Annexure A

Information Security Committee (ISC) and Chief Information Security Officer (CISO)

An Information Security Committee was constituted in the Central Board of Direct Taxes (CBDT) through order dated 7th April, 2015 and 19th June 2015, F. No. 500/137/2011-FTTR-III. The members of the Information Security Committee (ISC) are:-

(a) Member (IT), CBDT

(b) Joint Secretary (FT&TR-I)

(c) Joint Secretary (FT&TR-II)

(d) Joint Secretary (TPL-II)

(e) CIT (Inv.)

(f) CIT (InternationalTaxation-3), New Delhi

(g) DIT (I&CI), New Delhi

(h) DIT (Systems-II)

Member (IT), CBDT will be the Chairman of the ISC. CIT (InternationalTaxation-3), New Delhi shall also perform the role of Chief Information Security Officer (CISO).

Broad Responsibilities of ISC have been specified as under:

(a) Ratification of the Information Security Policies and Procedures (ISPP) suggested by the CISO.

(b) Ensure that ISPP is implemented by ensuring the involvement of the business heads.

(c) Conduct the management review of the ISPP to ensure continuing suitability, adequacy and effectiveness of ISPP.

(d) Initiate internal and external security reviews and ensuring that action is taken to rectify any identified shortfalls.

(e) Responsible for disciplinary action in cases of breach of ISPP.

Broad Responsibilities of CISO have been specified as under:

(a) Responsible for preparing, maintaining and communicating ISPP.

(b) Oversee all information security processes and serve as the focal point for all information security issues and concerns.

(c) Ensure that responsibilities are defined for and that procedures are in effect to promptly detect, investigate, report and resolve security incidents.

(d) Ensure that ongoing information security awareness education and training is provided to all employees.

(e) Provide reports to the ISC on the status of information security, policy violations and information security incidents.

Annexure B

Information Classification Guidelines

All information available with the office concerned should be classified into one of the following categories (based on Manual of Departmental Security Instructions issued by the Ministry of Home Affairs in 1994):

Classification	Description	Example
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
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
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	Treaty exchanged information, Seized material etc.
Restricted	Information, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose	Income Tax Return, Assessment orders etc.
Unclassified	Information that requires no protection against disclosure.	Public releases etc.

Annexure-C: Security Guidelines for Field Officers

Contents

1. Physical and environmental security

a. Background

1.1.1. 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

1.1.2. Physical security in an important component of information security and requires a careful attention in planning, selecting countermeasures, deploying controls, ensuring secure operations and respond in case of an event

1.1.3. 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.

b. Relevance of domain to information security

i. 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

ii. Insufficient entry controls may give access to unintended persons. It may allow entry of unauthorized assets or easy passage of sensitive assets from premises

iii. Without adequate interior physical control, unauthorized personnel may gain access to sensitive areas. Instances such as theft of information may remain undetected

iv. 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

c. Physical and environmental security guidelines

i. **Map and characteristics of physical facilities:** The organization must create an map of access point and information assets and systems housed within **PH.G1**

i. **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 **PH.G2**

i. **Physical boundary protection:** The organization must deploy an adequate level of perimeter security measures such as barriers, fencing, protective lighting, etc. **PH.G3**

i. **Restricting entry:** The organization must deploy an adequate level of countermeasures for restricting the entry to the facilities only to authorized persons **PH.G4**

i. **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 **PH.G5**

i. **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 **PH.G6**

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 within the premise

c. **Security and monitoring of zones:** Strict security measures in addition to round the clock monitoring of such areas must be done

i. **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 **PH.G7**

i. **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. **PH.G8**

d. **Physical and environmental security controls**

i. **Map and characteristics of physical facilities:** The organization must obtain visibility over physical facilities and information systems housed within **PH.C1**

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

i. **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 **PH.C2**

i. **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 **PH.C3**

i. **Securing gateways:** All entry and exit points to facilities housing information assets and systems must be secured by deploying manpower and appropriate technological solutions **PH.C4**

i. **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 **PH.C5**

i. **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 **PH.C6**

i. **Visitor verification:** All visitors to the facility must only be permitted to enter post validation from concerned employee. Visitor must be instructed to record **PH.C7** their identity credentials into the visitor register prior to permitting them inside the facility

i. **Infrastructure protection:** Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage **PH.C8**

ι. **Guarding facility:** The organization must ensure that an adequate number of security guards are deployed at the facilities **PH.C9**

ι. **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 **PH.C10**

i. **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. **PH.C11**

i. **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 **PH.C12**

i. **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. **PH.C13**

/. **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 **PH.C14**

/. **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 **PH.C15**

i. **Inactivity timeout:** All information systems must be configured to time-out a user's activity post inactivity for a designated period of time **PH.C16**

i. **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 **PH.C17**

i. **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 **PH.C18**

ι. **Categorization of zones:** The facilities in the organization must be categorized based on parameters such as the sensitivity of information in the facility, roles **PH.C19** of employees in facilities, operational nature of facility, influx of visitors etc.

