INFORMATION AND CYBER SECURITY POLICY

Document Code: - HUDCO/ IT-Policies/2024/03

Document Classification: Internal

(Version 1.1)

HOUSING & URBAN DEVELOPMENT CORPORATION LIMITED

Core 7-A, HUDCO Bhawan, India Habitat Centre, Lodhi Road, New Delhi 110003

Website: www.hudco.org.in CIN: L74899DL1970GOI005276

Version History

S. No.	Version No.	Prepared By	Proposed By	Approved By	Dated
1.	1.0	Deloitte Corporate Finance Services India	ED (IT)	HUDCO Board	08.01.2019
2.	1.1	AKS IT Services Pvt. Ltd.	ED (IT)	HUDCO Board	16.12.2024

Table of Contents

1. Introduction

The Information and Cyber Security Policy provides structure and direction for protecting information systems and any other available forms of information from a wide range of threats including cyber-attacks in order to ensure safeguard information assets, minimize damage and business continuity. This policy is segregated into multiple sections, where each section covers a single domain crucial for protecting the information assets and information systems of HUDCO.

2. Information and Cyber Security Objectives

Information Security at HUDCO is driven by the following objectives:

- Protection of information against unauthorized access by maintaining its confidentiality.
- Ensuring the integrity of information. Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- Ensuring the availability of information to those who are authorized and require it. Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- Ensuring the authenticity of data, transactions, communications and documents (electronic or physical)
- Meeting the statutory requirements.
- Creation, maintenance, and testing of Business Continuity Plans.
- Imparting information security awareness training to all staff.
- Reporting and investigation of security breaches.
- Effective Role definition for all employees to avoid conflict in duties and areas of responsibility.
- Managing Information security risk by integrating Information security governance in the overall enterprise governance framework of the organization.
- Ensuring Continual Improvement to the information security management system.

Cyber security at HUDCO is driven by the following control objectives:

- Establishing cyber incident detection and handling mechanisms to protect HUDCO infrastructure from cyber threats and risks.
- Formalizing Vulnerability Management process for eliminating or mitigating vulnerabilities based upon the risk associated with the vulnerabilities and cost involved for mitigation.

- Informing Cyber Crisis Management Plan to all Stakeholders.
- Providing a catalogue of security controls to meet current information protection needs and the demands of future protection needs based on changing threats, requirements, and technologies.
- Establishing a comprehensive risk assessment process for HUDCO IT systems to find out the risks associated and to determine the appropriate level of controls necessary for mitigating risks.
- HUDCO shall understand, manage and comply with relevant cybersecurity and data security/ protection requirements mentioned in government guidelines/ policies/ laws/ circulars/ regulations, etc. issued by RBI/SEBI/ GOI such as IT Act 2000, Digital Personal Data Protection Act, 2023 (DPDP Act 2023) or any other law/ circulars/ regulations issued from time to time.

3. Management

IT department in consultation with CISO shall review the Information and Cyber Security Policy annually and shall put up for approval of Board of Directors.

4. Policy Standard and Procedures

Standards are detailed requirements that need to be met for complying with the Cyber Security Policies. Separate set of standards are to be developed for each policy statement. Standards include measures that need to be taken for mitigating all risks associated with the respective domain covered by the policy statements. Separate Standard Operating Procedures are to be created as per requirements to document the detailed guidelines of how to implement the policies and standards.

The key objectives of developing Procedures and Guidelines are:

- To ensure that Cyber Security Policy and Standards are interpreted correctly and uniformly across the HUDCO.
- To provide guidelines for implementation of the policy and standards.
- To create awareness about policy and standards and assist in their compliance.

Implementation of Policy is to be done in phased manner prioritizing the critical activities first.

5. Scope

Information and Cyber Security Policy is applicable to:

- All employees, contractors, third-parties, outsourced partners and personnel associated with HUDCO.
- All information assets which include, but are not limited to: software assets, hardware assets, paper assets, service assets, people assets and assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.

6. Exceptions

There may be instances where there is a justifiable business need to perform actions that are in conflict with Information and Cyber Security Policy. Whenever for technical or business reasons, it is not possible to comply with this policy, a time bound waiver must be requested. The waiver needs to be approved by CISO. All approved exceptions should be reviewed at least annually or as and when required. Any issue related to interpretation shall be approved by the competent authority.

7. Enforcement

Non-compliance to the minimum requirements or violation of HUDCO Information and Cyber Security Policy could result in action that may include, but is not limited to, the following:

- Warning
- Suspension
- Civil and/or criminal prosecution as deemed fit
- Other actions as per CDA rules of HUDCO.

8. Cyber Security Strategy

In response to the cyber-attacks, management at HUDCO has set up a strategy to protect its IT assets from cyber-attacks and respond to any cyber-attacks, threats in a timely and appropriate manner to ensure confidentiality, integrity and availability of data/IT Systems. The cyber security strategy, as represented in figure 1, is to Identify, Protect, Detect, Respond, and Recover and Learn. Table below provides a stage-wise description of the stages of HUDCO's cyber security strategy.

S.no.	Stage	Description
1	Identify	Identification of critical assets and management of cyber security risks
2	Protect	Safeguarding continually identified assets by deploying controls such as security architecture mechanisms, event correlation systems, intrusion prevention and detection systems, and enforcement of secure configurations.
3	Detect	Detecting incidents related to attacks or anomalies through continuous monitoring of critical infrastructure
4	Respond	Take steps to assess the incident impact and take appropriate response measures including escalation to relevant authorities

5	Recover	Recover from incident in a timely manner adequately following the organization's incident management, business continuity and disaster recovery policies and procedures and to ensure that there is no loss of confidential data and that its IT assets are protected against cyber-attacks.
6	Learn	Post recovery record the relevant learnings from the cyber-incidents and form a plan to prevent similar incidents.

9. Information Security Framework

This identifies major issues related to information security and provides broad guidelines to deal with them. Detailed instructions and procedures will be developed on basis of this policy and would require close monitoring.

HUDCO shall form Information Security Committee (ISC) operating at an executive level to ensure the Information and Cyber Security framework is effectively implemented and maintained. Proceeding of ISC are to be briefed to IT Strategy Committee of the Board quarterly.

10. Risk Management

HUDCO shall establish a robust IT and Information Security Risk Management Framework, addressing, among others, the following aspects:

- Implementation of a comprehensive Information Security management function, internal controls, and processes (including applicable insurance coverage) to mitigate or manage identified risks. The effectiveness of these controls and processes must be periodically reviewed to address a dynamically changing risk environment.
- Definition of roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Potential role conflicts and accountability gaps must be specifically identified and appropriately addressed or managed.
- Identification of the organisation's critical information systems and strengthening the security environment surrounding these systems; and
- Definition and implementation of necessary systems, procedures, and controls to ensure the secure storage, transmission, and processing of data and information.

10.1. Security Risk Assessment

- The risk assessment for each information asset within HUDCO's scope shall be guided by appropriate security standards and IT control frameworks.
- HUDCO shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies applicable to them.

- HUDCO shall review its security infrastructure and security policies at least annually, considering its own experiences as well as emerging threats and risks. HUDCO shall take appropriate measures to address cyber-attacks, including phishing and spoofing attacks, and mitigate their adverse effects.
- The Information Security committee is required to oversee risk assessment on all IT assets at least annually and prior to introducing any significant change in the environment.
- The HUDCO's priorities, constraints, risk tolerance and risk appetite statements, assumptions and constraints are established, communicated, and used to support operational risk decisions.
- Following activities shall be undertaken as part of risk assessment:
    - **Risk Identification** – Identifying potential threats and their sources, vulnerabilities, impact consequences on information assets, and risk owners are identified.
    - **Risk Estimation** – Assessing business impact value, likelihood of an incident (qualitatively or quantitatively) and estimating the level of risk.
    - **Risk Evaluation** – Comparing the level of risk against the risk acceptance or risk treatment criteria and prioritizing for risk treatment.

