आज़ादी का अमृत महोत्सव

केन्द्रीय भण्डारण निगम
(भारत सरकार का उपक्रम)
CENTRAL WAREHOUSING CORPORATION
(A Govt. of India Undertaking)
जन-जन के लिए भण्डारण/Warehousing for Everyone

CWC CO-MIS/22/2020-MIS Date: - 11.01.2023

SUB.:- Standard Operating Procedures for ISO 27001 Information Security.

1. Corporation's e-Tools, and the information, including data they contain, are fundamental for its daily operations and effective service provision. In this regard, ISO 27001 (formally known as ISO/IEC 27001:2005) stipulates international standards for any organization to protect their data, information or assets etc., from any possible informational loss/ breach or from cyber-attacks. ISO 27001 is a specification for an **Information Security Management System (ISMS**). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.
2. Accordingly, Corporation aims to implement adequate security guidelines, procedures and controls to protect confidentiality, maintain integrity, and ensure availability of all information stored, processed and transmitted through its information systems.
3. "Information Security Procedures" outlines the overall direction and intent on implementation of controls for integrity, confidentiality and availability of information and information assets.
4. These security procedures applies to any person (such as employees, system administrator or in-charge, users, auditors, contractors, consultants, outsourced vendors, third parties and others) who access or use Corporation's information/ information systems.
5. While Corporation would like to respect privacy of its employees, it reserves the right to audit and/or monitor the activities of its employees and information stored, processed, transmitted or handled by the employees using Corporation's information systems.
6. With the implementation of these procedures, it shall be stipulated that Corporation is committed to maintain robust security practices and controls to preserve confidentiality, integrity and availability of information assets by optimal processes, technology and trained personnel from all threats, whether internal or external, deliberate or accidental.
7. The instructions are to be implemented across PAN India. Corporation is also using 46+ e-Tools. The Corporation is going first time for the ISO 27001 Certification therefore MIS Division every year shall look into these policies and procedures in terms of implementation and latest updates required as per the latest security standards and guidelines issued by Cert-In and any other government bodies.
8. The overall objective of this Information Security is to ensure:

   8.1. Information is available and usable when required and the systems that provide it can appropriately resist and recover from failures (Availability)

   8.2. Information is observed by or disclosed to only those who have right to know. (Confidentiality)

8.3. Information is protected against un-authorized modification (Integrity)

8.4. Protecting information against un-authorized access (Access Control)

8.5. Business transactions as well as information exchanges between Corporation’s different locations or with partners/users can be trusted (Authenticity and non-repudiation)

9. Corporation and all employees of Corporation shall be committed in true spirit for compliance of ISMS in accordance with the set documented procedures as per ISO 27001:2013.

10. Approval for exceptions or deviations from the procedures, wherever warranted, will be provided only by Competent Authority.

11. The review of all the procedures shall be ensured once in a year (During Quarter April to June) or if there is any change in ISO/regulatory guidelines or any reason pointed out in surveillance audit etc.

12. The security guidelines mentioned in the SoPs shall supersede all earlier guidelines stipulated in the Corporation.

13. The SoPs with the functionalities given below shall aim to comply standard controls as per ISO 27001, which are attached as a booklet with this circular for compliance:-

13.1 Information Security:-

13.1.1 To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

13.1.2 A set of procedures for information security shall be defined, approved, published and communicated to employees and relevant external parties.

13.1.3 The procedures for information security shall be reviewed at yearly basis or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

13.2 Organization of Information Security:-

13.2.1 To establish a management framework to initiate and control the implementation and operation of information security within the Corporation.

13.2.2 All information security responsibilities shall be defined and allocated.

13.2.3 Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Corporation’s assets.

13.2.4 Appropriate contacts with relevant authorities for regular interactions/ discussions on the IT security matters shall be maintained.

13.2.5 Appropriate contacts with special interest groups or other specialist security forums and professional associations for IT security matters shall be maintained.

13.2.6 Information security shall be addressed in project management, regardless of the type of the project.

13.3 Mobile Devices & Teleworking:-

13.3.1 To ensure the security of teleworking and use of mobile devices.

13.3.2 Procedures and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

13.3.3 Procedures and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

13.4 Human Resource Security (Prior to Employment):-

13.4.1 To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered.

13.4.2 Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

13.4.3 The agreements with employees and/or contractors shall state their and the Corporation's responsibilities for information security.

13.5 Human Resource Security (During Employment):-

13.5.1 To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

13.5.2 Management shall require all employees and contractors to comply information security in accordance with the established policies and procedures of the Corporation.

13.5.3 All employees of the Corporation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in the stipulated policies and procedures, as relevant for their job function.

13.5.4 There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. Necessary actions stipulated in Corporation for non-abidance of SoPs shall be adopted.

13.6 Human Resource Security (Termination or change of employment):-

13.6.1 To protect the Corporation's interests as part of the process of changing or terminating employment.

13.6.2 Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

13.7 Asset Management:-

13.7.1 To identify Corporation's assets and define appropriate protection responsibilities.

13.7.2 Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

13.7.3 Assets maintained in the inventory shall be owned. The owner of the assets shall be the official to whom the concerned asset has been issued.

13.7.4 Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

13.7.5 All employees and external party users shall return all of the Corporation's assets in their possession upon termination of their employment, contract or agreement.

13.8 Information Classification:-

13.8.1 To ensure that information receives an appropriate level of protection in accordance with its importance to the Corporation.

13.8.2 Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

13.8.3 An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the Corporation.

13.8.4 Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the Corporation.

13.9 Media Handling:-

13.9.1 To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

13.9.2 Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the Corporation.

13.9.3 Media shall be disposed of securely when no longer required, using formal procedures.

13.9.4 Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

13.10 Access Control:-

13.10.1 To limit access to information and information processing facilities.

13.10.2 Access control procedures shall be established, documented, and reviewed based on business and security requirements.

13.10.3 Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

13.11 User Access Management: -

13.11.1 To ensure authorized user access and to prevent unauthorized access to systems and services.

13.11.2 A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

13.11.3 A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

13.11.4 The allocation and use of privileged access rights shall be restricted and controlled.

13.11.5 The allocation of secret authentication information shall be controlled through a formal management process.

13.11.6 Asset owners shall review users' access rights at regular intervals.

13.11.7 The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

13.12 User responsibilities:-

13.12.1 To make users accountable for safeguarding their authentication information.

13.12.2 Users shall be required to follow the Corporation's practices in the use of secret authentication information.

13.13 System & application access control:-

13.13.1 To prevent unauthorized access to systems and applications.

13.13.2 Access to information and application system functions shall be restricted in accordance with the access control procedures.

13.13.3 Where required by the access control procedures, access to systems and applications shall be controlled by a secure log-on procedure.

13.13.4 Password management systems shall be interactive and shall ensure quality passwords.

13.13.5 The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

13.13.6 Access to program source code shall be restricted.

13.14 Cryptography:-

13.14.1 To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

13.14.2 Procedures on the use of cryptographic controls for protection of information shall be developed and implemented.

13.14.3 Procedures on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

13.15 Physical & Environmental security: -

13.15.1 To prevent unauthorized physical access, damage and interference to the Corporation's information and information processing facilities.

13.15.2 Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information or information processing facilities.

13.15.3 Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

13.15.4 Physical security for offices, rooms and facilities shall be designed and applied.

13.15.5 Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

13.15.6 Procedures for working in secure areas shall be designed and applied.

13.15.7 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

13.16 Equipment:-

13.16.1 To prevent loss, damage, theft or compromise of assets and interruption to the Corporation's operations.

13.16.2 Information critical equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

13.16.3 Information critical equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

13.16.4 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

13.16.5 Equipment shall be correctly maintained to ensure its continued availability and integrity.

13.16.6 Equipment, information or software shall not be taken off-site without prior authorization.

13.16.7 Security shall be applied to off-site assets taking into account the different risks of working outside the Corporation's premises.

