities shall be defined and allocated. (A.6.1.1)
4.	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or

		unintentional modification or misuse of the organization's assets.(A.6.1.2)
5.	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.(A.6.1.3)
6.	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained. (A.6.1.4)
7.	Information security In project management	Information security shall be addressed in project management, regardless of the type of the project.(A.6.1.5)
	<b>A6.2 Mobile devices and teleworking</b>	
8	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.(A.6.2.1)
9	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.(A.6.2.2)
	<b>A.7.1 Prior to employment</b>	
10	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.(A.7.1.1)
11	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.(A.7.1.2)
	<b>A.7.2 During employment</b>	
12	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.(A.7.2.1)
13	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.(A.7.2.2)
14	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. (A.7.2.3)
	<b>A.7.3 Termination and change of employment</b>	
15	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.(A.7.3.1)
	<b>A.8.1 Responsibility for assets</b>	
16	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.(A.8.1.1)
17	Ownership of assets	Assets maintained in the inventory shall be owned.(A.8.1.2)
18	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.(A.8.1.3)
19	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contractor agreement.(A.8.1.4)
	<b>A.8.2 Information classification</b>	
20	Classification of information	Information shall be classified in terms of legal



		requirements, value, criticality and sensitivity to unauthorized disclosure or modification.(A.8.2.1)
21	Labelling of information	An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.(A.8.2.2)
22	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.(A.8.2.3)
	<b>A.8.3 Media handling</b>	
23	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. (A.8.3.1)
24	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.(A.8.3.2)
25	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.(A.8.3.3)
	<b>A.9.1 Business requirements of access control</b>	
26	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.(A.9.1.1)
27	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.(A.9.1.2)
	<b>A.9.2 User access management</b>	
28	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.(A.9.2.1)
29	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.(A.9.2.2)
30	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.(A.9.2.3)
31	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.(A.9.2.4)
32	Review of user access rights	Asset owners shall review users' access rights at regular intervals. (A.9.2.5)
33	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change. (A.9.2.6)
	<b>A.9.3 User responsibilities</b>	
34	Use of secret authentication information	Users shall be required to follow the organization's practices in the Use of secret authentication information.(A.9.3.1)
	<b>A.9.4 System and application access control</b>	
35	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.(A.9.4.1)
36	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.(A.9.4.2)
37	Password management	Password management systems shall be interactive and shall ensure quality passwords. (A.9.4.3)

	system	
38	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.(A.9.4.4)
39	Access control to program source code	Access to program source code shall be restricted.(A.9.4.5)
	<b>A.10.1 Cryptographic controls</b>	
40	Policy on the use of Cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.(A.10.1.1)
41	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole life cycle.(A.10.1.2)
	<b>A.11.1 Secure Areas</b>	
42	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.(A.11.1.1)
43	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.(A.11.1.2)
44	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied. (A.11.1.3)
45	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.(A.11.1.4)
46	Working in secure areas	Procedures for working in secure areas shall be designed and applied.(A.11.1.5)
47	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.(A.11.1.6)
	<b>A.11.2 Equipment</b>	
48	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. (A.11.2.1)
49	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.(A.11.2.2)
50	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage. (A.11.2.3)
51	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity. (A.11.2.4)
52	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization. (A.11.2.5)
53	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.(A.11.2.6)
54	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.(A.11.2.7)
55	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.(A.11.2.8)
56	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.(A.11.2.9)
	<b>A.12.1 Operational procedures and responsibilities</b>	
57	Documented operating	Operating procedures shall be documented and made