11. Organization of Information Security

11.1. Internal Organization

11.1.1. Segregation of Duties

Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized or unintentional modification or misuse of information assets.

Responsibilities to be performed by the role holders in the development, processing, administration or management of HUDCO's information systems are needed to be identified, documented, approved and users will be accordingly set up with the approved privileges.

It is required that the user account creation requests and access entitlement requests are not self-approved by the requestor. Business managers or their delegates cannot review or approve their own access entitlements.

It is required that conflicting roles and users are identified. Assignment of such conflicting roles is not recommended. Following is an indicative list of conflicting duties:

- A single user responsible for implementing and approving their own transaction, such as lack of dual control or 'maker-checker'.

- Application development/ testing team carrying out application administration in production environment.
- Users carrying out log monitoring for their own machines; and
- Server or network administrators carrying out database administration.
- Management of network and security device being carried out by single operational team.

When conflicting roles need to be assigned to a user, it is required that the following controls are implemented:

- Valid business justification for the exception request is documented.
- Risks are identified that may arise because of conflicting roles.
- User IDs with such conflicting roles are logged.
- Monitoring of activities through audit trails, exception reporting, reconciliation and transaction logs.
- Conflicting roles are reviewed at least once a year by respective functional heads. A formal approval for continuation of conflicting roles shall be obtained after the yearly review.

11.1.2. Contact with Authorities

It is required that appropriate contacts with relevant authorities including but not limited to law enforcement authorities, regulatory bodies, fire department, emergency services and telecommunication providers for combating emergencies are maintained.

11.1.3. Contact with Special Interest Groups

It is required that appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained. Membership in special interest groups or Information Security committee forums are considered as a means to:

- Improve knowledge about best practices and stay up to date with relevant security information.
- Ensure the understanding of the information security environment is current and complete.
- Upgrade knowledge and skillset with adequate skillset.
- Receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities.
- Gain access to specialist Information security advice.
- CISO and staff of CISO’s office may join forums/groups to remain updated with the latest security threats, solutions etc.

11.2. Mobile Device and Teleworking

11.2.1. Mobile Device Policy

- HUDCO managed mobile devices such as Smartphones, tablets, PDAs etc. shall have a strong password protection enabled on the device or the encrypted container containing HUDCO data.
- Employees are required to notify their manager or the IT Support desk within 24 hours as soon as the employee is aware that a device was lost or stolen.
- Users shall use internet on mobile devices for business activities and restrict non-business activities or allow occasional and reasonable personal use of internet services.
- Employees shall access internet only through the connectivity provided by HUDCO and shall not set-up internet access without authorization from IT Department.
- HUDCO shall have the right to filter and prohibit access to certain websites at its own discretion.
- HUDCO reserves the right to monitor and review internet usage of users to ensure compliance to this policy.
- Users shall be held responsible for any misuse of Internet access originating from their account.

11.2.2. Teleworking

- Remote access to the HUDCO network will be permitted only where there is a legitimate business need and is subject to management approval. It is required that the end users request the VPN access and take requisite approval from the reporting manager and IT Department.
- HUDCO should ensure that remote access user follow approved policies.
- Implement multi-factor authentication for enterprise access (logical) to critical systems.
- Put in place a mechanism to identify all remote-access devices attached/ connected to the HUDCO's systems and ensure that data/ information shared/ presented in teleworking is secured appropriately.

12. Personnel Security

The purpose of the human resource security policy is to reduce the risks of human error, theft, fraud or misuse of facilities. HUDCO shall conduct independent identity checks before confirming the employment. The independent identity checks shall be conducted keeping in mind the level at which the selected candidates join HUDCO.

12.1 Terms and Conditions of employment

The security roles and responsibilities need to be clearly communicated to every new employee during the induction process and also through sessions.

The HR function needs to ensure that the 'Terms and Conditions of Employment' reflect the Information security requirements and it is required that the following points are included as well:

- The requirement for all employees to sign a confidentiality agreement will hold them liable for any unauthorized disclosure, modification and/ or destruction of information.
- The responsibility for maintaining the confidentiality and integrity of information.
- The actions to be taken, if any user disregards the requirements of the HUDCO Security Framework.
- The continuation of the employee's responsibilities for protecting the confidentiality of the information of HUDCO even after termination of employment.
- Immediate removal from services in case of any information security breach is performed by any employee, which is of damaging nature.

12.2 Information Security Awareness, Education and Training

Management needs to provide an ongoing awareness and training program in information security and in the protection of HUDCO information resources for all personnel whose duties bring them into contact with confidential or sensitive information resources.

It is required that the HUDCO employees accept and acknowledge their information security responsibilities.

The purpose of user training is to ensure that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work.

- To ensure awareness of information and cybersecurity policies, all employees, vendors, service providers, and stakeholders will be informed of their roles, responsibilities, and the potential consequences of non-compliance. Departments will ensure that relevant personnel understand their contributions to the cybersecurity framework's effectiveness.
- Cybersecurity awareness sessions will be conducted annually for all employees, including top management, to reinforce the importance of compliance and security objectives.

- Educate HUDCO customers about current online and mobile banking threats, gather feedback, and periodically update them on emerging cyber risks, encouraging reporting of any cyber-attacks.
- Launch online and offline cybersecurity awareness campaigns to inform customers about the risks of sharing sensitive HUDCO credentials (e.g., login, passwords, PINs) with third-party vendors.

13. Asset Management

Asset Management specifies the importance of maintaining records of each information asset including identification of the asset owner and asset classification.

Information assets of HUDCO shall receive comprehensive protection and shall have an identified owner. It provides direction to ensure that:

- An information asset register documenting the types of information assets of each business function is maintained.
- Information assets of each business function have designated owners.
- The data, personnel, devices, systems, and facilities that enable the HUDCO to achieve its business purposes are identified and managed consistently in accordance with their relative importance to organizational objectives and the HUDCO's risk strategy.
- Physical devices, digital assets (such as URLs, domain names, applications, APIs, etc.), shared resources (including cloud assets) and other interfacing systems within the organization are inventoried in a time bound manner.
- Organizational communication, data flows and encryption methods shall be mapped and inventoried with respect to all IT systems and network resources.
- HUDCO's shall ensure that no shadow IT assets are present in the organization.
- Inventories of data, and corresponding metadata for designated data types are maintained.

13.1. Management of Assets

HUDCO is required to prepare and maintain an up to date inventory of all information assets associated with business function and define classification guidelines.

13.1.1 Inventory of Assets

The HUDCO will maintain an inventory of assets that are used for information processing, including the information itself, to ensure that these assets are effectively protected. The assets will be grouped in four major groups:

- Information Asset - This would include Databases and Data files (including important data in local desktops/laptops), System documentation, User

documentation, Training materials, Operational / Support procedures, Continuity plans, Archived information, Licenses etc. An Information asset can be further subcategorized into two formats - Electronic and Paper format.

- Software Asset - This would include Application software, System software, Development tools and Utilities etc.
- Hardware Asset - This would include Computer equipment (servers, desktops, laptops, modems, printers etc.), Communication equipment (Network devices.), Unused magnetic media (Tapes etc.
- Services Asset - This would include general utility services such as Power, Lighting, and Air Conditioning etc.
- Key Personnel - This would include personnel required to support and run another asset.
- Each asset will have a nominated owner and the responsibility for the maintenance of appropriate controls will be assigned to the owner. Inventory Registers for all the four types of assets will be maintained and periodic review of the inventory will be carried out to ensure the accuracy of the Inventory registers
- It is required that all the information assets are documented in the information asset registers.

13.1.2 Ownership of Assets

- All information assets are required to have a designated owner. Asset Owner will be responsible for identifying authorized users who can access the information asset.
- All information assets shall be classified based on their business value and impact to business operations.
- Information asset register needs to be reviewed at least once in a year, or any significant change occurs.