13.16.8 All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

13.16.9 Users shall ensure that unattended equipment has appropriate protection.

13.16.10 Clear desk procedures for papers and removable storage media and a clear screen procedure for information processing facilities shall be adopted.

13.17 Operations Security: -

13.17.1 To ensure correct and secure operations of information processing facilities.

13.17.2 Operating procedures shall be documented and made available to all users.

13.17.3 Changes to the Corporation, business processes, information processing facilities and systems that affect information security shall be controlled.

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

13.17.5 Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

13.18 Protection from malware:-

13.18.1 To ensure that information and information processing facilities are protected against malware.

13.18.2 Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

13.19 Backup:-

13.19.1 To protect against loss of data.

13.19.2 Backup copies of information, software and system images shall be taken and tested at regular intervals.

13.20 Logging & Monitoring:-

13.20.1 To record events and generate evidence of the critical events.

13.20.2 Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

13.20.3 Logging facilities and log information shall be protected against tampering and unauthorized access.

13.20.4 System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

13.20.5 The clocks of all relevant information processing systems within Corporation or security domain shall be synchronized to a single reference time source.

13.21 Installation of software on operational systems:-

13.21.1 To ensure the integrity of operational systems.

13.21.2 Procedures shall be implemented to control the installation of software on operational systems.

13.22 Technical vulnerability management:-

13.22.1 To prevent exploitation of technical vulnerabilities.

13.22.2 Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the Corporation’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

13.22.3 Rules governing the installation of software by users shall be established and implemented.

13.23 Information systems audit considerations: -

13.23.1 To minimize the impact of audit activities on operational systems.

13.23.2 Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

13.24 Communication security:-

13.24.1 To ensure the protection of information in networks and its supporting information processing facilities.

13.24.2 Networks shall be managed and controlled to protect information in systems and applications.

13.24.3 Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

13.24.4 Groups of information services, users and information systems shall be segregated on networks.

13.25 Information transfer:-

13.25.1 To maintain the security of information transferred within Corporation and with any external entity.

13.25.2 Formal transfer procedures and controls (such as secure medium of transfer and encryption used) shall be in place to protect the transfer of information through the use of all types of communication facilities.

13.25.3 Agreements shall address the secure transfer of business information between the Corporation and external parties.

13.25.4 Information involved in electronic messaging shall be appropriately protected.

13.25.5 Requirements for confidentiality or non-disclosure agreements reflecting the Corporation’s needs for the protection of information shall be identified, regularly reviewed and documented.

13.26 System acquisition, development & maintenance:-

13.26.1 To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

13.26.2 The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

13.26.3 Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

13.26.4 Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

13.27 Security in development & support process: -

13.27.1 To ensure that information security is designed and implemented within the development lifecycle of information systems.

13.27.2 Rules for the development of software and systems shall be established and applied to developments within the Corporation.

13.27.3 Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on Corporation’s operations or security.

13.27.4 Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

13.27.5 Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

13.27.6 Corporation shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. Testing of security functionality shall be carried out during development.

13.27.7 Corporation shall supervise and monitor the activity of outsourced system development.

13.27.8 Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

13.28 Test data:-

To ensure the protection of data used for testing. Test data shall be selected carefully, protected and controlled.

13.29 Supplier relationship:-

13.29.1 To ensure protection of the Corporation’s assets that is accessible by suppliers.

13.29.2 Information security requirements for mitigating the risks associated with supplier’s access to the Corporation’s assets shall be agreed with the supplier and documented.

13.29.3 All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the Corporation’s information.

13.29.4 Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

13.30 Supplier service delivery management:-

13.30.1 To maintain an agreed level of information security and service delivery in line with supplier agreements. Corporation shall regularly monitor, review and audit supplier service delivery.

13.30.2 Changes to the provision of services by suppliers, including maintaining and improving existing information security procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

13.30.3 Contract Agreement with the outsource vendor shall include the clause for the Security Audit of the related IT infrastructure of the outsourced vendor. Outsource vendor shall conduct the Security Audit by the Cert-In empallended vendor on annual basis and submit the report to the corporation.

13.31 Information security incident management:-

13.31.1 To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

13.31.2 Responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

13.31.3 Information security events shall be reported through appropriate management channels as quickly as possible.

13.31.4 Employees and contractors using the Corporation’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

13.31.5 Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. Information security incidents shall be responded to in accordance with the documented procedures.

13.31.6 Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

13.31.7 Corporation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

13.32 **Information security aspects of business continuity management:-**

13.32.1 Information security continuity shall be embedded in the Corporation's business continuity management systems.

13.32.2 Corporation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

13.32.3 Corporation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

13.32.4 Corporation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

13.33 **Redundancies:-**

To ensure availability of information processing facilities. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

13.34 **Compliance with legal requirements:-**

13.34.1 To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

13.34.2 All relevant legislative statutory, regulatory, contractual requirements and the Corporation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system.

13.34.3 Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

13.34.4 Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

13.34.5 Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations. To ensure that information security is implemented and operated in accordance with the Corporation’s policies and procedures.

13.34.6 Corporation’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

13.34.7 Compliance of information processing and procedures shall be ensured by the officials within their area of responsibility with the appropriate security policies, standards and any other security requirements. Information systems shall be regularly reviewed for compliance with the Corporation’s information security policies and standards.

14. In order to comply to the above detailed control mechanisms as per ISO 27001 standards, the SoPs are attached as **Annexures.**

Group General Manager (System)

Copy to:-

1. All employees, through e-Office dashboard for compliance.
2. All software vendors.
3. MIS Division’s circulars on website.

Table of Contents

Annexures

1. Title: SOP for Access Control Management

All possible logical access paths to the information and computing resources of CWC must be controlled to prevent, detect, and minimize the effects of unintended or unauthorized access. Access control must be established by imposing standards for protection at the Operating System level, the Application level and at the Database level.

1.1 User Access Management

Users should be granted access to the IT resources through unique user identification (user ID e.g., the employee code), wherever feasible.

1.2 User Credentials

User credentials consist of a user ID and password or may consist of other credential (such as digital certificates, token, biometric etc.) that is unique to an individual.

1.3 User Access Management

1.3.1 CWC employees or third parties that need access to information systems and/or resources to perform their job role shall be granted appropriate access on need basis post head of department’s approval.

1.3.2 Before giving access of information systems to any party, a declaration must be signed with them and he/she shall have CWC’s security requirements communicated to them.

1.3.3 Users will be assigned a unique identifier (User ID) meant for their personal and sole use so that his / her activities can subsequently be traced to ascertain responsibility for actions or in case of any system misuse.

1.3.4 Users shall be responsible for all activities performed with their unique official user-ids. They should not allow others to perform any activity with their user-ids.

1.3.5 User IDs or passwords shall not be shared amongst employees.

1.3.6 A formal record of all persons granted access to critical information systems/ restricted zones will be maintained by each systems administrator and kept up to date.

1.3.7 In case of user de-registration, de-registration of the users shall be performed from all the systems and applications.

1.4 User Privilege Management

1.4.1 Privileges will be allocated to individuals on a need-to-know and need-to-use basis.

1.4.2 Users will be provided the minimum privilege required to perform his task.

1.4.3 In case the user having privileged access leaves the CWC, all privileged account passwords (known to him/her) shall be changed, and privileged access rights should be revoked on immediate basis.