ι. **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 **PH.C20**

i. **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 **PH.C21**

i. **Physical access auditing and review:** All attempts of physical access must be audited on a periodic basis **PH.C22**

e. **Physical security implementation guidelines**

i. **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 **PH.IG1**

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, 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.

i. **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, flood control assessment and other natural calamities amongst others **PH.IG2**

i. **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 **PH.IG3**

/. **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 **PH.IG4**

/. **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 **PH.IG5**

a. Appropriate measures must be undertaken to prevent tailgating inside the organizations facility

i. **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. **PH.IG6**

b. 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

c. Authorized personnel permitted to enter the data center or computer room must display their identification cards at all instances

d. Visitor access record shall be kept and properly maintained for audit purpose. The access records may include details such as name and organisation of the person visiting, signature of the visitor, date of access, time of entry and departure, purpose of visit, etc.

e. 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

i. **Visitor verification:** Visitor entry must be permitted only if prior notification has been shared via email from the concerned personnel. **PH.IG7**

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

i. **Infrastructure protection:** **PH.IG8**

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

i. **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, medical records must be maintained as a minimum **PH.IG9**

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 new storage devices, etc.

i. **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. **PH.IG10**

i. **Correlation between physical and logical security:** Physical security and logical security linkages must be created **PH.IG11**

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

i. **Monitoring & surveillance:** The organization must establish mechanism for 24/7 surveillance of all areas inside the physical perimeter by use of technology such as security cameras (or closed-circuit TV) **PH.IG12**

a. The organization must monitor the areas such as hosting critical/sensitive systems and have video images recorded. The recording 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

i. **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. **PH.IG13**

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

i. **Protection of information assets and systems:** Physical access to information assets and systems must be governed by employing techniques such as biometric access, smart cards, passwords etc. **PH.IG14**

i. **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 **PH.IG15**

i. **Inactivity timeout:** All information systems should be configured to automatically lock the computer system after 10 minutes of inactivity **PH.IG16**

i. **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 **PH.IG17**

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

i. **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 **PH.IG18**

ι. **Categorization of zones:** The facility should be categorized as follows: **PH.IG19**

a. **Public zone:** where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples: the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings

b. **Reception zone**: where the transition from a public zone to a restricted-access area is demarcated and controlled. It is typically located at the entry to the facility where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons

c. **Operations zone:** an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously. Examples: typical open office space, or typical electrical room

d. **Security zone:** area to which access is limited to authorized personnel, and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously. Example: an area where secret information is processed or stored

e. **High security zone**: an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications, monitored continuously and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel

ι. **Access to restricted areas:** Visitors requiring access to restricted areas must be accompanied by authorized personnel. Visitor details such as name of the visitor, time of visit, purpose of visit, serial number of the equipment (if being carried), name of authorized person, signature of authorized person etc. must be **PH.IG20** maintained by the security personnel responsible for the area/facility

a. In case, any equipment is being carried out by the visitor, appropriate written authorization granted by the head of the department/ concerned official must be presented to security personnel

b. An inventory of all equipment taken out of the facility should be maintained. Details such as equipment name, serial number, model number, department/ owner, name of approver etc. must be maintained

c. The information security team must co-authorize the removal of equipment from its deployment site

i. **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. **PH.IG21**

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 assets. 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

i. **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 **PH.IG22**

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

f. **Adoption matrix for Physical Security**

	Top secret	**Secret**	**Confidential**	**Restricted**	**Unclassified**
Guidelines					
Map and characteristics of physical facilities	PH.G1	PH.G1	PH.G1	PH.G1	
Protection from hazard	PH.G2	PH.G2	PH.G2	PH.G2	PH.G2
Physical boundary protection	PH.G3	PH.G3	PH.G3	PH.G3	PH.G3
Restricting entry	PH.G4	PH.G4	PH.G4		
Interior security	PH.G5	PH.G5	PH.G5	PH.G5	
Security zones	PH.G6	PH.G6	PH.G6	PH.G6	
Access to restricted area	PH.G7	PH.G7	PH.G7	PH.G7	
Physical activity monitoring and review	PH.G8	PH.G8	PH.G8	PH.G8	
Controls					
Map and characteristics of physical facilities	PH.C1	PH.C1	PH.C1	PH.C1	
Hazard assessment	PH.C2	PH.C2	PH.C2	PH.C2	PH.C2
Hazard protection	PH.C3	PH.C3	PH.C3	PH.C3	PH.C3
Securing gateways	PH.C4	PH.C4	PH.C4	PH.C4	
Identity badges	PH.C5	PH.C5	PH.C5	PH.C5	
Entry of visitors & external service providers	PH.C6	PH.C6	PH.C6	PH.C6	
Visitor verification	PH.C7	PH.C7	PH.C7	PH.C1	
Infrastructure protection	PH.C8	PH.C8	PH.C8	PH.C2	PH.C8
Guarding facility	PH.C9	PH.C9	PH.C9	PH.C9	
Vehicle entry	PH.C10	PH.C10	PH.C10	PH.C10	
Correlation between physical and logical security	PH.C11	PH.C11	PH.C11		
Monitoring & surveillance	PH.C12	PH.C12	PH.C12		
Disposal of equipment	PH.C13	PH.C13	PH.C13	PH.C13	
Protection of information assets and systems	PH.C14	PH.C14	PH.C14		
Authorization for change	PH.C15	PH.C15	PH.C15		
Inactivity timeout	PH.C16	PH.C16	PH.C16	PH.C16	
Protection of access keys and methodology	PH.C17	PH.C17	PH.C17	PH.C17	
Shoulder surfing	PH.C18	PH.C18	PH.C18	PH.C18	