13.1.3 Acceptable Use of Assets

- HUDCO employees are accountable for all the activities associated with their user IDs.
- Use of HUDCO resources is limited to business purposes and HUDCO reserves the right to monitor and report this usage.
- Use of HUDCO managed resources is prohibited for the use of commercial activities other than those related to HUDCO business purposes.
- Computing and network resources provided by HUDCO can be used only by the authorized employees and Third Parties.
- The following will be deemed unacceptable uses of HUDCO technology resources:

- Transmitting or otherwise removing information from the office for personal use, that contravenes the privacy of customers and HUDCO personnel and HUDCO intellectual property.
- Wasting computer resources or monopolizing those resources to the exclusion of other users.
- Circumventing user authentication or authorization on any system.
- Installing and/or using unlicensed / non-approved / cracked software, data and hardware.
- Connecting any hardware that is unapproved to the HUDCO network.
- Under no circumstances an employee of the HUDCO shall be engaged in any activity that is illegal under Corporate, Local, State, National or International laws while utilizing HUDCO owned resources.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by HUDCO.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Organization or the end user does not have an active right.
- Exporting/importing software, technical information, encryption software or technology, in violation of international or National export control laws, is illegal. It is required that appropriate management is consulted prior to export / Import of any material that is in question.
- Introduction of malicious programs or Spywares, Proxy Bypass tools etc. into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) which may bring any potential threat to the organization.
- In view of the risks associated with the usage of unsecured internet devices use of Internet data cards, Broadband Connections or other mechanics of Internet connectivity excluding use of Authorized Enterprise Internet setups is banned from being used within the Organization’s Premises and on organization’s enterprise systems and the employees violating this policy will be liable for disciplinary action.
- Other activities that are deemed unacceptable by the HR or similar function and that are illegal.

- It is required that only HUDCO-managed technology resources (e.g. desktops, laptops) are used to store, transmit and/or connect to the HUDCO internal network.

- It is required that formal approval is obtained from the Information Security committee before non-HUDCO managed technology resources are used to connect to the HUDCO network.
- Where approval has been obtained, non- HUDCO managed technology resources used to connect to the HUDCO network is subject to HUDCO's security requirements set out for:
    - Viruses & other malware
    - Mobile devices
    - Wireless networks
    - Unified communication
    - Messaging and Internet use
- Prior to sensitive HUDCO information being taken away from the office, the following shall be considered:
    - Sensitivity of the information
    - Potential impact of loss or disclosure of the information
    - Precautions that need to be taken to avoid loss or disclosure
    - Users are required to promptly report the loss of HUDCO-managed technology resources, used to store HUDCO information, to the IT Department.
- Encryption or an equivalent method of protection shall be used to secure sensitive HUDCO information when:
    - Transmitted over non-corporate networks such as the internet.
    - Stored on mobile devices and removable media.
- Users shall lock their desktop, laptop and any other mobile devices before leaving them unattended. Users shall take due caution of not leaving any mobile device unattended which have Organizations data/emails.
- Users shall shut down desktops/ laptops at the end of a workday to save power consumption.

13.2. Information Classification

13.2.1 Classification of Information

All information shall be protected in accordance with the following information classification categories:

- **Public**: This information has been specifically approved by concerned department for public release. Unauthorized disclosure of this information need not cause

problems for HUDCO, its customers, or its business partners. Example: marketing brochures and material posted to the HUDCO Internet web page. Disclosure of HUDCO information to the public requires the existence of this label, the specific permission of the information owner, or long- standing practice of publicly distributing this information.

- **Internal**: This information is intended for use within HUDCO, and in some cases within affiliated organizations, such as HUDCO business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for HUDCO, its customers, or its business partners.
- **Confidential**: This information is private or otherwise sensitive in nature and it is required that this information is restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for HUDCO, its customers, or its business partners.
- **Executive**: This information is the most private or otherwise sensitive and requires to be strictly monitored and controlled at all times. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause severe problems for HUDCO, its customers, or its business partners.

13.2.2 Labelling of Information

It is required that an appropriate set of procedures for information labelling is developed and implemented in accordance with the information classification scheme adopted by HUDCO. Information Owners are required to review the information classification categories for determining whether information is to be declassified or not.

13.2.3 Handling of Information

- All the Confidential and Executive documents in paper form shall be kept under lock and key. Any such information in electronic form shall be protected by technology control, wherever feasible.
- Access list for using executive document shall be known to the document owner.
- Any document when printed or scanned shall be cleared from printers or scanners immediately.
- All the system documentations shall be stored in a secure environment and physically protected from unauthorized access.
- The distribution list for system documentation is strictly on 'need-to-know' basis and authorized by the respective information asset owner.

13.3. Backup Media

To ensure the protection and recoverability of critical company data, backup media will be utilized for regular data backups. The following procedures will be followed:

1. Selection of Backup Media: The company will use reliable and secure backup media, including external hard drives, cloud storage, and other appropriate methods, based on the type and volume of data being backed up.
2. Backup Schedule: Data backups will be performed on a regular schedule (e.g., daily, weekly) as determined by the business requirements and data criticality.
3. Data Encryption and Security: All backup media will be encrypted to ensure data confidentiality and protection against unauthorized access. Backup data will be stored securely, both on-site and off-site, where applicable.
4. Testing and Verification: Regular testing of backup systems and data restoration processes will be conducted to ensure the integrity and effectiveness of backups.
5. Retention and Disposal: Backup data will be retained according to company retention policies, and outdated or unnecessary backups will be securely destroyed to prevent unauthorized access.
6. Responsibility: Designated personnel will be responsible for overseeing the backup process, ensuring timely execution, and addressing any issues that may arise with the backup media.

This backup media implementation is designed to minimize the risk of data loss and to ensure business continuity in case of an emergency. Ensure that copies of ERP Back-ups are maintained physically in fire-proof almirah/safe.

13.4. Media Handling

13.4.1 Management of Removal Media

HUDCO removable media shall not be connected to computers that are not owned or leased by Organization without explicit permission of Head of Concerned Department.

Confidential and Executive data that is stored on removable media such as USB devices, portable hard drives, magnetic tape shall be encrypted using HUDCO approved encryption technologies.

Exceptions to this policy may be requested on a case-by-case basis by permitted exception procedures. Any employee found to have violated this policy may be subject to disciplinary action.

HUDCOs shall define and implement policy for restriction and secure use of removable media (such as USB, external hard disks, etc.) and electronic devices (such as laptops, mobile devices, etc.).

13.4.2 Disposal of Media

Executive and Confidential information as well as licensed software shall be removed from computer equipment and removable media prior to disposal or re-use.

Disposal or destruction of data is prohibited without confirming that the data has reached the end of its retention period as defined by HUDCO and that there is no additional retention period (such as a litigation hold or preservation notice).

Secure methods of disposal such as wiping, degaussing or physical destruction are acceptable. The following are the procedures:

- Hard Disks: Data to be overwritten using tools with the capability discussed above.
- Tapes: Destroy - Disintegrate, pulverize, or shred.
- CD-ROM: Destroy - Disintegrate, pulverize, or shred.
- USB Drives: Destroy - Disintegrate, pulverize, or shred.
- All other non-rewriteable storage mediums (i.e., write once, read only after the write): Destroy - Disintegrate, pulverize, or shred.

13.4.3 Physical Media Transfer

Confidential and Executive data that is shipped on removable media (like tape, USB, etc.) shall be encrypted using HUDCO approved encryption methods. Where encryption is technically not feasible, it shall be ensured that such media is transported in person/ in a secure manner by an authorized HUDCO personnel. Record of movement should be maintained at the site.