	procedures	available to all users who need them. (A.12.1.1)
58	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled. (A.12.1.2)
59	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.(A.12.1.3)
60	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.(A.12.1.4)
	<b>A.12.2 Protection from malware</b>	
61	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.(A.12.2.1)
	<b>A.12.3 Backup</b>	
62	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed back up policy.(A.12.3.1)
	<b>A.12.4 Logging and monitoring</b>	
63	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.(A.12.4.1)
64	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access. (A.12.4.2)
65	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.(A.12.4.3)
66	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source. (A.12.4.4)
	<b>A.12.5 Control of operational software</b>	
67	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems. (A.12.5.1)
	<b>A.12.6 Technical vulnerability management</b>	
68	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.(A.12.6.1)
69	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.(A.12.6.2)
	<b>A.12.7 Information systems audit considerations</b>	
70	Information systems audit controls	Audit requirements and activities involving verification of Operational systems shall be carefully planned and agreed to minimize disruptions to business processes.(A.12.7.1)
	<b>A.13.1 Network security management</b>	
71	Network controls	Networks shall be managed and controlled to protect information in systems and applications.(A.13.1.1)
72	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or out sourced.(A.13.1.2)
73	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.(A.13.1.3)
	<b>A.13.2 Information transfer</b>	
74	Information transfer policies	Formal transfer policies, procedures and controls shall be in

	and procedures	place to protect the transfer of information through the use of all types of communication facilities.(A.13.2.1)
75	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.(A.13.2.2)
76	Electronic messaging	Information involved in electronic messaging shall be appropriately protected. (A.13.2.3)
77	Confidentiality or non disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented. (A.13.2.4)
<b>A.14.1 Security requirements of information systems</b>		
78	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.(A.14.1.1)
79	Securing application Services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.(A.14.1.2)
80	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.(A.14.1.3)
<b>A.14.2 Security in development and support processes</b>		
81	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.(A.14.2.1)
82	System change control procedures	Changes to systems with in the development life cycle shall be controlled by the use of formal change control procedures. (A.14.2.2)
83	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. (A.14.2.3)
84	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.(A.14.2.4)
85	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.(A.14.2.5)
86	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.(A.14.2.6)
87	Outsourced development	The organization shall supervise and monitor the activity of out sourced system development. (A.14.2.7)
88	System security testing	Testing of security functionality shall be carried out during development.(A.14.2.8)
89	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.(A.14.2.9)
<b>A.14.3 Test Data</b>		
90	Protection of test data	Test data shall be selected carefully, protected and controlled. (A.14.3.1)
<b>A.15.1 Information security in supplier relationships</b>		
91	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.(A.15.1.1)
92	Addressing security Within	All relevant information security requirements shall be

	supplier agreements	established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.(A.15.1.2)
93	Information and communication Technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.(A.15.1.3)
	<b>A.15.2 Supplier service delivery management</b>	
94	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.(A.15.2.1)
95	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.(A.15.2.2)
	<b>A.16.1 Management of information security incidents and improvements</b>	
96	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.(A.16.1.1)
97	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.(A.16.1.2)
98	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.(A.16.1.3)
99	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.(A.16.1.4)
100	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures. (A.16.1.5)
101	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. (A.16.1.6)
102	Collection of evidence	The organizations shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.(A.16.1.7)
	<b>A.17.1 Information security continuity</b>	
103	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.(A.17.1.1)
104	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.(A.17.1.2)
105	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented Information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.(A.17.1.3)
	<b>A.17.2 Redundancies</b>	
106	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. (A.17.2.1)
	<b>A.18.1 Compliance with legal and contractual requirements</b>	
107	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information

		system and the organization.(A.18.1.1)
108	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.(A.18.1.2)
109	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.(A.18.1.3)
110	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.(A.18.1.4)
111	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.(A.18.1.5)
<b>A.18.2 Information security reviews</b>		
112	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.(A.18.2.1)
113	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. (A.18.2.2)
114	Technical compliance review	Information systems shall be regularly reviewed for compliance With the organization's information security policies and standards. (A.18.2.3)

### Annexure 3 Glossary

S. No.	Primary Security Domain	ISO 27001 Requirement (Reference)
1.	Access Control Mechanism	Security safeguards i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.
2.	Access Type	Privilege to perform action on an object. Read, write, execute, append, modify, delete, and create are examples of access types.
3.	Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
4.	Administrative Account	A user account with full privileges on a computer
5.	Advance Persistent	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve



	Threat (APT)	its objectives by using multiple attack vectors e.g., cyber, physical, and deception. These objectives typically include establishing and extending foot holds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: i) pursue its objectives repeatedly over an extended period of time; ii) adapts to defenders' efforts to resist it; and iii) is determined to maintain the level of interaction needed to execute its objectives.
6.	AES	Advanced Encryption Standard, is a symmetric block data encryption technique.
7.	AP	A wireless Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.
8.	Application	A software program hosted by an information system; Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.
9.	Attribute-Based Access Control	Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.
10.	Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
11.	Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
12.	Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
13.	Back Door	Typically unauthorized hidden software or hardware mechanism used to circumvent security controls.
14.	Base line Security	The minimum security controls required for safe guarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.
15.	BCP	Business continuity planning identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity.
16.	Black Box Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.
17.	Botnets	Collection of computers that are infected with small bits of code (bots) that allows a remote computer to control some or all of the functions of the infected machines. The bot-master who controls the infected computers has the ability to manipulate them individually, or collectively as bot armies that act in concert. Botnets are typically used for disreputable purposes, such as Denial of Service attacks, click fraud, and spam.
18.	Boundary Protection Device	A device with appropriate mechanisms that: i) facilitates the adjudication of different inter connected system security policies e.g., controlling the flow of information into or out of an inter connected system); and/or ii) provides information system boundary protection.
19.	BS25999	BS25999 is the British Standards Institution (or BSI) standards for business continuity management.
20.	Buffer overflow	The result of a programming flaw. Some computer programs expect input from the user for example; a Web page form might accept phone numbers from prospective customers). The program allows some virtual memory for accepting the expected input. If the programmer did not write his program to discard extra input e.g., if instead of a



		phone number, someone submitted one thousand characters), the input can overflow the amount of memory allocated for it, and break in to the portion of memory where code is executed. A skillful hacker can exploit this flaw to make someone's computer execute the hacker's code. Used interchangeably with the term, "buffer overruns."
21.	CMF	A content management framework (CMF) is a system that facilitates the use of reusable components or customized software for managing web content. It shares aspects of a web application framework and a content management system (CMS).
22.	CMS	A content management system (CMS) is an interface that allows users to publish content directly to the Web. The process of adding content pages directly to the Web is one step ahead of creating and uploading pages from a local machine because it allows a large number of people to add and share the data remotely.
23.	COBIT	Control Objectives for Information and Related Technology is a framework created by ISACA for information technology management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
24.	Code	System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.
25.	Code Review	Code review is systematic examination of computer source code. It is intended to find and fix mistakes overlooked in the initial development phase, improving both the overall quality of software and the developers' skills.
26.	Common Control	A security control that is inherited by one or more organizational information systems.
27.	Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
28.	Configuration Control	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
29.	Criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.
30.	Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
31.	Cyber Incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing there in.
32.	Cyber Infrastructure	Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services e.g., managed security services) are part of cyber infrastructure.
33.	Cyber Security	The ability to protect or defend the use of cyber space from cyber-attacks.
34.	DAST	Dynamic application security testing (DAST) technologies are designed to detect conditions indicative of security vulnerability in an

		application in its running state.
35.	Data Security	Protection of data from unauthorized accidental or intentional modification, destruction, or disclosure.
36.	DB Security	Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability.
37.	Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
38.	Denial of service attacks/ distributed denial-of- service(DDoS)	A type of attack aimed at making the targeted system or network unusable, often by monopolizing system resources. A distributed denial of service (DDoS) involves any computer systems, possibly hundreds, all sending traffic to a few choice targets. The term "Denial of Service" is also used imprecisely to refer to any outwardly-induced condition that renders a computer unusable, thus "denying service" to its rightful user.
39.	DHCP	The Dynamic Host Configuration Protocol is a standardized network protocol that is used by network devices to configure the IP settings of another device, such as a computer, laptop or tablet.
40.	DLP	Data loss/leak prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
41.	DMZ	Demilitarized zone is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network.
42.	DR	Disaster recovery (DR) the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning in the midst of disruptive events.
43.	DRM	Digital rights management (DRM) is a systematic approach to copyright protection for digital media. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they've purchased.
44.	DSF	DSCI Security Framework is comprised of 16 disciplines that are organized in four layers. DSF brings a fresh outlook to the security initiatives of an organization by focusing on each individual discipline of security.
45.	Encryption	Conversion of plain text to cipher text through the use of a cryptographic algorithm.
46.	End-to-End Security	Safe guarding information in an information system from point of origin to point of destination.
47.	External network	Any network that can connect to yours, with which you have neither a trusted or semi-trusted relationship. For example, a company's employees would typically be trusted on your network, a primary vendor's network might be semi-trusted, but the public Internet would be untrusted — hence, External.
48.	Firewall	A gateway that limits access between networks in accordance with local security policy.
49.	Hashing	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.
50.	HTTP	Hyper Text Transfer Protocol is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and