	Top secret	**Secret**	**Confidential**	**Restricted**	**Unclassified**
Categorization of zones	PH.C19	PH.C19	PH.C19	PH.C19	
Access to restricted areas	PH.C20	PH.C20	PH.C20	PH.C20	
Visitor device management	PH.C21	PH.C21	PH.C21	PH.C21	
Physical access auditing and review	PH.C22	PH.C22	PH.C22	PH.C22	
Implementation Guidelines					
Map and characteristics of physical facilities	PH.IG1, PH.IG1(a), (b),(c)	PH.IG1, PH.IG1(a), (b),(c)	PH.IG1, PH.IG1(a), (b),(c)	PH.IG1, PH.IG1(a), (b),(c)	
Hazard assessment	PH.IG2	PH.IG2	PH.IG2	PH.IG2	PH.IG2
Hazard protection	PH.IG3	PH.IG3	PH.IG3	PH.IG3	PH.IG3
Securing gateways	PH.IG4	PH.IG4	PH.IG4	PH.IG4	
Identity badges	PH.IG5, PH.IG5(a)	PH.IG5, PH.IG5(a)	PH.IG5, PH.IG5(a)	PH.IG5	
Entry of visitors & external service providers	PH.IG6, PH.IG6 (a) to (e)	PH.IG6, PH.IG6 (a) to (e)	PH.IG6, PH.IG6 (a) to (e)	PH.IG6	
Visitor verification	PH.IG7, PH.IG7(a), (b),(c)	PH.IG7, PH.IG7(a),(b), (c)	PH.IG7, PH.IG7(a), (b),(c)	PH.IG7, PH.IG7 (a),(b) ,(c)	
Infrastructure protection	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)	PH.IG8, PH.IG8 (a),(b),(c)
Guarding facility	PH.IG9, PH.IG9(a), (b)	PH.IG9, PH.IG9 (a),(b)	PH.IG9, PH.IG9(a)	PH.IG9	
Vehicle entry	PH.IG10	PH.IG10	PH.IG10		
Correlation between physical and logical security	PH.IG11, PH.IG11(a), (b)	PH.IG11, PH.IG11(a),(b)	PH.IG11, PH.IG11(a), (b)		
Monitoring & surveillance	PH.IG12, PH.IG12(a), (b)	PH.IG12, PH.IG12(a), (b)	PH.IG12, PH.IG12(a), (b)		
Disposal of equipment	PH.IG13, PH.IG13(a)	PH.IG13, PH.IG13(a)	PH.IG13, PH.IG13(a)	PH.IG13, PH.IG13(a)	
Protection of information assets and systems	PH.IG14	PH.IG14	PH.IG14		
Authorization for change	PH.IG15	PH.IG15	PH.IG15		

	Top secret	Secret	Confidential	Restricted	Unclassified
Inactivity timeout	PH.IG16	PH.IG16	PH.IG16	PH.IG16	
Protection of access keys	PH.IG17, PH.IG17 (a),(b),(c)	PH.IG17, PH.IG17 (a),(b),(c)	PH.IG17, PH.IG17(c)		
Shoulder surfing	PH.IG18	PH.IG18	PH.IG18	PH.IG18	
Categorization of zones	PH.IG19, PH.IG13(e)	PH.IG19, PH.IG13(d)	PH.IG19, PH.IG13(d)	PH.IG19, PH.IG13(c)	
Access to restricted areas	PH.IG20, PH.IG20 (a),(b),(c)	PH.IG20, PH.IG20 (a),(b),(c)	PH.IG20, PH.IG20(a), (b),(c)	PH.IG20	
Visitor device management	PH.IG21, PH.IG21 (a),(b),(c)	PH.IG21, PH.IG21 (a),(b),(c)	PH.IG21, PH.IG21 (a),(b)	PH.IG21, PH.IG21 (a),(b)	
Physical access auditing and review	PH.IG22, PH.IG22 (a),(b),(c)(d) (e)	PH.IG22, PH.IG22 (a),(b),(c)(d)(e)	PH.IG22, PH.IG22 (a),(b)	PH.IG22, PH.IG22 (a),(b)	

2. Personnel Security

a. **Background**

i. 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

ii. 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

iii. 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

b. **Relevance of domain to information security**

i. 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

ii. 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

iii. 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

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

v. 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

c. **Personnel security guidelines**

i. **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 **PE.G1**

i. **Employee verification**: The organization must conduct background checks or security clearance as part of its employee hiring process **PE.G2**

i. **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 **PE.G3**

/. **Record of authorized users:** The organization should maintain an updated record of all users granted access to each information asset and system **PE.G4**

/. **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 **PE.G5**

i. **Monitoring and review:** The organization must implement appropriate monitoring tools and technology to track compliance of personnel with organization's policies **PE.G6**

i. **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 **PE.G1**

d. **Personnel security controls**

i. **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: **PE.C1**

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 assets 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

i. **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 **PE.C2**

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

i. **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 **PE.C3**

b. 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

c. Under no circumstances shall third party vendors or partner be allowed unmonitored access to the organizations information or information systems