14. Access Control

- Access to information assets shall be allowed only where a valid business need exists. HUDCOs shall have documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system.
- Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed.
- HUDCOs shall adopt multi-factor authentication for privileged users of

  i) critical information systems

  ii) for critical activities, basis the HUDCO's risk assessment.

- Access controls are required for all HUDCO IT systems in accordance with risk in order to protect information assets against unauthorized logical access.

14.1. Business Requirement of Access Control

14.1.1 Management of Access Control

- Managers shall be accountable for the access rights of the users under their supervision.

- Users shall be granted with least privilege required for a particular role or function.
- Additional restrictions shall be implemented for Special Privilege Accounts.
- All accesses shall be reviewed on periodic basis and appropriate actions shall be taken.
- Additional authentication methods (like two factor authentication) shall be used when allowing users to connect remotely.
- Access to operating system shall be controlled by a secure logon procedure.
- The use of utility programs that might be capable of overriding the system and application controls shall be restricted and tightly controlled.
- Restrictions on connection times shall be used to provide additional security for high-risk applications.
- Inactive sessions shall be terminated after a defined period of inactivity.

14.1.2 Access to network and network services

- Computer networks shall be segregated to isolate critical HUDCO IT assets and those exposed to higher risks (Internet facing).
- Sensitive systems shall have a dedicated (isolated) computing environment.
- Any category / website that poses a security risk shall be blocked explicitly after due diligence.
- Access to non-business-related website shall be prohibited such as pornography, terrorism, hacking and religious provoking sites etc.

14.1.3 Advanced Real-time Threat Defense and Management

To ensure the protection of information through real time monitoring of threat landscape for HUDCO's network across India and foreign offices.

- The HUDCO will build a robust defense against the installation, spread, and execution of malicious code at multiple points in the enterprise.
- The HUDCO will Implement Anti-malware, Antivirus protection including behavioral detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralized management and monitoring.
- A whitelist of authorized websites required for business operations shall be defined and maintained.

- Force point application will be implemented to secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway.

14.2. User Access Management

14.2.1 User registration and de-registration

A formal documented procedure shall be in place for granting and revoking access to all HUDCO IT systems.

All usernames should to be uniquely identifiable and the principles of non-repudiation have to be met.

Ensure the deletion of user IDs is completed within specified timeline of receiving an approved request.

14.2.2 User access provisioning

All user access requests shall be authorized by the user's reporting manager. The level of access to be granted, or role profile to be assigned to a user, shall be approved by the business system owner or their approved deputies / Project Manager / reporting managers.

It is the responsibility of the approver(s) to ensure the person has a legitimate business need for the level of access requested, after doing due diligence.

14.2.3 Management of privilege access rights

Creation and allocation of privileged user accounts / IDs on the information systems shall be authorized. Procedure shall ensure the following:

- The privilege associated with each system (e.g. Operating Systems, Databases, and Applications) and their corresponding users are identified.
- Privileges are allocated to individuals on a 'need-to-have' basis in strict adherence to the authorization process for privilege access.
- A record of all privilege accounts used on the information systems is maintained; Changes made to privileged accounts are recorded.

14.2.4 Management of secret authentication information

- Temporary passwords shall be provided only after confirming the user identity and it shall prompt the user to change the password on its first use.
- Default vendor passwords require to be altered following installation of systems or software. Such altered passwords shall be known only on need to know basis to privilege users.

14.2.5 Review of user access rights

Accounts that access executive or confidential data shall be reviewed semi-annually, using a documented business process. Review process shall verify that an on-going process is in place to ensure that employees who have left HUDCO no longer have active accounts, and those unnecessary entitlements have been removed when roles have changed.

14.2.6 Removal or adjustment of access rights

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.

14.3. User Responsibilities

14.3.1 Use of secret authentication information

It is required that:

- Passwords shall not be written down or stored in clear text.
- Users shall ensure that the passwords are kept confidential and shall not be shared or disclosed to anyone including the IT Help Desk.
- If a temporary password has been provided to the user, it is required that it is changed immediately upon the next logon.

14.4. System and application access control

14.4.1 Information access restriction

Access to information and application system functions shall be restricted in accordance with this policy and supporting procedures.

14.4.2 Secure log-on procedure

Access to systems and applications shall be controlled by a secure log-on procedure.

14.4.3 Password management system

Allocation of user passwords shall be controlled by implementing the following controls:

- User IDs shall be unique and traceable to HUDCO Owner that is responsible for the account.
- Enforce expiry of password for 90 days and maintain a history of at least three previous passwords to prevent re-use.
- Password complexity including alphanumeric characters shall be enforced.
- Passwords shall be minimum of eight (8) characters in length.
- Passwords shall be encrypted or hashed in transmission and in storage (excluding temporary passwords).

- Account lockout after no more than a total of five (5) failed login attempts shall be enforced.
- All generic user accounts shall be traceable to HUDCO owner, who is responsible for the account. Default software and hardware accounts shall be restricted by either disabling them or by maintaining an audit trail traceable to a unique individual.

14.4.4 Database Password management requirements

- In order to maintain the security of Organization's internal databases, it is required that the access by software programs shall be granted only after authentication with credentials. The credentials used for this authentication need not reside in the main, executing body of the program's source code in clear text.
- Database usernames and passwords shall be stored in a file separate from the executing body of the program's code. This file should not be readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials shall be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Passwords or pass phrases used to access a database shall adhere to the Password Policy.
- Every program or every collection of programs implementing a single business function shall have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs shall be system-level passwords as defined by the password guidelines.
- Developer groups shall have a process in place to ensure that database passwords are controlled and changed in accordance with the password guidelines.
- This process shall include a method for restricting knowledge of database passwords to a need-to-know basis.

14.4.5 Use of privilege utility program

- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
- All the unnecessary utility programs shall be removed or disabled including LAN setting options in the browser.

14.4.6 Access control to program source code

- Access to program source code shall be restricted and properly documented.
- The program source code and the program source libraries shall be managed according to established procedures.

15. Maintenance, Monitoring and Analysis of Audit Logs

Logging, monitoring and reporting capabilities shall be implemented to detect security events.

- Log Generation- HUDCO will Identify Log Source, determine all systems, applications, and devices that generate logs.
- Log Content: Ensure logs contain relevant information such as timestamps, event types, user activities, source and destination IP, addresses, etc.
- Log Format: Standardize log formats across different sources to facilitate easier analysis.
- Centralized Log Collection: HUDCO will Collect logs from various sources into a centralized log management system or Security Information and Event Management (SIEM) system.
- Secure Transmission: HUDCO will ensure logs are transmitted securely using encryption to protect against interception and tampering
- Retention Policy: HUDCO will Define and implement a log retention policy, typically retaining logs for at least six months or as per regulatory requirements.
- Storage Security: Store logs in a secure environment with access controls to prevent unauthorized access, modification, or deletion.
- Redundancy: HUDCO will ensure logs are stored redundantly to protect against data loss.
- Real-Time Monitoring: HUDCO will Implement real-time monitoring of logs to detect suspicious activities and security incidents promptly.
- Automated Analysis: HUDCO will Use automated tools and scripts to analyse logs for patterns, anomalies, and known indicators of compromise (IOCs).
- Manual Review: HUDCO will Conduct regular manual reviews of logs to identify any missed anomalies or incidents.
- All logs should be integrated with HUDCO's centralized Security Operations Center (SOC) based on criticality and Risk Assessments.
- HUDCO will use a centralized application to manage and analyze audit logs in a systematic manner so as to detect, understand or recover from an attack.

16. Audit Trails

Every IT application that can access or impact critical or sensitive information must include necessary audit and system logging capabilities, ensuring the provision of comprehensive audit trails. These audit trails should meet HUDCO's business requirements in addition to regulatory and legal mandates.

The audit trails must be sufficiently detailed to support audit processes, serve as forensic evidence when needed, and aid in dispute resolution, including ensuring non-repudiation. HUDCO shall establish a system for the regular monitoring of audit trails and system logs to identify and address any unauthorized activities.