		transmitted, and what actions Web servers and browsers should take in response to various commands.
51.	IAM	An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.
52.	ICT Personnel	An information and communication technology personnel is responsible for the development, management and support of the infrastructure at an organization.
53.	Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
54.	IDS	Intrusion Detection systems - A class of networking products devoted to detecting attacks from hackers. Network-based intrusion detection systems examine the traffic on a network for signs of unauthorized access or attacks in progress, while host-based systems look at processes running on a local machine for activity an administrator has defined as "bad."
55.	IEEE	The Institute of Electrical and Electronics Engineers is dedicated to advancing technological innovation and excellence
56.	Information Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity; 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and 3) availability, which means ensuring timely and reliable access to and use of information.
57.	Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
58.	Information Security Life Cycle	The phases through which an information system passes, typically characterized as initiation, development, operation, and termination i.e., sanitization, disposal and/or destruction).
59.	Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
60.	Information Security Risk	The risk to organizational operations including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
61.	Information Type	A specific category of information e.g., secret, confidential, proprietary, investigative, public, contractor sensitive, security management) etc. defined by an organization.
62.	Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
63.	Intrusion	Unauthorized act of bypassing the security mechanisms of a system.
64.	IP	Internet Protocol is the principal communications protocol in the Internet protocol suite for relaying data-grams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.
65.	IPS	Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances that

		monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it
66.	IP sec	IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks
67.	ISO 27001	It is an information security management system (ISMS) standard published by the International Organization for Standardization (ISO). ISO/IEC 27001:2005 formally specifies a management system that is intended to bring information security under explicit management control.
68.	ISO27005	The purpose of ISO 27005 is to provide guidelines for information security risk management. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
69.	MAC	Media Access Control address is a hardware address that uniquely identifies each node of a network.
70.	Malicious agents	A person of malicious intent who researches, develops, and uses techniques to defeat security measures and invade computer networks.
71.	Management Security Controls	The security controls i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security.
72.	NAC	Network Access Control is an approach to computer network security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement
73.	Need-to-Know	A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know' and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.
74.	Network Hardening	Hardening is usually the process of securing a system by reducing its surface of vulnerability. A system has a larger vulnerability surface, the more that it does; in principle a single-function system is more secure than a multipurpose one. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.
75.	NIST800	The NIST 800 Series is a set of documents that describe United States federal government computer security policies, procedures and guidelines.
76.	NIST800-53	NIST 800-53 is a publication that recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security.
77.	OCATVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation are a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.
78.	OSSTMM	The Open Source Security Testing Methodology Manual (OSSTMM) was released by Pete Herzog and is distributed by the Institute for Security and Open Methodologies (ISECOM). This document is concentrated on improving the quality of enterprise security as well as the methodology and strategy of testers.
79.	OTP	One-time password is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords.
80.	OWASP	The Open Web Application Security Project is an open-source web application security project. The OWASP community includes corporations, educational organizations, and individuals from around

		the world.
81.	Password	A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.
82.	Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
83.	PCI-DSS	The Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure.
84.	Penetration Testing	Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.
85.	Privilege Management	The definition and management of policies and processes that define the ways in which the user is provided access rights to enterprise systems. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information in directories.
86.	Protocol	Set of rules and formats, semantic and syntactic, permitting information systems to exchange information
87.	Remote Access	The ability for an organization's users to access its non public computing resources from external locations other than the organization's facilities.
88.	Role-Based Access Control-(RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.
89.	Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
90.	SAST	Static application security testing (SAST) is a set of technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyze an application from the "inside out" in a non running state.
91.	SDLC	The software development life cycle is a framework defining tasks performed at each step in the software development process. It consists of a detailed plan describing how to develop, maintain and replace specific software.
92.	Secure Socket Layer (SSL)	A protocol used for protecting private information during transmission via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL and many Websites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:"
93.	Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
	Security Incident Breach	A security incident breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of