/. **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 **PE.C4**

/. **Disciplinary processes**: Ensure that a mechanism and supporting disciplinary processes are established to resolve non-compliance issues and other variances in a timely manner **PE.C5**

i. **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 **PE.C6**

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

i. **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 **PE.C7**

i. **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 **PE.C8**

ι. **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 **PE.C9**

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

ι. **Communication practices:** The organization must prohibit its employees and external parties from disseminating/ communicating classified information for any other purpose expect its authorized and intended use **PE.C10**

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

e. **Personnel security implementation guidelines**

i. **Training and awareness:** Organization must undertake the development, implementation and evaluation of role-based training for all personnel **PE.IG1**

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, incident reporting amongst others

i. **Employee verification:** Organization must conduct employee verification by using methods such as **PE.IG2**

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, family details amongst others

i. **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 **PE.IG3**

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

i. **Acceptable use policies:** Organization must identify, document, and implement acceptable usage policy and incorporate the following: **PE.IG4**

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

i. **Disciplinary process:** Organization must establish disciplinary process to cater to instances of non-compliance to its security or acceptable usage policy **PE.IG5**

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

i. **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: **PE.IG6**

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 areas allowed to access

e. Registered/allocated devices and information systems

f. Category of classified information permitted to access

i. **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. **PE.IG7**

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

i. **Non-disclosure agreements:** Organization should include signing of non- **PE.IG8** disclosure contracts and agreements in HR process during employment

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

ɩ. **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 **PE.IG9**

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.

ɩ. **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 **PE.IG10**

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

c. Information/ communication shared with internal or external personnel or entities must be approved by top management

f. **Adoption matrix for Personnel Security**

	Top secret	Secret	Confidential	Restricted	Unclassified
Guidelines					
Awareness & training	PE.G1	PE.G1	PE.G1	PE.G1	
Employee verification	PE.G2	PE.G2	PE.G2	PE.G2	
Authorizing access to third parties	PE.G3	PE.G3	PE.G3	PE.G3	
Record of authorized users	PE.G4	PE.G4	PE.G4	PE.G4	
Acceptable usage policy	PE.G5	PE.G5	PE.G5	PE.G5	
Monitoring and review	PE.G6	PE.G6	PE.G6	PE.G6	
Limiting exposure of information	PE.G7	PE.G7	PE.G7	PE.G7	
Controls					
Training and Awareness	PE.C1	PE.C1	PE.C1	PE.C1	
Employee verification	PE.C2	PE.C2	PE.C2	PE.C2	
Authorizing access to third parties	PE.C3	PE.C3	PE.C3	PE.C3	
Acceptable use policies	PE.C4	PE.C4	PE.C4	PE.C4	
Disciplinary processes	PE.C5	PE.C5	PE.C5	PE.C5	
Record of authorized users	PE.C6	PE.C6	PE.C6	PE.C6	
Monitoring and review	PE.C7	PE.C7	PE.C7	PE.C7	
Non- disclosure agreements	PE.C8	PE.C8	PE.C8	PE.C8	
Legal and contractual obligations	PE.C9	PE.C9	PE.C9	PE.C9	
Communication practices	PE.C10	PE.C10	PE.C10	PE.C10	
Implementation guidelines					
Training and awareness	PE.IG1, PE.IG1 (a), to (j)	PE.IG1, PE.IG1 (a) to (j)	PE.IG1, PE.IG1 (a),(b),(d) to (j)	PE.IG1, PE.IG1 (g),(h),(i),(j)	
Employee verification	PE.IG2, PE.IG2 (a),(b),(c)	PE.IG2, PE.IG2 (a),(b),(c)	PE.IG2, PE.IG2 (a),(b),(c)	PE.IG2, PE.IG2 (a),(b),(c)	
Authorizing access to third parties	PE.IG3, PE.IG3 (a) to (f)	PE.IG3, PE.IG3 (a) to (f)	PE.IG3, PE.IG3 (a) to (f)	PE.IG3, PE.IG3 (a) to (f)	

	Top secret	Secret	Confidential	Restricted	Unclassified
Acceptable use policies	PE.IG4, PE.IG4 (a), (b), (c)	PE.IG4, PE.IG4 (a), (b), (c)	PE.IG4, PE.IG4 (a), (b), (c)	PE.IG4, PE.IG4 (a), (b), (c)	
Disciplinary process	PE.IG5, PE.IG5(a)	PE.IG5, PE.IG5(a)	PE.IG5, PE.IG5(a)	PE.IG5, PE.IG5(a)	
Record of authorized users	PE.IG6, PE.IG6 (a) to (f)	PE.IG6, PE.IG6 (a) to (f)	PE.IG6, PE.IG6 (a) to (f)	PE.IG6, PE.IG6 (a) to (f)	
Monitoring and review	PE.IG7, PE.IG7(a)	PE.IG7, PE.IG7(a)	PE.IG7, PE.IG7(a)	PE.IG7, PE.IG7(a)	
Non-disclosure agreements	PE.IG8, PE.IG8(a)	PE.IG8, PE.IG8(a)	PE.IG8, PE.IG8(a)	PE.IG8, PE.IG8(a)	
Legal and contractual obligations	PE.IG9, PE.IG9(a), (b)	PE.IG9, PE.IG9(a),(b)	PE.IG9, PE.IG9(a),(b)	PE.IG9, PE.IG9(a), (b)	
Communication practices	PE.IG10, PE.IG10 (a),(b),(c)	PE.IG10, PE.IG10 (a),(b),(c)	PE.IG10, PE.IG10 (a),(b),(c)	PE.IG10, PE.IG10 (a),(b),(c)	