17. Cryptography

17.1 Cryptographic Controls

17.1.1 Policy on the use of Cryptographic controls

- The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. HUDCOs shall adopt internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.
- HUDCO understands the importance of information either in transit or stored and hence strives to protect it via cryptographic keys & certificate management wherever feasible and appropriate. The level of protection applied requires to commensurate with the sensitivity and frequency of use of the information along with the environment where it resides/used.
- Key custodians shall be made aware, and they shall formally acknowledge their obligations in administering the security of the keys.

17.2 Key Management

It is required that Encryption Key Management Guidelines for secure key generation, ownership, distribution, archival, storage and revocation shall be defined, released and followed to protect the keys throughout their lifecycle. The procedure documents shall address following aspects related to key management, including:

- key generation;
- key distribution;
- key storage;
- key change;
- key destruction;
- key custodians and requirements for dual control;
- prevention of unauthorized substitution of keys;
- replacement of known or suspected compromised keys;
- Change of cryptographic key at the end of defined crypto period.

It is required that the cryptographic keys shall be protected against unauthorized modification, substitution, unintended destruction and loss. Secret keys associated

with symmetric cryptographic algorithms and private keys associated with asymmetric cryptosystems shall be protected against unauthorized disclosure.

18 Maker Checker

- Maker Checker principle shall be applied for all HUDCO employees in the Information system.
- HUDCO shall put in place an appropriate maker checker system to ensure that the relevant furnished is correct and free from errors.

19 Vulnerability Management

- Timely information about technical vulnerabilities of information systems being used shall be obtained by internal teams, external teams and sources. HUDCO's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken to address the associated risk.
- Conduct of Vulnerability Assessment (VA) / Penetration Testing (PT) (a) For critical information systems and/ or those in the De-Militarized Zone (DMZ) having customer interface, VA shall be conducted at least once in every six months and PT at least once in 12 months. Also, HUDCO shall conduct VA/ PT of such information systems throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.).
- HUDCO shall put in place a documented approach for conduct of VA/ PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This may also apply to the HUDCO's information systems hosted in a cloud environment.
- Conducting VA/PT of internet facing web / mobile / cloud-based applications, servers & network components throughout their lifecycle. Such assessments shall only be carried out by professionally qualified teams.
- Ensuring that the vulnerability scanning tools are adopted / implemented and regularly updated with latest security vulnerabilities information.
- Vulnerabilities and system patches shall be prioritized by the information security team for remediation commensurate with the risk to HUDCO systems, networks and data.
- Vulnerability remediation and patching activity for systems, applications, servers and network devices shall be tracked as per defined timelines.
- Critical patches in test environment shall be evaluated before pushing them onto production systems.
- Expedite the resolution of identified vulnerabilities including ERP Systems, ICT infrastructure.
- Thoroughly review and block websites posing security risks and all non-business-related websites.

20 Cyber Security Preparedness Indicator

- Technical compliance checking shall be conducted at regular intervals by the Information Security Committee either manually or with the assistance of automated tools to assess the level of Information and Cyber risk preparedness.
- All functions should obtain a security clearance for projects, products, applications, services, etc., having information security impact, from the CISO'S office prior to deployment in production environment.
- Technical compliance checking shall cover penetration testing, vulnerability assessments, architecture review which could be carried out internally or by independent experts specifically contracted for this purpose.
- CISO shall report Information Security Preparedness and arrangements to IT Strategy Committee on the quarterly basis.

20.1 Cyber Crisis Management Strategy

Cyber Incident handling activities include:

- Incident Detection
- Incident reporting
- Resolution includes response, containment and remediation.
- Recovery identifies how to safely put the impacted systems back into production.
- Post-remediation review is performed to ensure that the incident has been resolved successfully and its resolution has no security impact on the information asset.
- Root cause analysis identifies the underlying reasons of why an incident occurred, and preparing corrective action plan to eliminate Root Cause.

20.2 Test preparedness to withstand cyber attacks

20.2.1 Exercising and Testing

IT department in coordination with CISO shall develop various exercises such as crisis simulation exercises, mock drills, red teaming exercise etc., which assess the adequacy and consistency of Cyber crisis management plan. Testing exercise shall also be performed to measure the HUDCO defensive and responsive capabilities. These exercises tests are conducted at planned intervals or whenever significant changes occur. Resiliency tests are to be conducted in line with Cyber Crisis Management Plan (CCMP) scope and its objectives. Resiliency tests are to be based on appropriate scenarios that are well planned and clearly defined aims and objectives. Post exercise reports should contain outcomes recommendations and actions to implement improvement.

20.2.2 Cyber Incidence HUDCO Response and Recovery Management

- The cyber incident Response and recovery management policy shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage such incidents, contain exposure and achieve timely recovery.

- HUDCO shall analyze cyber incidents (including through forensic analysis, if necessary) for their severity, impact and root cause. HUDCO shall take measure, corrective and preventive, to mitigate the adverse impact of incidents on business operations.
- HUDCO shall have written incident Response and recovery procedure including identification of key roles of staff/ outsourced staff handling such incidents.
- HUDCO shall have clear communication plans for escalation and reporting the incidents to the Board and Senior Management as well as to customers, as required. HUDCO shall pro-actively notify CERT-In and RBI regarding incidents, as per regulatory requirements.
- HUDCO shall establish processes to improve incident response and recovery activities and capabilities through lessons learnt from past incidents as well as from the conduct of tests and drills. HUDCO, inter alia, shall ensure effectiveness of crisis communication plan/ process by conduct of periodic drills/ testing with stakeholders (including service providers).

20.2.3 Business Continuity Management

Cyber security shall be embedded in the organization's business continuity management systems. Business continuity plan and procedures shall be established and maintained, to ensure continuity of operations in the event of disasters.

- The HUDCO will establish and implement an IT process to support business continuity management to ensure that in the event of a disaster, natural or manmade, the business-critical information processing services and systems are restored within defined time scale.
- The IT Department will be the owner of this process. The process will understand the risk assessment and impact of disasters on business processes and drive the development of disaster recovery and IT contingency plans backed up by their continuous maintenance (improvement).
- The HUDCO will identify the critical business processes and carry out formal risk assessment and business impact analysis due to disruptions caused by disasters to determine the requirements of continuity plans.
- Business continuity plans will be developed based on the requirements identified by the business continuity and impact analysis.
- The HUDCO will define a schedule for periodic testing of the continuity plans. The testing will be to verify that the plans are workable and for training to familiarize staff with the operation of the plans.
- Business continuity plans shall be reviewed and updated at least once in a year.
- The HUDCO will store one set (copy) of all critical backups offsite i.e. away from its premises. The off-site arrangement for keeping backups will be in accordance with classification of the information stored in the backups.

21 Incident Reporting

- All Information and cyber security incidents shall be reported to Information Security Committee.
- Incidents involving compromise of the IT systems of the HUDCO such as data breach, data destruction etc. severely affecting the operations of the company shall be reported to CERT-In/other statutory bodies as per requirement along with the action taken thereon by the HUDCO.
- All information and cyber security incidents shall be recorded in a cyber-security incident database.
- Facility for monitoring shall be set up for proactive monitoring of intrusions, attacks and fraud.
- User community shall be educated on how to identify and report information and cyber security incidents.
- Incidents classified as high, critical should be reported to CISO, Head (IT) and other relevant stakeholders.

22 Digital Signature

Digital Signatures were introduced by the Information Technology Act 2000 and elaborated further in its amendment in 2008. The act provided for the creation of the Controller of Certifying Authorities (CCA) which in turn created Certifying Authorities (CA) which formed the Public Key Infrastructure (PKI) for the country.

Digital signatures are to be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged.

Digital Signatures provide the following three features: -

Authentication- Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions

Non-Repudiation – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

23 Social Media Risks

The purpose of social media guidelines is to provide guidance to the authorized employees for secure use of social media for various business purposes.