1.4.4 Privilege access shall be approved by head of department.

1.4.5 Privilege access shall be time bound and same shall be revoked/reauthorized on the completion granted timeline.

1.4.6 All administrators should have a separate user account for such privilege work; they should not use such account for their normal day-to-day work.

1.4.7 The default administrator account passwords of all systems should be changed every quarter and kept in a sealed envelope / Secured vault solution with the IT Infra Head.

1.4.8 A record of all privileges allocated will be made through an “Access Control Matrix”.

1.4.9 All activities related to privileged users will be logged and reviewed every month to detect any misuse of privileges.

1.5 Sharing of User IDs

Common user IDs should not be used unless they are absolutely essential. Common user IDs should not be issued to multiple users when it is technically feasible to provide individual IDs.

1.6 Sharing of User IDs

Efforts must be made for only one user ID common across multiple systems and applications for a single user. Sharing of user ID should be strictly prohibited.

1.7 Control of User ID

1.7.1 Users must not be allowed to log on simultaneously from more than one PC in to the same application.

1.7.2 User accounts that are inactive for more than 15 days are to be disabled automatically wherever possible.

1.7.3 Application Owner or IT Head should re-enable it only on the request of the specific user.

1.7.4 In case a user is going on leave for a period of more than 30 days, then the user should ensure that the User ID is disabled for the period of absence.

1.7.5 **System to notify user of last login/logout** :- Where appropriate, upon login, the user should be presented with date and time of last login and logout, if possible, along with contact information to report any discrepancy.

1.8 Monitoring User activities

1.8.1 The Operating Systems and applications should log all user activities. These logs should be reviewed on a pre-defined interval.

1.8.2 All unusual activities should be noted and investigated.

1.8.3 New User IDs are to be monitored for a reasonable period to ensure that the access given is not used with malicious intent or that changes to data have not been made by mistake due to inexperience on the part of the user.

1.9 User Access Rights Review

1.9.1 User list is to be reviewed periodically.

1.9.2 All unused and old user accounts shall be deleted / disabled.

1.9.3 Access shall be given on a need-to-know basis (Minimum rights required for a user to access resources that he wants).

1.9.4 User Access rights shall be reviewed periodically by Concerned HOD/RM or any official authorized by them and shall be revoked if warranted.

1.10 Management of Secret Authentication Information of Users

1.10.1 Users shall sign confidentiality agreement to keep all the confidential information secured including all the passwords shared with them.

1.10.2 Secret authentication information shall share in secured manner, if possible, in-person.

1.10.3 Secret authentication information shall be changed on first login.

1.10.4 Default vendor secret authentication information should be altered following installation of systems or software.

1.11 Access Control to Program Source Code

1.11.1 Program source code should be accessible to limited personnel only.

1.11.2 Access to source code shall be reviewed on quarterly basis.

1.11.3 Wherever feasible, for the critical applications, either source code must be received from the vendor or a software escrow agreement needs to be in place with a third party to ensure source code availability in case the vendor goes out of business.

1.11.4 Any changes in the source code shall be logged.

1.11.5 Version of changes shall be maintained.

1.12 Use of secret authentication information

1.12.1 Users should be required to follow the CWC's practices in the use of secret authentication information.

1.12.2 Users should keep secret authentication information confidential, ensuring that it is not divulged to any other parties.

1.12.3 Users should change secret authentication information whenever there is any indication of its possible compromise.

1.12.4 Users should not share individual user's secret authentication information.

1.12.5 Users should not use the same secret authentication information for business and non-business purposes.

1.13 Secure log-on Procedures

1.13.1 All operating systems shall be configured such that they should not display the username of the last user logged in.

1.13.2 log unsuccessful and successful attempts.

1.13.3 not display a password being entered.

1.13.4 Session time out shall be enabled.

1.14 Use of System Utilities

1.14.1 Restricting Users with privileged access to the OS

1.14.2 Removing / Disabling such system utilities if not required

1.14.3 Document the ports used to diagnose and configure systems.

1.14.4 Secure the physical and logical access to ports used to diagnose and configure systems.

1.14.5 Disable the physical and logical access to ports used to diagnose and configure systems when not in use.

1.14.6 Only privileged personnel in the IT Infrastructure & IT Security Teams shall be given access to system utilities.

2. Title: SOP for Acceptable Usage Change Management

2.1 Acceptable use of Communication Facilities (Internet, Email)

Internet access to the employees should be provided as per need to know basis and authorized by the MIS division through a formal process.

2.1.1 Users must use these services for business/official purpose only. Users should be made aware that their usage activities are be monitored.

2.1.2 Users shall not try to alter the browser settings.

2.1.3 Users should scan the attachments received by emails before opening them.

2.1.4 Users shall not post any information proprietary to CWC on public forums, such as chat rooms and discussion rooms, on the Internet.

2.1.5 Abuse of Internet access for sexual, ethnic and / or racial harassment is prohibited.

2.1.6 All information downloaded from the Internet is considered suspect until confirmed by information from another source.

2.1.7 Users shall confirm the identity of individuals, over the Internet, through approved methods.

2.1.8 Internet sites which might contain profane, obscene and any other material which is not connected to work shall not be accessed.

2.1.9 Users shall not download and install software including screensavers, wallpapers, instant messengers, games and other applications from the Internet.

2.1.10 All files downloaded from the Internet shall be checked for malicious code and other bugs before usage.

2.1.11 Users shall not send any confidential information through the Internet unless authorized.

2.1.12 Users on receipt of information about system vulnerabilities, actual or suspected (hoaxes), users shall inform relevant authority for necessary action.

2.1.13 Users should not share/register their official email ID, unless justified, in subscription sites, blogs and other websites in order to avoid spam/bulk mails.

2.1.14 While sending mails internally to a group of people, users shall avoid sending bulk attachments (like personal photos, etc.).

2.1.15 While sending sensitive information users should double check the recipients' name and use appropriate secure email standards

2.2 Acceptable Usage of Assets

2.2.1 Users must be aware of their roles and responsibilities of using the assets. They must use them for business purpose only.

2.2.2 Users shall not try to experiment with the existing settings, existing access controls or set-up of the information assets.

2.2.3 Users shall return all the assets allocated to them by the CWC.

2.2.4 Users shall be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

2.2.5 Users shall be responsible for any non-compliant activities on the assets allocated to them.

2.3 Acceptable Usage for Mobile computing devices

2.3.1 Users shall adhere to Mobile device usage procedures document.

2.3.2 Users shall not leave the mobile devices unattended without screen lock and physically fastened (in case of a laptop).

2.3.3 Users must avoid using CWC’s mobile devices at public or crowded places (like airport, railway station, etc.) and shall safeguard them.

2.3.4 Users must not connect external devices or try to transfer CWC’s data from the mobile devices without approvals.

2.3.5 Users must ensure that their devices have an updated antivirus.

2.4 Acceptable Usage of Access Control

Logical Access:

2.4.1 All users shall use their unique ID assigned to them for accessing CWC’s informational assets.

2.4.2 All users should ensure that access to any information asset or IT service should be obtained after adequate approval from management.

2.4.3 Users shall not share any of their authentication credentials with other person under any circumstances.

2.4.4 Users shall not write or paste passwords in public spaces like desk or stick it near workspace.

Physical Access:

2.4.5 Users shall wear a visible identification (badge) while within the CWC’s premises.

2.4.6 All staffs, vendors and visitors need to cooperate with the CWC’s security checks and access formalities. Users must enter into all information processing facilities within the CWC after authenticating themselves at the physical access control unit.

2.4.7 Users should be aware of procedures to report any lost or stolen item assigned to them (ex. Laptop, access card, etc.)