3. Identity, access and privilege management

a. Background

i. 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

ii. 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

iii. 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

b. Relevance of domain to information security

i. 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

ii. As there is significant complexity of user identities, privileges and access patterns, the organization may struggle to comprehend the exposure of information and exposure of information to unintended persons may get unnoticed

iii. 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

c. Identity, access and privilege management guidelines

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. **IA.G1**

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

i. **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, users roles and security requirements **IA.G2**

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

i. **Password management:** The organizations must have standardized, reliable and secure way of managing passwords of users **IA.G3**

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

/. **Credential monitoring:** The organization must ensure that instances of user access provisioning, identification, authentication, access authorization, credential changes and deprovisioning are logged **IA.G4**

a. The access instances should be monitored and reviewed for identifying discrepancies

b. Malicious attempts of authentication should be prevented, recorded and reviewed

/. **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 **IA.G5**

i. **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 **IA.G6**

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

i. **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. **IA.G7**

i. **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 **IA.G8**

i. **Disciplinary actions:** The organizations must incorporate provisions for managing discrepancies and non-conformance in the disciplinary processes **IA.G9**

d. **Identity, access and privilege management controls**

i. **Operational requirement mapping:** The organization must ensure that operational requirements are carefully studied to translate them into access requirements **IA.C1**

i. **Unique identity of each user:** The organization must ensure that each user identity (User-ID) is uniquely attributable to only one unique user **IA.C2**

i. **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 **IA.C3**

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

i. **Access control policies:** The organization must define access control policies which are integrate-able with existing architecture and technological, administrative and physical controls **IA.C4**

i. **Need – to – know access:** Access rights to information and information systems must only be granted to users based on a need-to-know basis **IA.C5**

i. **Review of user privileges:** The organization must enforce a process to review user privileges periodically **IA.C6**

i. **Special privileges:** The organization must ensure that the use of special privileges shall be restricted, controlled and monitored as per organization's policy **IA.C7**

i. **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. **IA.C8**

i. **Inactive accounts:** Inactive accounts must be disabled as per organizations policy **IA.C9**

i. **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 use of user account privileges **IA.C10**

i. **Password policy:** The organization must define a password policy **IA.C11**

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

i. **Default device credentials:** The organization must ensure that all vendor-supplied default passwords for equipment and information systems are changed before any information system is put into operation **IA.C12**

i. **Monitoring and retention of logs:** The organization must monitor and retain records for all activity related to granting access to users **IA.C13**

/. **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 **IA.C14**

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

/. **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 **IA.C15**

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

i. **Remote access:** The organization must ensure that security measures are in place to govern the remote access to information systems **IA.C16**

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 IPsec

i. **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 **IA.C17**

i. **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 **IA.C18**

ι. **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 be accountable and responsible for all activities performed with their User-IDs **IA.C19**

e. Identity, access and privilege implementation guidelines

i. **Operational requirement mapping:** The organization must develop a formal procedure to govern allocation of user identification and access mechanism. All **IA.IG1** 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

i. **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 **IA.IG2**

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

i. **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 **IA.IG3**

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, access level authorization, access requirement for applications, databases, files, 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 asset/ system owner approval

/. **Access control policies:** The organization must enforce, govern and measure compliance with access control policy. **IA.IG4**

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

/. **Need – to – know access:** Access privileges to users must be based on operational role and requirements **IA.IG5**

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

i. **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. **IA.IG6**

i. **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 **IA.IG7**

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

i. **Authentication mechanism for access**: The organization must have various levels of authentication mechanisms **IA.IG8**

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

d. Use directory services such as LDAP and X500

ί. **Inactive accounts:** The organization must ensure the following: **IA.IG9**

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

ί. **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 **IA.IG10**

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

i. **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 **IA.IG11**

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.

i. **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 **IA.IG12**

i. **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 **IA.IG13**

/. **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 **IA.IG14**

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

/. **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 **IA.IG15**

i. **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. **IA.IG16**

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 IPsec

b. Enable capture of logs of all activity conducted via remote access

c. Audit logs of all activity conducted via remote access

i. **Provisioning of personal devices:** *Refer personnel security* **IA.IG17**

i. **Segregation of duties:** The organization must ensure the following: **IA.IG18**