Below are the Social media guidelines which HUDCO abide by:

- Only authorized users/vendors shall manage social media accounts.
- Only official HUDCO social media accounts shall be used for social media activities.
- Only secure (https://) social media platforms shall be used by HUDCO.
- Social media accounts shall be operated from HUDCO issued desktops/laptops or authorized Third Party Vendor's systems.
- Only authorized employees should be allowed to post any official comment on social media.
- Employees/vendors are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the supervisor.
- Employees shall get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Although not an exclusive list, some specific examples of prohibited social media content include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, or that can create a hostile work environment.

24 Physical and Environmental Security

The purpose of this policy is to protect information assets as well as supporting services and processes from physical and environmental threats. Physical threats include physical tampering, unauthorized removal, damage and theft. Environmental threats include earthquake, flood, fire, civil unrest and other natural and man-made disaster.

24.1 Secure Areas

24.1.1 Physical Security Perimeter

- It is required that appropriate access to premises and secure areas are maintained to prevent unauthorized individuals from gaining physical access.
- Access to secure areas is given only to visitors who have genuine identifiable reason to visit the secure area.
- It is required that ID badges are issued to individuals before granting access to premises.
- A manned reception area or other means to control physical access to the building should be in place. It is required that access to secure areas are restricted to authorized-personnel only.
- It shall be ensured that access rights to secure areas is regularly reviewed and updated.
- It is required that remote locations where data is processed or stored provides access control and protection which reduce risk of loss or damage to an acceptable level.
- All movements of information assets between location(s) and / or floor(s) are to be controlled by authorized personnel.

- It shall be ensured that access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled to avoid unauthorized access.
- HUDCO Data Center (DC) require to have physical security controls in place that prevent unauthorized individuals from gaining physical access. It is required that these controls include the following:
    - All entry points to the Data Center have access control facility for both entry and exit. It is required that there are technology-based access control solutions like biometrics or access cards.
    - Physical access to Data Center shall be restricted.
    - Cabinets housing servers, disks, tapes and other network equipment are secured with locked doors. All racks in the server room needs to be locked. Access to these racks will be restricted to authorized personnel only.
    - Access to Data Center shall be given only on business need to have and on approval from Head – IT.
    - Access to Data Center is to be approved and logged.
    - Access logs for all the areas requires to be retained for a minimum duration of six (6) months.
    - Access logs to server room shall be reviewed to ensure that only appropriate access is granted.
    - Access control cards with photo-identity may be provided to users who need to access server room on need to have basis.
    - Visitor cards may be issued to non-employees i.e. vendors, auditors, visitors.
    - All the entry points to the server room and movement within the server room shall be monitored by Closed Circuity Television (CCTV). It is required that no physical access / entry points are left unmonitored.
    - Photography and video shooting in server room is prohibited except for the purposes of monitoring movement of people and assets and inventory collection of hard assets with beforehand permission from facility in-charge.
    - It shall be ensured that the security guards ensure that there is no unauthorized movement of IT equipment into or out of server room.
    - It shall be ensured that all the personnel entering the premises declare if they are carrying any IT equipment like storage media or portable storage device. Carrying of portable storage devices

is to be strictly prohibited to ensure against loss of information from server room. If any item needs to be taken out from the server room, it is required that suitable gate pass are issued by authorized personnel and inventory collection of hard assets with beforehand permission from facility in-charge / project in-charge.

24.1.2 Physical Entry

- All visitors have to make an entry in the visitor register at the reception after which a temporary ID card/visitor card is issued which should be worn and is visible at all times whilst on HUDCO premises.
- It shall be ensured that visitors are escorted to and from their destination by a facility employee or the concerned official from HUDCO.
- Laptop, pen drives and other removable storage media are not be allowed into the Data Center without prior approval from Data Center Administrator.
- It is required that employees hosting visitors:
    - Give Site security prior notice of the visit; stating the name and company represented by the visitor.
    - Collect/ return visitor (s) from the reception (or site security desk).
    - Escort the visitor at all times whilst on HUDCO's premises.
- Visitors to secure areas such as operations area are to be supervised, and their date and time of entry and departure recorded.
- It is required that all staff should display their Identity badge at all times when in the company premises.
- Access card issued to all employees, contract employees, and vendor staff are to be used to gain access to control areas within the building. This access card is personal to an individual and hence, it is required that it is not shared with co staff members.
- Access rights would be revoked immediately for staffs that leave employment.

24.1.3 Securing offices, rooms and facility

- Key facilities shall be sited to avoid access by the public.
- It shall be ensured that the facilities are configured to prevent confidential information or activities from being visible and audible from the outside.
- Directories and internal telephone books identifying locations of confidential information processing facilities are not to be readily accessible to anyone unauthorized.

24.1.4 Protection against external and environmental threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. These are required to include:

- Power systems to be designed to provide power, at appropriate levels and quality, without interruption;
- Implementation of appropriate fire protection measures, including installation of fire-suppression systems;
- Adequate redundancy for power sources and no single points of failure is ensured. Appropriate agreements with building administration are to be signed where power sources are managed by them;
- Fire detection and alarm system are to be placed at identified locations inside HUDCO's premises;
- Combustible materials shall be avoided in the server room. Only the minimum supplies absolutely necessary to the functioning are to be kept within the server room. Packing materials and other unnecessary items shall be removed as soon as possible;
- All personnel are to be trained in basic firefighting techniques. Fire drills shall be conducted periodically to check preparedness of the personnel;
- It is required that the temperature and humidity are monitored and controlled as per acceptable standards; and
- Pest Control and rodent control are periodically carried out.

24.1.5 Working in secure areas

- Appropriate physical access controls, are implemented in these areas;
- Employees are provided access to the restricted areas on 'need to have' basis only;
- Entry and exit, as well as, movement of any assets in restricted areas is monitored and recorded;
- Photographic, video, audio or other recording equipment, such as google glass, cameras etc. in mobile devices are not allowed in restricted areas;
- A list of equipment/ devices that are not allowed inside restricted areas is displayed at the entry points; and

24.2 Equipment

- All equipment requires to be correctly maintained to ensure its continued availability and integrity.
- All equipment (including supporting utilities) requires to be physically protected from security threats and environmental hazards.

- Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
- An Uninterrupted Power Supply (UPS) needs to be installed to ensure the continuity of services during outage.

24.2.1 Supporting utilities

- It is required that all supporting services and processes, such as electricity, water supply, heating/ventilation and air conditioning, are adequately scaled for the information assets they are supporting and are regularly inspected and tested.
- Suitable electrical supply is to be provided that conforms to the Original Equipment Manufacturer (OEM) specification.
- UPS and generators shall be installed to support controlled shutdown or continued functioning of information assets supporting critical business operations.
- UPS equipment and generators shall be regularly checked to ensure they have adequate capacity and are tested in accordance with the OEM recommendations.

24.2.2 Cabling Security

- Power and telecommunication network cables shall be protected from damage or unauthorized interception.
- Power and telecommunications lines inside the secure areas shall be underground or adequately protected.
- Power cables shall be segregated from communications cables to prevent interference.
- Documents, including the detailed physical network diagrams, showing cable routings and terminations are held by the facilities head or his designated personnel.
- Monitoring procedures are to be in place to ensure the regular examination for cable/ ducts are done for unauthorized entry.

24.2.3 Equipment Maintenance

- HUDCO shall put in place a robust IT Service Management Framework for supporting their information systems and infrastructure to ensure the operational Resilience of their entire IT environment (including DR sites).
- A Service Level Management (SLM) process shall be put in place to manage the IT operations while ensuring effective segregation of duties.