3. Title: SOP for Asset Management

3.1 Asset Inventory

3.1.1 All information assets shall be maintained in the Asset inventory.

3.1.2 Assets will be maintained with the description of the assets, custodian of the assets and owner of the assets

3.1.3 All physical assets must have an ID/Serial number. Either an internal tracking number will be assigned when the asset is acquired, or the Manufacturer ID numbers shall be used.

3.1.4 When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset register.

3.1.5 Asset's criticality shall be determined based on Confidentiality, Integrity and Availability.

3.1.6 Assets shall be classified on the basis of criticality.

3.1.7 Critical assets would be identified.

3.2 Asset Register

The asset register documents the information assets of a business function.

3.3 Asset Owner

3.3.1 Asset owners shall ensure that their assets are included in the asset inventory.

3.3.2 Asset owners shall ensure that their assets are classified.

3.3.3 Asset owners shall ensure proper handling of the assets.

3.4 Asset Tagging

To identify invent-arable assets as belonging to the Corporation. All physical assets will be tagged.

3.5 Return of Asset

All employees and external party users should return all the CWC's assets in their possession upon termination of their employment, contract or agreement.

3.6 Information Classification

Information shall be classified as per following Information Classification scheme -

3.6.1 **Public Information** that is available to the general public and intended for distribution outside Corporation such as Contents on CWC website, financial statements of organisation.

3.6.2 **Internal Information** that is deemed sensitive due to financial or legal ramifications and which is for use only by authorized corporation employees and auditors, supplier personnel, legal and regulatory authorities. Example includes IS policies & SOPs etc.,

3.6.3 **Confidential Information** that is proprietary to the Corporation and its unauthorized disclosure could adversely impact the corporation, its employees and its customers. Example includes Legal Agreements, Some confidential approvals, Customer Confidential Information and Technical documents (Design) etc.

3.6.4 **Secret is information** for which unauthorized disclosure (even within the Corporation) would cause serious damage to the interests of Corporation. It would normally inflict harm by virtue of serious financial loss, severe loss of profitability or opportunity, or loss of reputation. Example includes Board papers, Cost estimates and price bids etc.

3.7 Information Labelling

3.7.1 Information shall be labelled as per the classification.

3.7.2 All the confidential labelled information shall be handling with utmost care.

3.8 Asset Disposal

3.8.1 Assets shall always be disposed in secure manner to ensure that data has been wiped out completely.

3.8.2 The user of the asset must determine what level of maximum sensitivity of data is stored on the device like hard disk drives and below is listed the action for the device based on data sensitivity according to the data assessment process.

3.8.2.1 Public - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.

3.8.2.2 Internal - Erase the data using any means such as reformatting or degaussing.

3.8.2.3 Confidential - The data must be erased with an approval from the data owner/IT Manager to make sure it is not readable/reusable. All the paper-based confidential data shall be shredded.

3.8.2.4 Secret - The data must be erased done by the data owner to make sure in such manner that it is not readable/reusable. All the paper-based secret data shall be shredded.

4. Title: SOP for Back-up and Recovery

The Backup & Recovery procedures provides the directions to maintain the confidentiality and availability of information and information processing facilities. The SoP intends to ensure backups of critical information are taken and can be relied up on in case of eventualities

4.1 Backup Procedures

4.1.1 The number of backup sets to be maintained should be decided by MIS Division.

4.1.2 A list of all the data files for critical applications should be maintained by the System Custodians along with a brief description of the contents of those files.

4.1.3 In addition to the scheduled backups, backups should be taken in case any of the following events occurs

4.1.3.1 Configuration change

4.1.3.2 Upgrade of an operational system

4.1.3.3 Replacement of systems

4.1.3.4 At the time of archival

4.1.4 All identified systems level and user level shall be backed up as per backup schedule guideline.

4.1.5 CWC Information with the service providers shall be backed up as per the General Conditions of Contract and terms and conditions of the agreement.

4.1.6 The backup media shall be stored with sufficient protection and proper environmental conditions.

4.1.7 To confirm media reliability and information integrity, the back-up information shall be tested at some specified frequency.

4.1.8 Backup information shall be selectively used to restore information system functions as a part of business continuity process.

4.1.9 Backup copies of operating systems and other critical information system software shall not be stored in the same location as the active server room.

4.1.10 The system backup information shall be provided with protection from unauthorized modification and environmental conditions.

4.2 Backup Schedule & Retention

4.2.1 The schedule of backup and the period of retention shall be decided based on the criticality of the information being backed up

4.2.2 The data shall also be backed up at the time of a version upgrade or any major change.

4.2.3 Appropriate media shall be used to take backups.

4.2.4 The media shall be phased out periodically, in line with the media manufacturers' recommendations. Re-use of media, under no circumstances, shall be carried out after the life of the media.

4.2.5 Disposal of backup media shall be carried out in a secure manner, in line with the type of media being disposed.

4.3 Information to be backed up

4.3.1 Information contained in business applications (data and program files) and Operating systems residing on the servers as decided by MIS division shall be backed up.

4.3.1.1 Data & information residing in the concerned business application shall be owned by the users of the applications.

4.3.1.2 The concerned asset owner (to whom the asset has been issued) of the business critical data on Workstations and mobile computing devices shall ensure the backup & security of the information.

4.3.1.3 Network device configuration files

4.3.1.4 Logs and audit trails

4.3.1.5 Active Directory

4.4 Backup logs

4.4.1 The backup logs maintained by the Systems Custodians should either be manual registers or the reports generated by the system (operating systems or the applications), which should be kept handy.

4.4.2 The Systems Custodians should maintain the backup movement logs for the backups at off-site location.

4.5 Backup Restoration

4.5.1 To verify the readability of backup media, mock restoration tests should be carried out periodically depending upon the criticality of the application or as per schedule defined. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

4.5.2 Log is to be maintained by the Systems Custodian, containing date and time along with name and signature of the person who requested for the restoration of the data. The log also includes number of backup media used for restoration.

4.5.3 Backup data shall be tested (restored) on a periodic basis

4.5.4 Occasionally offsite backups should be used for testing restoration.

4.5.5 Upon restoring the data on the test server, the results should be documented. At end of the restoration exercise, a second level officer must verify these test results. The data restored is deleted from the test server after successful completion of the exercise.

4.6 Data Archival

4.6.1 Data needs to be archived as per the policies/regulatory/statutory requirements. Archived data shall be retained in appropriate media so as to ensure the integrity of the data

4.6.2 The access to the archived data shall be controlled with appropriate access right.

4.6.3 The archival media and contents shall be tested periodically to ensure the quality and usability of the same.

4.6.4 Training shall be provided for the restoration of the data.

4.7 Data Purging

4.7.1 Purging of data shall be taken up on retirement of data after it has met the requirements of legal/regulatory/statutory compliance.

4.7.2 Appropriate media sanitization methods should be adopted for the purging of data.

4.7.3 The purging of the data shall be controlled and shall not be outsourced. All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

5. Title: SOP for Capacity Management

This SoP aims at establishing procedures to ensure that the capacity of IT infrastructure and IT services is able to deliver the agreed service level targets to the CWC, in a timely and cost effective manner.

5.1 Capacity Monitoring

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

5.1.2 Resources with long procurement lead times or high costs should be identified. Utilization of such key system resources should be monitored.

5.1.3 The trends in in usage, particularly in relation to business applications or information systems management tools shall be identified.