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

k. **User awareness & liability:** *Refer Personnel security* **IA.IG19**

f. **Adoption matrix for Identity, access and privilege management**

	Top secret	Secret	Confidential	Restricted	Unclassified
Guidelines					
Governance procedures for access rights, identity & privileges	IA.G1	IA.G1	IA.G1	IA.G1	IA.G1
Authentication & authorization for access	IA.G2	IA.G2	IA.G2	IA.G2	
Password management	IA.G3	IA.G3	IA.G3	IA.G3	
Credential monitoring	IA.G4	IA.G4	IA.G4	IA.G4	
Provisioning personal devices and remote access	IA.G5	IA.G5	IA.G5	IA.G5	
Segregation of duties	IA.G6	IA.G6	IA.G6	IA.G6	
Access record documentation	IA.G7	IA.G7	IA.G7		
Linkage of logical and physical access	IA.G8	IA.G8			
Disciplinary actions	IA.G9	IA.G9	IA.G9	IA.G9	
Controls					
Operational requirement mapping	IA.C1	IA.C1	IA.C1	IA.C1	
Unique identity of each user	IA.C2	IA.C2	IA.C2	IA.C2	
User access management	IA.C3	IA.C3	IA.C3	IA.C3	
Access control policies	IA.C4	IA.C4	IA.C4	IA.C4	
Need – to – know access	IA.C5	IA.C5	IA.C5	IA.C5	
Review of user privileges	IA.C6	IA.C6	IA.C6	IA.C6	
Special privileges	IA.C7	IA.C7	IA.C7	IA.C7	
Authentication mechanism for access	IA.C8	IA.C8	IA.C8	IA.C8	
Inactive accounts	IA.C9	IA.C9	IA.C9	IA.C9	
Acceptable usage of Information assets & systems	IA.C10	IA.C10	IA.C10	IA.C10	
Password policy	IA.C11	IA.C11	IA.C11	IA.C11	
Default device credentials	IA.C12	IA.C12	IA.C12	IA.C12	
Monitoring and retention of logs	IA.C13	IA.C13	IA.C13	IA.C13	
Unsuccessful log-in attempts	IA.C14	IA.C14	IA.C14	IA.C14	
Ad-hoc access to systems	IA.C15	IA.C15	IA.C15	IA.C15	
Remote access	IA.C16	IA.C16	IA.C16	IA.C16	
Provisioning of personal devices	IA.C17	IA.C17	IA.C17	IA.C17	

	Top secret	Secret	Confidential	Restricted	Unclassified
Segregation of duties	IA.C18	IA.C18	IA.C18	IA.C18	
User awareness & liability	IA.C19	IA.C19	IA.C19	IA.C19	
Implementation Guidelines					
Operational requirement mapping	IA.IG1, IA.IG19 (a) to (d)	IA.IG1, IA.IG1 (a) to (d)	IA.IG1, IA.IG1 (a) to (d)	IA.IG1, IA.IG1 (a),(b)	
Unique identity of each user	IA.IG2, IA.IG2 (a) to (g)	IA.IG2, IA.IG2 (a) to (g)	IA.IG2, IA.IG2(a) to (g)	IA.IG2, IA.IG2(a) to (g)	
User access management	IA.IG3, IA.IG3 (a) to (d)	IA.IG3, IA.IG3 (a) to (d)	IA.IG3, IA.IG3 (a) to (d)	IA.IG3, IA.IG3 (a) to (d)	
Access control policies	IA.IG4, IA.IG4(a) to (d)	IA.IG4, IA.IG4(a) to (d)	IA.IG4, IA.IG4(a) to (d)	IA.IG4, IA.IG4 (a),(b),(c)	
Need – to – know access	IA.IG5, IA.IG5 (a) to (d)	IA.IG5, IA.IG5 (a) to (d)	IA.IG5, IA.IG5 (a),(b),(c)	I IA.IG5, IA.IG5 (a),(b)	
Review of user privileges	IA.IG6	IA.IG6	IA.IG6	IA.IG6	
Special privileges	IA.IG7, IA.IG7 (a),(b),(c)	IA.IG7, IA.IG7 (a),(b),(c)	IA.IG7, IA.IG7 (a),(b),(c)	IA.IG7, IA.IG7 (a),(b),(c)	
Authentication mechanism for access	IA.IG8, IA.IG8 (a) to (d)	IA.IG8, IA.IG8 (a) to (d)	IA.IG8, IA.IG8 (a) to (d)	IA.IG8, IA.IG8 (a)	
Inactive accounts	IA.IG9, IA.IG9 (a) to (d)	IA.IG9, IA.IG9 (a) to (d)	IA.IG9, IA.IG9 (a) to (d)	IA.IG9, IA.IG9 (a)	
Acceptable usage of Information assets & systems	IA.IG10, IA.IG10 (a),(b),(c)	IA.IG10, IA.IG10 (a),(b),(c)	IA.IG10, IA.IG10 (a),(b),(c)	IA.IG10, IA.IG10 (a),(b),(c)	
Password policy	IA.IG11, IA.IG11 (a) to (f)	IA.IG11, IA.IG11 (a) to (f)	IA.IG11, IA.IG11 (a) to (f)	IA.IG11, IA.IG11 (a) to (e),	
Default device credentials	IA.IG12	IA.IG12	IA.IG12	IA.IG12	
Monitoring and retention of logs	IA.IG13	IA.IG13	IA.IG13		
Unsuccessful login attempts	IA.IG14, IA.IG14 (a),(b)	IA.IG14, IA.IG14 (a),(b)	IA.IG14, IA.IG14 (a),(b)	IA.IG14, IA.IG14 (a),(b)	
Ad-hoc access to systems	IA.IG15	IA.IG15	IA.IG15	IA.IG15	