- HUDCO shall ensure identification and mapping of the security classification (in terms of Confidentiality, Integrity, and Availability) of information assets based on their criticality to the HUDCO' operations.
- For seamless continuity of business operations, HUDCO shall avoid using outdated and unsupported hardware or software and shall monitor software 's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.
- HUDCO shall develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.

24.2.4 Removal of Assets

- For movement of information assets off-premises, it is required that appropriate security measures are followed. Movement of any equipment outside premises is to be accompanied by gate pass.
- All assets moving outside the organization shall be tracked in the material in/out register.
- All returnable assets are to be tracked as per the returning date till the asset arrives back in the organization.
- It is the responsibility of the IT department to track and maintain the updated records of the IT assets moving inside and outside of the organization's premises.

24.2.5 Security of equipment and assets off-premise

- Each user carrying / managing the portable devices / equipment such as Laptops, Cellphones, etc. that is owned or hired by HUDCO will be responsible for the security of equipment;
- All equipment (backup tapes, removable media etc.) must receive an appropriate level of protection against physical and environmental threats;
- The equipment/ media to be couriered are packed providing the adequate physical protection to the equipment / media;
- Equipment installed outside the organization premises undergo basic hygiene check at the time of commissioning and at scheduled intervals thereafter;
- Equipment installed outside the organization premises shall be monitored at specified intervals;
- It is required that a valid gate-pass signed by authorized personnel is issued for any media or equipment moving outside the organization on an ad-hoc basis or for repair; and

- It shall be ensured that there is reconciliation of all returnable gate pass at periodic intervals to ensure that the materials are returned after its intended use/repair.

.

24.2.6 Unattended user equipment

- All HUDCO personnel requires to protect HUDCO information in digital and in physical format that is used or stored at their workspace.
- All HUDCO personnel requires to ensure that their workstations and other equipment's are locked when not in use.
- Users shall terminate/ log-off from applications or network services active sessions when finished.
- It shall be ensured that password protected screensavers are used to protect the system automatically by locking the screens.

24.2.7 Clear desk and clear screen policy

- It shall be ensured that where appropriate, paper and computer media are to be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially during off-office hours.
- At the end of the working day the employee is expected to put away all office papers and files in the cabinets.
- It shall be ensured that Confidential and restricted data are not left in open view after general business hours and are kept in a secured place to prevent unauthorized access.
- Confidential and restricted data in printed format should be disposed-off in a secured shredding bin or a paper shredder in accordance with retention periods in the relevant records retention schedule.

25 Operations Security

Effective and secure operation of information systems and computing devices are to be ensured. Appropriate controls shall be implemented to protect the information contained in and/or processed by these information systems and computing devices.

25.1 Operational procedures and responsibilities

The objective is to ensure the correct and secure operations of information processing facilities.

❖ Documented Operating Procedures

- Standard Operating Procedures (SOP) are to be developed for all information systems, information processing facilities and services in a function and shall be approved by the departmental heads of each department.
- SOP shall be documented to an appropriate level of details for the users. SOP must include but not limited to:
    - Operational tasks that need to be performed;
    - Instructions and guidance for handling errors;
    - System restart and recovery procedures in the event of system failure;
    - Roles and responsibilities of the users performing the task;
    - Potential security implications/ considerations for the critical activities; and
    - Record of approvers and version numbers for all changes made to the procedure document.
- It is required that SOP are reviewed at specified intervals and updated whenever there is any operating change and system change. The updated SOP's are to be duly approved and released, with updated version number, by the respective departmental head.
- For all critical equipment periodically check on updates from third parties on technical guide and/ or user guide.
- All SOPs shall be centrally located and are easily accessible on a 'need to know' basis.

❖ Change Management

It is required that changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.

❖ Capacity Management

- HUDCO shall ensure that information systems and infrastructure are able to support business functions and ensure availability of all service delivery channels.
- On an annual or more frequent basis, HUDCO shall proactively assess capacity requirement of IT Resources. HUDCO shall ensure that IT capacity planning across components, services, system Resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements and projected future needs as per the IT strategy.
- The assessment of IT capacity requirements and measure taken to address the issues shall be reviewed by the ITSC

❖ **Separation of development, test and production environments**

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

25.2 Protection from malware

It is required that HUDCO ensures that precautions are implemented to detect and prevent the introduction of malicious code into information processing facilities through periodic testing.

This control sets out the minimum requirement for managing the risks to HUDCO's computing environment caused by malware such as viruses, worms, Trojan, and spyware, adware, spam, ransomware and keystroke loggers.

HUDCO will define controls to protect its operations system processing facilities against software and virus attacks to ensure availability of IT services without interruptions.

It will include:

1. Use of only authorized software
2. Use of technology for protection against software attacks.
3. Procedure for reporting and reacting to virus attacks.
4. Usage policies.
5. Protection of portable computers.
6. Constant training.

Controls against malware

- HUDCO is required to ensure that malicious code prevention, detection and removal controls are in place in all devices. HUDCO approved Anti-malware software are to be installed, updated and functioning on all HUDCO managed desktops, laptops and servers.
- Proactive patching shall be performed to aid in protecting against malicious software.
- IT Infrastructure team is required to install anti-malware software on all servers, desktops and laptops for which anti-malware solution is available. IT Infrastructure team must install anti-malware software that is fully supported by the vendor.
- All devices and servers shall report to anti-virus software console in order to monitor the devices effectively. IT Department is responsible for monitoring the anti-virus console and submit the report to the Information Security committee for compliance. It is required that periodic reports are generated which should include the following information:
    - Number of machines where the latest signature pattern is not present.
    - Agents not communicating with the console for prolonged duration.

- Updated definition coverage for the endpoints, servers; and
- Latest malware definitions to be updated on all applicable devices every day or defined interval.

25.3 Secure configuration documents and periodic Assessments

Configuration shall base on secure configuration documents. HUDCO shall develop baselines secure configuration document based on OEM recommendations and industries best practices.

Application Security Life Cycle

Applications should have controls to secure input, output and securing of storage.

- For business-critical applications, either source code should be received from the supplier or a software escrow agreement should be in place to ensure source code availability in the event the supplier goes out of business.
- Any application, i. procured from suppliers/OEM, ii. used as an open-source tool, or iii. purchased off-the-shelf should conform to HUDCO's Cyber Security Policy and procedures.
- Secure Software Development Lifecycle (Secure SDLC) should be followed for all new and existing applications throughout the application lifecycle as per established procedure.
- Source code audits should be conducted by professionally competent personnel/service providers or should have assurance from application providers/OEMs that the application is free from embedded malicious or fraudulent code.
- Secure coding practices should be implemented for internally/collaboratively developed applications.
- Procedures should be clearly specified at the initial and ongoing stages of the system for business functionalities and security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking, and exception handling during development/acquisition/implementation.
- Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking, and exception handling should be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.
- The development, test, and production environments should be properly segregated.
- Software/Application development approaches should be based on threat modelling, incorporate secure coding principles, and include security testing based on global standards and secure rollout.
- Software/Application development practices should address vulnerabilities based on best practice baselines such as the Open Web Application Security Project

(OWASP) proactively and adopt the principle of defence-in-depth to provide a layered security mechanism.

- Applications should be updated with the latest patches and hotfixes as per the Change Management - Patch Management Policy.

25.4 Change and Patch Management

HUDCO shall put in place documented policies and procedure for change and patch management to ensure the following:

- The business impact of implementing patches/ changes (or not implementing a particular patch/ change request) are assessed.
- The patches/ changes are applied/ implemented and reviewed in a secure and timely manner with necessary approvals.
- any changes to an application system or data are justified by genuine business needs and approvals supported by documentation and subjected to a robust change management process; and
- Mechanism is established to recover from failed changes/ patch deployment or unexpected HUDCO results.

25.5 Network Management

The network is a key resource for all operations system facilities. The protection of the network is therefore of maximum importance. HUDCO will define wide range of controls for protection of network device, services and the data/ information flowing through its networks. The control will include:

- Basic network connectivity.
- Network availability.
- Protection during transmission.
- Third party connectivity.
- Internet.
- Network administration.