5.1.4 Use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

5.1.5 All servers, network and devices should be monitored for their usage and performance. Following parameters should be checked at a minimum;

5.1.5.1 CPU utilization

5.1.5.2 Hard disk utilization

5.1.5.3 Memory utilization

5.1.5.4 Network devices;

5.1.5.5 Uptime

5.1.5.6 Bandwidth utilization

5.1.5.7 CPU utilization

5.1.5.8 Memory utilization

5.1.6 Performance and up time reports should be generated periodically and analyzed. These reports along with trend analysis should be used in capacity planning.

5.1.7 Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. Examples of managing capacity demand include:

5.1.7.1 Deletion of obsolete data (disk space);

5.1.7.2 Decommissioning of applications, systems, databases or environments;

5.1.7.3 Optimizing batch processes and schedules;

5.1.7.4 Optimizing application logic or database queries;

5.1.7.5 Denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

6. Title: SOP for Change Management

Changes to the system are essentially of two kinds: scheduled and unscheduled. Scheduled changes are changes that are planned and carried out in a systematic manner. Unscheduled changes shall generally be avoided but shall be carried out only in case they are required to ensure proper working of the production environment. Changes if not carried out in a secure manner, may affect the live/ production environment in an adverse manner.

6.1 Scheduled Changes

6.1.1 Various kinds of changes to the system shall be identified and classified.

6.1.2 The procedure, that will be carried out, during the change must be documented and evaluated for security aspects and approved by the relevant authority before being carried out.

6.1.3 All changes are to be tested and there shall be a system acceptance procedure before being carried out in the live/ production environment.

6.1.4 A roll back procedure shall be defined, documented and approved before any changes are carried out.

6.1.5 All changes must be scheduled and all the affected parties are to be informed in advance of the change.

6.1.6 All changes have to be reviewed after the roll out and approved after successful reviewing.

6.1.7 A log of all changes shall be maintained for record and audit purposes.

6.2 Unscheduled Changes

6.2.1 Unscheduled changes shall be carried out only in case there are critical production issues, which require the change to be carried out. Such changes must necessarily go through appropriate authorization procedures.

6.2.2 Back-end updates to database are not allowed. However, exceptions may be made during exigency with a clear business need and after due authorization.

6.2.3 After unscheduled changes are carried out, normal change procedures shall be followed.

6.2.4 Unscheduled changes shall be documented and reviewed subsequent to the change. Appropriate version control must also be performed on the critical files.

6.2.5 A log of all changes shall be maintained for record and audit purposes.

6.3 Impact & Assessment

Impact and risk assessment shall be performed for all types of changes.

6.4 Records of Changes

Records of changes must be maintained on email or automated tool. Any kind of changes related to system; application shall be approved by the authorized person.

7. Title: SOP for Clear Screen and Clear Desk

7.1 Clear Screen Procedures and Guidelines

7.1.1 When away from place of work, laptop/desktop user shall ensure that the system is locked. Locking computer screen not only prevents someone else from using that PC, which is already logged on, but it also prevents someone from reading confidential information left open on the screen.

7.1.2 All desktop and laptop screen shall be configured to lock out when inactive beyond a threshold limit of a defined number of minutes of inactivity.

7.1.3 If working on sensitive information, and you have a visitor to your desk, lock the screen to prevent the contents being read.

7.2 Clean Desk Procedures and Guidelines

7.2.1 All employees at CWC shall be responsible for ensuring important business information in their custody (both paper and digital media) are kept securely and are inaccessible to unauthorized access until their disposal.

7.2.2 At the end of each day, or when desks/offices are unoccupied, any 'confidential' information must be locked away in filing cabinets or offices, as appropriate. The key to the filing cabinets or offices, as appropriate should be maintained securely at all times.

7.2.3 All waste paper, which has any personal or confidential information or data, must be torn properly or shredded. Sensitive documents that are no longer needed must be disposed securely. It is recommended to use a paper shredder for this purpose.

7.2.4 All business documents including digital media such as CDs and DVDs etc. shall be secured in locked cabinets when not in use or when left unattended, especially after working hours.

7.2.5 CDs / DVDs with information that are not required by the user must be shredded.

7.2.6 Confidential and Restricted information, when printed, shall be cleared from printers immediately.

7.2.7 All fax machines and printers shall be protected from unauthorized access.

7.2.8 When transmitting sensitive facsimile message, users are advised to inform the recipient of the facsimile first before transmission.

7.2.9 When receiving sensitive facsimile message users must be physically present to receive the same.

7.2.10 Users must not leave such papers unattended on printer trays, photocopiers, fax machines or their desks. Users must collect the printouts from the printer trays promptly.

7.2.11 Portable devices such as laptops, mobiles or PDAs shall not be left unattended and shall be locked when not in use.

7.2.12 Users must ensure the confidentiality and integrity of information that they deal with or is made available to them in day-to-day operations.

8. Title: SOP for Cryptography

8.1 Data Encryption

8.1.1 CWC shall incorporate cryptographic controls to achieve the following information security objectives:

8.1.1.1 Confidentiality of sensitive or critical information, either stored or transmitted

8.1.1.2 Integrity/Authenticity of stored or transmitted sensitive or critical information

8.1.1.3 Non repudiation of occurrence/non-occurrence of an event or action

8.1.1.4 Secure Authentication of users and other system entities

8.1.1.5 Data over third-party networks - Any data traveling over third-party networks and communication backbone must be encrypted wherever possible.

8.2 Encryption of confidential/restricted information

8.2.1 Confidential/restricted information transmitted over any communication network must be sent in an encrypted form.

8.2.2 Confidential information not being actively used, when stored or transported in computer-readable storage media (such as servers, magnetic tapes, floppy disks or CDs), must be in encrypted form wherever possible.

8.2.3 To prevent unauthorized disclosure of data when computers are sent out for repair or used by personnel, other than the normal users within or outside the Corporation, all data stored on hard disks must be encrypted.

8.2.4 The strength of the encryption algorithm to be used in a given situation must be based on the classification of the data to be encrypted.

8.2.5 Certifying Authority - CWC shall use only those Digital Certificate issued by Certifying Authorities registered with Controller of Certifying Authorities of Government of India.

8.3 Managing electronic keys

Electronic keys are used to encrypt and decrypt messages or digital signatures on messages sent between one or more parties. The management of the electronic keys is critical if confidentiality, authenticity and integrity are to be preserved. Therefore, a procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements. Information security issues to be considered when implementing a procedure include the following:

8.3.1 Digital Signature issued by licensed Certifying Authorities (CA) under Controller of Certifying Authority (CCA) should only be used.

8.3.2 Keys need to be communicated by reliable and secure methods and kept confidential.

8.3.3 If a private key becomes compromised, invalid messages could be sent which forge the identity of CWC. Such security breaches could result in substantial fraud. A process to cancel compromised keys to prevent their further use is therefore required.

8.3.4 Failure to manage the keys of the various senders of encrypted data may result in a failure to decrypt an incoming message, with potential costly delays.

8.3.5 Security risks (e.g., of damage, theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures.

8.4 <u>Using and Receiving electronic signatures</u>

When using digital signatures, consideration should be given to any relevant legislation that describes the conditions under which a digital signature is legally binding. Information security issues to be considered when implementing procedures include the following:

8.4.1 Even signed documents cannot be relied upon unless the keys being used are trustworthy.

8.4.2 Relying upon unsigned email, whilst acceptable in many circumstances, carries a risk, as source and destination fields can be readily forged.

8.4.3 Receiving email via unsecured public lines (e.g., the internet) can compromise the confidentiality and integrity of the contents.

8.4.4 Important email communications might not be authenticated, which could result in un-authorized instructions being issued.

9. Title: SOP for Compliances

9.1 Licensing

9.1.1 All information processing systems used in the CWC shall comply with the licensing terms or the agreement executed between vendor & CWC.