	Top secret	Secret	Confidential	Restricted	Unclassified
Remote access	IA.IG16, IA.IG16 (a),(b),(c)	IA.IG16, IA.IG16 (a),(b),(c)	IA.IG16, IA.IG16 (a),(b),(c)	IA.IG16, IA.IG16 (a),(b),(c)	
Provisioning of personal devices	IA.IG17	IA.IG17	IA.IG17	IA.IG17	
Segregation of duties	IA.IG18, IA.IG18 (a) to (g)	IA.IG18, IA.IG18 (a) to (g)	IA.IG18, IA.IG18 (a) to (g)	IA.IG18, IA.IG18 (a)	
User awareness & liability	IA.IG19	IA.IG19	IA.IG19	IA.IG19	

4. Security monitoring and incident management

a. **Background**

i. 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

ii. 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

b. **Relevance of domain to information security**

i. 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

ii. 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 able to steal information. This requires continuous monitoring of operations to identify likely instances of information loss

iii. 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

iv. 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

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

c. **Security monitoring & incident management guidelines**

i. **Incident response coverage:** The organization must develop the monitoring and incident response program such that it addresses the requirements of its extended ecosystem **SM.G1**

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

i. **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 **SM.G2**

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

i. **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 **SM.G3**

/. **Enterprise log management:** The organization must ensure that logs are collected, stored, retained and analyzed for the purpose of identifying compromise or breach **SM.G4**

/. **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 **SM.G5**

i. **Disciplinary action:** The organization must establish procedures in dealing with individuals involved in or being party to the incidents **SM.G6**

i. **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 **SM.G7**

i. **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 **SM.G8**

ι. **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 clients and regulators **SM.G9**

d. **Security monitoring & incident management controls**

i. **Security incident monitoring:** The organization must build capability to monitor activity over information assets and systems that are being used across its ecosystems **SM.C1**

i. **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 **SM.C2**

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

i. **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 **SM.C3**

/. **Incident evaluation:** The organization must define polices and processes for logging, monitoring and auditing of all activity logs **SM.C4**

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

/. **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 **SM.C5**

i. **Breach information:** Ensure that knowledge of incidents, and corrective action taken should be compiled in a structured manner. The organizations **SM.C6** 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

i. **Configuring devices for logging:** The organization must configure the devices to generate log information required to identify security compromise or breach **SM.C7**

i. **Activity logging:** The organization must define a process for collection, management and retention of log information from all information sources **SM.C8**

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

i. **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. **SM.C9**

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

i. **Log information correlation:** Organization should ensure that a process is established for regular review and analysis of logs and log reports **SM.C10**

i. **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. **SM.C11**

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

i. **Deployment of skilled resources:** The organization must deploy personnel with requisite technical skills for timely addressing and managing incidents **SM.C12**

i. **Incident reporting:** The organization must ensure that a mechanism exists for employees, partners and other third parties to report incidents **SM.C13**

a. Incident management should support information breach notification requirements as well as formal reporting mechanisms

b. Ensure that a significant level of efforts are dedicated towards spreading awareness about incident response process throughout the organization and to partners and other third parties

i. **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 **SM.C14**

i. **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. **SM.C15**

e. **Security monitoring and incident management implementation guidelines**

i. **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: **SM.IG1**

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

i. **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 **SM.IG2**

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

i. **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 **SM.IG3**

a. Security capability should seek to detect and/or "prevent" attacks through monitoring activity

b. Establish processes to identify and report intruders 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

iv. **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. **SM.IG4**

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 timely manner so that fastest possible remedial measures can be taken to reduce further damage to the IT assets

v. **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 **SM.IG5**

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

i. **Breach information:** The organization must ensure adequate knowledge of incident/ breach is obtained through post incident analysis. **SM.IG6**

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

i. **Configuring devices for logging:** The organization must establish logging policies on all ICT systems and devices including security devices such as firewalls etc., by enabling syslog, event manager amongst others **SM.IG7**

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

i. **Activity logging:** The organization must define a process for collection, management and retention of log information from all information sources **SM.IG8**

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

ι. **Log Information:** Ensure that system logs contain information capture including all the key events, activity, transactions such as: **SM.IG9**

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)

x. **Log information correlation:** The organization must schedule a periodic log review process for examination of any attempted system breaches, failed login attempts amongst others **SM.IG10**

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 implement 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

xi. **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 **SM.IG11**

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

i. **Deployment of skilled resources:** The organization must define the resources and management support needed to effectively maintain and mature an incident response capability **SM.IG12**

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 trains personnel in their incident response roles and responsibilities with respect to the information system

c. The organization should incorporate simulated events into 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

i. **Incident reporting:** The organization must ensure that appropriate procedures are followed to enable reporting of incidents both by employees and partner agencies **SM.IG13**