94.		sensitive information maintained or processed by the organization
95.	Sensitivity	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.
96.	Session hijacking	An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker's goal is to gain access to a server while bypassing normal authentication measures.
97.	SHA2	Secure hash algorithm SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256) designed by the U.S. National Security agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard(FIPS).
98.	SIEM	Security Information and Event Management (SIEM) provides real-time analysis of security alerts generated by network hardware and applications. SIEM is sold as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.
99.	SNMP	Simple Network Management Protocol is an "Internet-standard protocol for managing devices on IP networks". It is used mostly in network management Systems to monitor network-attached devices for conditions that warrant administrative attention
100.	Social Engineering	A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.
101.	Spoofing	Altering data packets to falsely identify the originating computer. Spoofing is generally used when a hacker wants to make it difficult to trace where the attacks are coming from.
102.	SSH	Secure Shell is a program to login to another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.
103.	SSID	Service set identifier is a case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network that acts as a password when a device tries to connect to the basic service set a component of the IEEE 802.11 WLAN architecture.
104.	Standard	A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard.
105.	Threat	Any circumstance or event with the potential to adversely impact organizational operations including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
106.	Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
107.	Threat Modeling	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
108.	TLS	Transport Layer Security, a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.



109.	Traffic flood attacks	Traffic flooding attacks such as DoS / DDoS and Internet Worm.
110.	UTM	UTM combines multiple security features in to a single platform to protect against attacks, viruses, Trojans, spyware and other malicious threats. Complexity is reduced and management is simplified because multiple layers of protection are delivered under this single management console
111.	VPN	Virtual private network is a network that is constructed by using public wires — usually the Internet — to connect to a private network, such as a company's internal network. There are a number of systems that enable to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
112.	Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
113.	Vulnerability assessments	Vulnerability Assessment is the process of identifying network and device vulnerabilities before hacker scan exploit the security holes. It helps detect network and system vulnerabilities.
114.	WAF	A web application firewall is a form of firewall which controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall.
115.	WLAN	A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
116.	WLANIPS	The primary purpose of a Wireless Intrusion Prevention system is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure.
117.	WPA	WPA is a security technology for Wi-Fi wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy).
118.	WPA-2	Wi-Fi Protected Access2, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a highlevelofassurancethatonlyauthorizeduserscanaccesstheirwirelessnetworks.



#### **Annexure 4 –Additional references**

1. Glossary of Key Information Security Terms, NIST:[http://infohost.nmt.edu/~sfs/Regs/NISTIR-7298\\_Glossary\\_Key\\_Infor\\_Security\\_Terms.pdf](http://infohost.nmt.edu/~sfs/Regs/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf)
2. Harvard :<http://www.security.harvard.edu/glossary-terms>
3. SANS :<http://www.sans.org/security-resources/glossary-of-terms/>
4. Cyber Security Framework :<http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf>
5. NISTSpecialPublicationsinthe800series:<http://csrc.nist.gov/publications/PubsSPs.html>
6. DSCI Security Framework :<http://www.dsci.in/taxonomypage/63>
7. Federal Information Security Management Act (FISMA):  
[www.csrc.nist.gov/drivers/documents/FISMA-final.pdf](http://www.csrc.nist.gov/drivers/documents/FISMA-final.pdf)
8. Risk Assessment Methodologies: OCTAVE-<http://www.cert.org/octave/>
9. COSO- <http://www.coso.org/>
10. PCIstandardsdocumentation:[https://www.pcisecuritystandards.org/security\\_standards/](https://www.pcisecuritystandards.org/security_standards/)
11. COBIT :<http://www.isaca.org/COBIT/Pages/default.aspx>
12. Opensourcearchitectureframeworks[www.opensecurityarchitecture.org](http://www.opensecurityarchitecture.org)