9.1.2 CWC may use Commercial Software, Software under the open source license and Evaluation Software.

9.1.3 Appropriate asset registers for the software shall be used in the CWC along with proof and evidence of ownership of licenses, master disks, manuals, etc. shall be maintained by the MIS Division.

9.1.4 Periodic checks shall be carried out using appropriate tools to detect unauthorized software in the Corporation.

9.1.5 CWC would not consider using Sharewares. Sharewares are software, which have validity for a limited period of time and have limited features enabled.

9.1.6 MIS Division shall use approved standards and guidelines for acquisition of software products.

9.1.7 The software products shall be purchased from authorized software vendors only.

9.1.8 The MIS Division shall maintain proof and evidence of ownership of licenses, master disks, manuals, that are being used.

9.1.9 The MIS Division shall ensure that any maximum number of users permitted is not exceeded.

9.1.10 The MIS Division shall carry out checks that only authorized software and licensed products are installed.

9.1.11 CWC shall endeavor to protect the confidentiality of personal data in compliance with the prevailing rules, regulation and laws.

10.Title: SOP for Information Classification and Handling

The Objective of this SoP to ensure proper classification of the information at CWC and to ensure appropriate level of protection of the information thus classified.

10.1 Information classification

10.1.1 CWC holds and processes various kinds of information. In order to ensure that appropriate care is taken while handling information, it is important that information be properly classified.

10.1.2 All information, irrespective of form and origin, shall be classified into “Public”, “Operational”, “Confidential” or “sensitive - Internal”.

10.1.2.1 **Public** – All information available for both internal as well as external entities“

10.1.2.2 **Operational**– All information that is generally available for all employees for the operations at CWC.

10.1.2.3 **Confidential**– intended only for certain entities in CWC including business plans, system passwords, salary information, IS Architecture details, user passwords, system documentation.

10.1.2.4 **Sensitive-** That information that is very sensitive and is available for named individuals within CWC only.

10.1.3 All forms of information shall have a designated owner. The information residing in any asset (desktop or mobile) shall be owned by the user to whom the asset has been assigned. The information resided in the business applications shall be owned by the concerned user responsible to access the information/ add or delete any information.

10.1.4 If information is not marked with one of these categories, it shall be considered “Public”.

10.1.5 Employees who update information shall classify the new collection appropriately after consulting with the designated owner of the information and any other relevant personnel.

10.1.6 Employees who create information or receive information from external sources shall classify the new collection appropriately.

10.1.7 Information shall be disclosed to only those users who have a legitimate business need to access the same.

10.1.8 The method of classification for any information shall be determined based on CWC needs.

10.2 Maintenance Process

10.2.1 Classification, declassification, storage, access, destruction and reproduction of classified data and the administrative overhead of this process shall be considered. The information classification should cover both non-electronic media (e.g.: physical documents) and electronic media (e.g.: Emails, CDROM, Tapes, Word etc.).

10.2.2 Documented records shall be maintained to track the process like time, access rights and destruction of information assets.

10.2.3 Classification of information should be reviewed by the information owner periodically, with the change in sensitivity.

10.2.4 While deciding the protection level for information, the associated legal, regulatory and statutory requirements should also be considered.

10.2.5 All document media must be physically labeled. The labeling format for both electronic and non-electronic media should be easily distinguishable and readable. Following are the recommendations for components of the labels:

10.2.5.1 Owner of information

10.2.5.2 Classification of information

10.2.5.3 Intended audience

10.2.5.4 All information for disposal should be approved and recorded.

10.3 Media Handling

10.3.1 The data storage devices and printed media at CWC shall be managed, stored and disposed of in a manner consistent with the classification of information stored, contained or printed in the media.

10.3.2 Media is anything on which information or data can be recorded or stored and includes both paper and a variety of electronic media. Storage devices include but are not limited to: computer hard drives, portable hard drives, backup tapes, DVD / CD media, USB drives and other Personal Digital Assistants (PDA), cell phones, iPods, MP3 players, digital cameras, fax machines, and photocopiers.

10.3.3 When handling and managing information it is essential to understand that maintaining security for both the information and the media on which it is stored is equally important.

10.3.4 This SoP offers guidance regarding media handling. It is intended to guide and inform relevant CWC personnel and help them understand their roles and responsibilities according to the procedures.

10.3.5 The primary area of concern is secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse throughout its life cycle.

10.3.6 Erasure of information from media and disposal of media shall be done by approved standards and using documented procedures.

10.3.7 Media shall be handled according to the highest level of sensitivity of contained information.

10.3.8 Media shall be protected from theft or tampering.

10.3.9 Where there is re-assignment or destruction of hardware and media, inventory records shall be kept current.

11.Title: SOP for Incident Management

11.1 Incident Severity Classification

11.1.1 All incidents shall be classified into appropriate levels based on their severity. Incidents could be classified into level 1, level 2 and level 3.

11.1.1.1 **Level 1** incidents are incidents, which if not resolved, could affect the functioning of the entire Corporation for over 1 hour.

11.1.1.2 **Level 2** incidents are incidents, which if not resolved, could affect the functioning of some of the branches for over 1 hour of CWC or could affect the entire Corporation after a period of say 1 day.

11.1.1.3 **Level 3** incidents are those incidents that do not directly affect the functioning of CWC immediately. Level 3 incidents may or may not affect the functioning of CWC or a part of it, if not resolved within say 2 days.

11.2 Cyber Security Incident

11.2.1 Cyber Risk represent the possibility that technologies, processes and practices at the CWC can be compromised, allowed unauthorized users to (Including but not limited to)

11.2.1.1 Modify and /or delete key applications and information which will affect the accuracy or integrity of processing

11.2.1.2 Access or extract protected or sensitive information (e.g., Intellectual Property- IP, Personally Identifiable Information- PII)

11.2.1.3 Disrupt computer-controlled operation or access to online system.

11.2.2 In response to the cyber-attack, CWC shall protect IT assets from cyber-attacks and respond to any cyber threat and attacks in timely and appropriate manner to ensure confidentiality, integrity and availability of data. CWC shall take steps to access the incident impact and take appropriate response measures including escalation to relevant authorities.

11.3 Reporting

11.3.1 There shall be a centralized reporting mechanism (MIS Division, CO) for reporting any incident, and this must be made known to all relevant staff at CWC.

11.3.2 All employees and contractors shall promptly report any incident, suspected and actual, through the centralized reporting mechanism.

11.3.3 Any information security vulnerability, if known to exist, shall be reported to the authorities concerned.

11.3.4 Suspected computer virus attacks shall be immediately reported to the authorities concerned.

11.3.5 Wherever relevant, information regarding incidents (Including Cyber Security Breach/Cyber Attack) shall be sent to external regulatory bodies, which may include:

11.3.5.1 Cyber Cell of Police.

11.3.5.2 CERT-IN/Forensic Experts.

11.3.5.3 Any other relevant institutions.

11.4 Incident Handling

11.4.1 An incident escalation matrix, detailing external and internal escalation points, shall be defined for the various incident classes.

11.4.2 Incidents are to be handled based on the severity levels and shall be escalated if not resolved within appropriate time limits.

11.4.3 A thorough investigation shall be conducted if a computer crime is committed, to prevent recurrence of such incidents.

11.4.4 The cybercrime or incidents related to frauds such as impersonation, virus attacks, financial frauds through e-media, ransomware attach, un-wanted activity of user's account in any e-Tool etc., shall be reported to MIS Division, CO. Wherever necessary, the fraud/ crime shall be reported to cyber crime portal/ cyber cell of local police including other preventive measures such as blocking/reporting the un-wanted activities on various platforms.