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

/. **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. **SM.IG14**

/. **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. **SM.IG15**

f. Adoption matrix for Security Monitoring and Incident Reporting

	Top secret	Secret	Confidential	Restricted	Unclassified
Guidelines					
Incident response coverage	SM.G1	SM.G1	SM.G1	SM.G1	
Breach information	SM.G2	SM.G2	SM.G2	SM.G2	
Security intelligence information	SM.G3	SM.G3	SM.G3	SM.G3	
Enterprise log management	SM.G4	SM.G4	SM.G4	SM.G4	
Deployment of skilled resources	SM.G5	SM.G5	SM.G5	SM.G5	
Disciplinary action	SM.G6	SM.G6	SM.G6	SM.G6	
Structure & responsibility	SM.G7	SM.G7	SM.G7	SM.G7	
Incident management awareness and training	SM.G8	SM.G8	SM.G8	SM.G8	
Communication of incidents	SM.G9	SM.G9	SM.G9	SM.G9	
Controls					
Security incident monitoring	SM.C1	SM.C1	SM.C1	SM.C1	
Incident management	SM.C2	SM.C2	SM.C2	SM.C2	
Incident identification	SM.C3	SM.C3	SM.C3	SM.C3	
Incident evaluation	SM.C4	SM.C4	SM.C4	SM.C4	
Escalation process	SM.C5	SM.C5	SM.C5	SM.C5	
Breach information	SM.C6	SM.C6	SM.C6	SM.C6	
Configuring devices for logging	SM.C7	SM.C7	SM.C7	SM.C7	
Activity logging	SM.C8	SM.C8	SM.C8	SM.C8	
Log information	SM.C9	SM.C9	SM.C9	SM.C9	
Log information correlation	SM.C10	SM.C10	SM.C10	SM.C10	
Protecting log information	SM.C11	SM.C11	SM.C11	SM.C11	
Deployment of skilled resources	SM.C12	SM.C12	SM.C12	SM.C12	
Incident reporting	SM.C13	SM.C13	SM.C13	SM.C13	
Sharing of log information with law enforcement agencies	SM.C14	SM.C14	SM.C14	SM.C14	
Communication of incidents	SM.C15	SM.C15	SM.C15	SM.C15	
Implementation Guidelines					
Security incident monitoring	SM.IG1, SM.IG1 (a) to (f)	SM.IG1, SM.IG1 (a) to (f)	SM.IG1, SM.IG1 (a) to (f)	SM.IG1, SM.IG1 (a) to (f)	
Incident management	SM.IG2, SM.IG2 (a) to (d)	SM.IG2, SM.IG2 (a) to (d)	SM.IG2 (c),(d)	SM.IG2 (c),(d)	

	Top secret	Secret	Confidential	Restricted	Unclassified
Incident identification	SM.IG3, SM.IG3(a) to (h)	SM.IG3, SM.IG3(a) to (h)	SM.IG3, SM.IG3 (g),(h)	SM.IG3, SM.IG3 (g),(h)	
Incident evaluation	SM.IG4, SM.IG4 (a) to (h)	SM.IG4, SM.IG4 (a) to (h)	SM.IG4, SM.IG4 (a) to (h)	SM.IG4, SM.IG4 (a) to (h)	
Escalation processes	SM.IG5, SM.IG5 (a) to (e)	SM.IG5, SM.IG5 (a) to (e)	SM.IG5, SM.IG5 (a) to (e)	SM.IG5, SM.IG5 (a) to (e)	
Breach information	SM.IG6, SM.IG6(a),(b)	SM.IG6, SM.IG6(a), (b)	SM.IG6, SM.IG6 (a),(b)	SM.IG6, SM.IG6 (a),(b)	
Configuring devices for logging	SM.IG7, SM.IG7(a)	SM.IG7, SM.IG7(a)	SM.IG7, SM.IG7(a)	SM.IG7, SM.IG7(a)	
Activity logging	SM.IG8, SM.IG8 (a) to (c)	SM.IG8, SM.IG8(a) to (c)	SM.IG8, SM.IG8 (a) to (c)	SM.IG8, SM.IG8 (a) to (c)	
Log Information	SM.IG9, SM.IG9 (a) to (v)	SM.IG9, SM.IG9 (a) to (v)	SM.IG9, SM.IG9 (a) to (v)	SM.IG9, SM.IG9 (a) to (v)	
Log information correlation	SM.IG10, SM.IG10 (a),(b),(c)	SM.IG10, SM.IG10 (a),(b),(c)	SM.IG10, SM.IG10 (a),(b),(c)	SM.IG10, SM.IG10 (a),(b),(c)	
Protecting log information	SM.IG11, SM.IG11 (a) to (f)	SM.IG11, SM.IG11 (a) to (f)	SM.IG11, SM.IG11 (a) to (f)	SM.IG11, SM.IG11 (a) to (f)	
Deployment of skilled resources	SM.IG12, SM.IG12 (a) to (d)	SM.IG12, SM.IG12 (a) to (d)	SM.IG12, SM.IG12 (a) to (d)	SM.IG12, SM.IG12 (a) to (d)	
Incident reporting	SM.IG13 SM.IG13 (a) to (d)	SM.IG13 SM.IG13 (a) to (d)	SM.IG13 SM.IG13 (a) to (d)	SM.IG13 SM.IG13 (a) to (d)	
Sharing of log information with law enforcement agencies	SM.IG14	SM.IG14	SM.IG14	SM.IG14	
Communication of Incidents	SM.IG15	SM.IG15	SM.IG15	SM.IG15	