11.5 Logging of Incidents

11.5.1 All incidents shall be logged and relevant information captured including resolution shall also be documented for future references. Changes/Customization, if any, in the software shall be identified and classified.

11.5.2 All incident logs shall be reviewed periodically to prevent and/ or better handle similar incidents in the future.

11.6 Learning from information security incidents

11.6.1 Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

11.6.2 The incident management team shall maintain records and details of all the incidents captured considering the types, volumes and costs of information security incidents (business impacts).

11.6.3 Recurring incidents shall be analysed to indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences.

11.7 Collection of evidence

11.7.1 CWC shall identify, collect, acquire and preserve all incident related information, which can serve as evidence for the purposes of disciplinary and legal action.

11.7.2 Forensic evidence may transcend jurisdictional boundaries. In all such cases, CWC shall endeavor to collect & collate the information available/ associated with the incidence.

12.Title: SOP for Mobile Device and Teleworking

12.1 Mobile Devices usage procedures

12.1.1 Asset owner shall ensure that OEM patches (such as patches released by android or iOS) are installed and are up to date.

12.1.2 Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas.

12.1.3 Email Access on mobile phones/tablets will only be provided after the proper approval and Authorization

12.1.4 Pay attention when granting permissions while installing an application

12.1.4.1 Permissions for your device's camera, microphone, contact list, call logs, SMS or other sensitive areas of your phone

12.1.4.2 Permission for special accesses like ‘Display over other apps’, ‘Modify System settings’, ‘Notification access’, ‘Picture-in-picture’, ‘Premium SMS access’, ‘Install unknown apps

12.1.5 Avoid using open or public Wi-Fi

12.1.6 Update your mobile operating system regularly

12.1.7 Update mobile device software and mobile apps, only from AppStore and PlayStore

12.1.8 Do not allow installation of any applications from unknown/untrusted sources

12.1.9 Keep a practice of uninstalling all the unused applications

12.1.10 Cautious against using untrusted freeware applications

12.1.11 Use Security and Privacy settings on websites and applications

12.1.12 Use unique, strong passwords for every single online account or use legitimate password managers for storing passwords (If required)

12.1.13 Consider using multi-factor authentication like Biometrics authentication/face recognition/pattern for mobile phone as well as for supported applications

12.1.14 Back Up Your Phone Regularly on physical backup devices

12.1.15 Enable remote lock and data wipe on mobile phone

12.1.16 Do not jailbreak (iOS) or root (Android) the mobile device

12.1.17 Limit Public Charging, Especially USB-Based

12.2 Company Property

12.2.1 Mobile computing systems assigned to employees by the company are the property of CWC.

12.2.2 These systems have been provided by the CWC for use in conducting business

12.2.3 All data, communications and information transmitted by, received from, passing through, or stored in these systems are the CWC’s records and the exclusive property of CWC.

12.3 Teleworking Procedures

12.3.1 All Information security policies and procedures hold true in case of telework as well.

12.3.2 Due care is expected to be exercised by teleworking employees to ensure confidentiality of CWC’s information and security of its assets

12.3.3 Any compromise of Information asset shall be reported immediately.

12.3.4 Mechanism and controls such as SSL, Multi factor authentication, captcha etc. should be implemented for secure connection wherever applicable. Cloud service provider (CSPs) should be certified with valid ISO 27001 standard.

12.3.5 CWC shall regularly ensure that the teleworking team is regularly updated with latest antivirus signatures.

12.3.6 CWC shall ensure revocation of authority and access rights and the return of equipment when the teleworking activities are terminated. Asset registers shall be updated accordingly

12.4 Use of Laptops/Computers/Handheld Devices/Smart Phone

12.4.1 Employees assigned with company laptops are allowed to use the laptop computer inside and outside the company premises.

12.4.2 Company assigned laptops are to be used as a productivity tool for company related business and communications.

12.4.3 All laptops and related equipment and accessories are CWC’s property and are provided to the staff members for a period of time as deemed appropriate by the management.

12.4.4 As a condition of their use of the CWC’s laptop computers, staff members must comply with and agree to all of the following: Refer SoP for Acceptable Usage.

13.Title: SOP for Malware

13.1 Virus Prevention

13.1.1 All workstations whether connected to CWC network, or standalone, must use approved anti-virus and anti-malware software and configuration.

13.1.2 CWC shall adopt centralized Antivirus & spam detection solution configured to automatically check for new signature updates periodically.

13.1.3 Signature updates shall be done whenever there is an outbreak of a new virus and efforts shall be made to ensure new outbreaks are tracked. Users shall be trained / informed, not to modify anti-virus program settings, uninstall and/ or deactivate the anti-virus program.

13.2 Virus Detection & Removal

13.2.1 Desktops shall be automatically scanned for virus on periodic basis.

13.2.2 If a user desktop is switched off, the user shall be trained to carry out the scan manually.

13.2.3 If the virus, detected by the scanner cannot be cleaned the anti-virus software must delete the file and the same shall be informed to the user. If the virus is not cleaned, the virus-infected computers shall be removed from the network until they are verified as virus-free. Media that contain virus-infected files (which cannot be cleaned) must be formatted /destroyed.

13.2.4 Users shall report all virus related incidents to the appropriate officials.

13.3 Controls

13.3.1 Transfer of executable files through the perimeter shall be restricted. All computers in the network shall be configured to perform auto-scans for viruses. Signature updates shall be monitored.

13.3.2 The centralized antivirus server should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.

13.3.3 External media shall be scanned before connecting to network.

13.3.4 Anti-virus console logs shall be monitored to correct any systems that failed to be updated.

13.3.5 Anti-malware software and signature auto update features should be implemented to automatically update signature files and scan engines whenever the vendor publishes updates.

13.4 Restrictions on software installation

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.

13.4.1 Users are restricted to install unauthorized and unapproved software on their systems.

13.4.2 Software installed on all IT systems within the CWC shall be approved by the management. An approved list of software shall be maintained and updated by the CWC.

13.4.3 User rights and account privileges shall be controlled as per the roles and requirements of the users to ensure that installation or upgradation of software does not open security risks to the CWC’s IT environment.

14.Title: SOP for Patch Management

14.1 Patch Testing

14.1.1 All patches should be tested thoroughly in the test bed prior to release into the production systems.

14.1.2 Appropriate change request should be raised for rolling out the patches in production environment. Hence, it mandates that for all critical central applications CWC should have a development, Test and production environment, which should be all separate.

14.1.3 All Critical and important security patches (Critical & High) would be patched within 60 days of the release of the patch. Moderate and Low Security Patches (Medium and Low) would be patched within 365 days of the release of the patch. Any time bound patches released by OEMs or security agencies would be patched immediately.

14.2 Patch Testing Procedure

14.2.1 **Applications/ Operating Systems: -** The followings should be followed to ensure proper patch testing has been completed before rolling out the same patches to production environment.

14.2.1.1 Once new application patches has been released by the OEM vendor it should be notified to the application owner and System/Application Custodian.

14.2.1.2 Thorough impact assessment towards the security of the concerned applications is to be done.

14.2.1.3 The application custodian should test the patches in the test environment and monitor the performance of the servers for some time.

14.2.1.4 The Asset custodian should also prepare a roll back plan, which should be executed in case the patch deployment fails or causes application breakdown.

14.2.1.5 Once it is confirmed that the patch deployment in test environment is successful and does not cause application breakdown, the same set of patches are to be deployed in the respective DR Set up and then to the production system.

14.2.2 **Network Devices - The followings should be followed to ensure proper patch testing has been** completed before rolling out the same patches to production environment.

14.2.2.1 Once a new patch for the network device operating system has been released by the OEM vendor, it should be analyzed to identify the impact of the patch on all devices used by the CWC.

14.2.2.2 A thorough impact assessment towards the security of the concerned devices should be done.

14.2.2.3 A change request should be raised for rollout to DR Setup and production environment.

14.2.2.4 The network administrators should test the patches in the DR Setup stand-by devices and observe the impact of patches on the devices for 1 week.

14.2.2.5 The Asset custodian should prepare a roll back plan, which should be executed in case the patch deployment fails or causes application breakdown.

14.3 Patch Management Review

The patch management activity shall be regularly updated in a tracker to ensure that all systems (servers, workstations, network and mobile devices are patched as per the defined schedule. The tracker shall be regularly reviewed by information security team. Issues and the corresponding corrective actions shall be recorded.

15.Title: SOP for Logging and Monitoring

15.1 Log Management

15.1.1 All the information systems should be configured with logging and audit settings, as per the specifics in the hardening checklists and the various international standards.

15.1.2 All logs shall be retained for 1 year with 3 months of online availability for immediate analysis of logs when required.

15.1.3 All login and logout events on domains, servers, applications and all devices should be logged.

15.1.4 All systems shall log the following when relevant;

15.1.4.1 user IDs;

15.1.4.2 system activities;

15.1.4.3 dates, times and details of key events, e.g. log-on and log-off;

15.1.4.4 device identity or location if possible and system identifier;

15.1.4.5 records of successful and rejected system access attempts;

15.1.4.6 records of successful and rejected data and other resource access attempts;

15.1.4.7 changes to system configuration;

15.1.4.8 use of privileges;

15.1.4.9 use of system utilities and applications;

15.1.4.10 files accessed and the kind of access;

15.1.4.11 network addresses and protocols;

15.1.4.12 alarms raised by the access control system;

15.1.4.13 activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;

15.1.4.14 records of transactions executed by users in applications

15.1.5 Necessary logging of the critical events shall be ensured.

15.1.6 Network device logs shall be maintained.

15.1.7 Logs shall be stored in such a way that they cannot be changed/ altered by anyone. Privileged users shall not have access to system logs in which their activities are captured.

15.1.8 All systems where logging is enabled shall be configured to take appropriate action if the logging mechanism fails.

15.1.9 Logging the data to write-only media like a write-once/read-many (WORM) disk or drive.

15.1.10 All logs shall be backed up before being deleted from the system and the backups shall be stored for appropriate periods.

15.1.11 Attempts to access deactivated accounts shall be monitored through audit logging.

15.1.12 Audit log settings for each hardware device and the software installed on it shall be validated.

15.1.13 Logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction.

15.1.14 Systems record logs in a standardized format such as syslog entries.

15.1.15 The Logging parameters shall be set to disallow any modification to previously written data.

15.2 Protection of Log Information

15.2.1 Log information shall be protected against unauthorized access, alterations, and operational problems. Access to logs shall be provided on ‘need-to-know’ and ‘need-to-have’ basis.

15.2.2 The logging facilities will be enforced with logical access controls and monitored to protect against tampering and unauthorized access. The logging facility should have a defined storage space for collection of logs from various systems and devices. Adequate monitoring shall be in place to ensure that logs are not overwritten

15.3 Log Monitoring

15.3.1 Logs shall be reviewed periodically and relevant action is taken based on the findings.

15.3.2 The log audit shall be done by an entity other than the entity whose logs are being audited.

15.3.3 Periodic auditing of host configurations, both manual and automated shall be done at the network level.

15.4 Clock Synchronization

The internal clock of all servers, desktops, networking devices, firewall, and other computing devices should be synchronized with an industry standard time source and shall be maintained as per Indian Standard Time unless explicitly mentioned.

16.Title: SOP for System Acquisition, Development and Maintenance

16.1 Processing in Applications

16.1.1 Appropriate controls shall be designed into applications. These controls include the validation of input data, internal processing and output data. Additional controls will be designed on the basis of security requirements and risk assessment of systems that process, or have an impact on sensitive, valuable or critical information.

16.1.2 Access to system files and program source code shall be controlled and IT projects and support activities be conducted in a secure manner. Care shall be taken to avoid exposure of sensitive data in test environments.

16.1.3 To minimize the risk of corruption to operational systems guidelines shall be in place to control changes.

16.1.4 The use of operational databases containing personal information or any other sensitive information for testing purposes shall be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition before use.

16.1.5 Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

16.1.6 Project and support environments shall be strictly controlled. Managers responsible for application systems shall also be responsible for the security of the project or support environment. They shall ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

16.1.7 Technical review of application shall be conducted after any changes to the operating system to ensure that the behavior of the application has not altered. Security requirements, if suggested by application vendor shall be applied.

16.1.8 Vendor-supplied software packages shall not be modified unless there is business requirement and all modifications shall pass through testing process and necessary audit records shall be maintained.

16.2 Outsourced Software Development

16.2.1 Licensing arrangements, code ownership, and intellectual property rights shall be documented.

16.2.2 Certification of the quality and accuracy of the work carried out.

16.2.3 Wherever feasible, for the critical applications, either source code must be received from the vendor or a software escrow agreement needs to be in place with a third party to ensure source code availability in case the vendor goes out of business.

16.2.4 Rights of access for audit of the quality and accuracy of work done.

16.2.5 Contractual requirements for quality and security functionality of code.

16.2.6 Testing before installation to detect malicious and Trojan code.

16.2.7 Availability of support.

16.3 Technical Vulnerability Management

Technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations shall include operating systems, and any other applications in use.

16.4 Software Implementation Procedures

Software implementation shall be preceded by user acceptance test by the relevant business groups. Software Implementation procedure shall be put in place and adhered to.

16.5 Separation of Testing and Production Environments

16.5.1 To reduce the risk of damage to the production environment due to activities in the testing environment.

16.5.1.1 Development, testing and production activities and areas must be clearly identified and separated.

16.5.1.2 Development, testing and production environments shall be separated logically and physically.

16.5.1.3 Utilities, such as Compilers, editors and other system, required for development and testing must not be accessible from the production systems.

16.5.1.4 Users must use different access mechanisms, including user ids and passwords, for operational and test systems and the application must display appropriate identification messages to reduce the risk of error.

17. Title: SOP for Information Security Audit

17.1 Audit Planning

Following are the procedures to be followed to administer the Information Security audit -

17.1.1 Before Go-Live of any Software, Audit should be conducted by CERT-IN empaneled auditor. Only after the closure of the observations/Gaps, application/software should be made live.

17.1.2 After any major changes/customization in the hosted Software, audit should be conducted by CERT-IN empaneled auditor.

17.2 Audit Periodicity

Cert-In empaneled vendor should conduct Information Security Audit) once in a Year for all the software including outsourced vendors and whenever there are any major changes in the software.

17.3 Outsourcing IS Audit activities

17.3.1 IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training.

17.3.2 As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by CWC. They should be competent audit professionals with sufficient and relevant experience.

17.3.3 The external professional service providers appointed should be competent in the area of work that is outsourced and should have relevant prior experience in that area.

17.3.4 The auditor to be on-boarded should be empaneled with CERTIN, Govt. Of India or as per guidelines issued by Govt. of India, time to time.

17.3.5 As a practice, Corporation shall ensure to include the relevant clauses in the tender document for stipulating the scope of work for yearly CERTIN audit of the software.

17.4 Audit Compliance

Since most of the application are hosted in the cloud environment managed by the different system integrators, CWC and system integrators should ensure the compliance and closure of the observations reported by the auditors in order to obtain the security audit certificate.