25.6 Segregation in Networks

Network shall be designed in conformance with good network security practices. The network design shall address the following.

- Incorporate coherent technical standards and support consistent naming conventions.
- Security network zones shall be created to segregate system with different criticality levels.
- Minimize single point of failure and number of entry points into the network.

HUDCO network architecture shall be clearly documented and updated as necessary to reflect changes to the architecture.

25.7 Exchange of information and software

Various new modes of information exchange have become available and the use of new modes is increasing. HUDCO has prepare itself for new modes of information exchange.

HUDCO will define controls for the following:

- Information and software exchange agreements.
- Security of media in transit.
- Security of electronic mail.
- Security of internet usage.
- Security of electronic office system.
- Other forms of information exchange.

25.8 Outsourcing

The nature of information processing for operations is undergoing change and outsourcing of some functions will become inevitable. HUDCO must ensure that the services used are from reputable companies with proven track record that operate in accordance with quality standards which should include a suitable service level agreement and non-disclosure agreement which meets the HUDCO requirements. IT outsourcing Policy in this regard is to be complied with.

A risk analysis study will be carried out in order to determine security implications and security control requirements of outsourcing of the information services.

25.9 Data Backup

25.9.1 Information Backup

The IT department is responsible for the setting up of backup process for data held in all servers and related databases.

The IT Department is required to monitor regular backups. The delegated person is required to develop a procedure for testing backups and test the ability to restore data from backups on a weekly basis. It is required that following principles are kept in mind:

- Backup media is to be stored in locked safes which are fire proof safe.
- Databases are backed up in every 24 hours.

25.10 Logging and monitoring

25.10.1 Event logging

- It is required that logging is enabled on all critical information assets including application servers, operating system, database, web servers, and security devices.
- Logging is to be enabled to track critical system activities and are required to include, at a minimum, the following:
    - User account management;

- Privileged user activities including Special Privilege Access;
- Changes in OS configuration;
- Authentication failures; and
- Access to audit trail.

- Faults reported by users or by system programs (i.e. errors) related to problems with information assets are to be logged.

25.10.2 Administrator and operator logs

- File integrity monitoring and change detection software may be used for stored logs to ensure that existing log data cannot be changed without generating alerts.
- Periodic reports are to be submitted to respective team SPOCs, Top Management and concerned stakeholders after reviewing of the logs of the information systems.

25.10.3 Protection of log information

- Access to log information and logging facilities are to be restricted to approved administrative personnel through the use of authentication mechanisms like user ID and password.
- Remote copy of log file shall be maintained in secondary storage or log server for critical IT systems. Only read-only access are authorized for the remote copy of logs.
- Wherever feasible, systems shall be configured to push logs to a central server to avoid deletion by unauthorized users.
- Logs may be encrypted using an acceptable one-way hash algorithm to ensure that the log files are not altered while copying to secondary storage for analysis or preserving audit trails.
- Alerts are to be configured in systems or log server to track log storage capacity. Preventive action by the log management team shall be defined to ensure that event logging does not fail due to overflow or over writing of past record events in the system.

25.10.4 Clock Synchronization

All information systems including application, operating system, database, network and security devices shall maintain time synchronization with a standard time device/ NTP server to provide an accurate and traceable record of logged events.

25.11 Control of operation software

25.11.1 Installation of software on operational system

It is required that there are procedures in place to control the installation of software on operational systems:

- Information systems shall be deployed only after extensive and successful testing. The tests shall include test-scenarios over usability, effects on other systems and user-friendliness.
- The testing activities are to be carried out on separate systems segregated from the production environment.
- During deployment, IT department is required to ensure that adequate logging and auditing capabilities are configured in best possible manner.
- IT Department is required to ensure that previous versions of the information systems are retained as a contingency measure. IT Department also needs to ensure archive of the previous version along with all required information, parameters, procedures, configuration details and supporting software.
- Rollback strategy and plan is to be in place prior to implementing the changes to the production environment.

25.11.2 Restrictions on software installations

- Rules governing the installation of software by users shall be established and implemented.
- It is required that the organization identifies what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect).
- Admin rights of the users would be restricted.
- LAN settings should not be available to the user for any unauthorized modification.
- Removable media ports access is to be provided only to limited users as per business requirement.

25.12 Information system audit control

25.12.1 Information system audit controls

To ensure that the Information Security controls are working effectively, the audit for the information systems shall be performed either by some external auditor for an independent review of the controls that have been implemented.

- Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risks of disruptions of business processes.

- Risk based approach shall be adopted to define the scope of the audit.
- It is required that annual audit schedule, audit requirements and scope of audit agrees upon with the appropriate representatives of business units involved.
- Wherever access to operational system is required, it shall be ensured that it is limited to read only access to software and data. This access is to be removed when the audit is completed.
- Exceptions to above requirement will only be allowed for isolated copies (copies of system files that are not linked to the original) of system files, which shall be erased when audit is completed.
- Audit procedures, requirements, responsibilities and findings are to be documented.
- Access to information system audit tools (for e.g. software and data) requires to be protected through appropriate controls to prevent any possible misuse or compromise.
- It shall be ensured that a Non-Disclosure Agreement is obtained from auditors.

26 Remote Access

It shall be ensured that information security is an integral part of information system across the entire lifecycle and also includes the requirements for information system which provide services over public network.

- HUDCO shall regularly review remote access approvals and revoke those that no longer have a compelling business justification.
- HUDCO should ensure appropriate and timely patching, updating and maintaining all software on remote access devices.
- Encryption should be used to protect communications of critical data between the access device and HUDCO.
- VLAN network, segment, directions and other techniques should be used to restrict remote access to authorized network areas and applications within HUDCO.
- Periodically auditing the access device configuration and patch levels.
- Logging remote access communications, analyzing them in a timely manner and following up on anomalies.
- Centralize modem and internet access to provide a consistent authentication process and to subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring.
- Logging and monitoring the date, time, user, user location, duration and purpose for all remote access including all activities carried out through remote access.

- Requiring a two-factor authentication process for remote access (PIN based token card with a onetime random password generator or token-based PKI)
- Implementing controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive system or database may include the controls like restricting the use of the access device by policy and configuration, requiring authentication of the access device itself and ascertaining the trustworthiness of the access device before granting access.

26.1 Role of an application owner

- Prioritizing any changes to be made to the application and authorizing the changes.
- Deciding on data classification, de-classification and archival procedures for the data pertaining to an application as per relevant policies in agreement with business owners.
- Ensuring that adequate controls are built into the application through active involvement in the application design, development and testing.
- Ensuring that the security of the application has been reviewed.
- Ensure review of access and roles are conducted periodically.

27 Communications Security

27.1 Network Security Management

27.1.1 Network access Controls

- It shall be ensured that network services along with service levels are identified, documented and approved to ensure business requirements are met.
- Network services need to monitored and reported for measuring its performance against agreed service levels.
- Access to critical network devices is to be managed through centralized access control solution for limiting the access to authorized users.
- The use of network diagnostic tools should be strictly controlled to prevent unauthorized users from obtaining sensitive information about the network.
- Only authorized users will be allowed to use Local Area Network.
- Only HUDCO approved Wireless Local Area Networks (WLANs) may be connected to the HUDCO network. All external networking connections are to be made through HUDCO managed network infrastructure and also include network security monitoring.
- Management Virtual Local Area Network (VLAN) shall be different from other VLANs. Wherever feasible, management traffic shall not to traverse the production network. Encrypted communication protocols such as SSH shall be used if in band (over the production network) communication is necessary.

- It shall be ensured that an architecture diagram of the HUDCO network (including wireless network) is documented and kept up to date. Any change in architecture (both high level & low level) is to be informed to Information security department with version control through concerned reporting structure.
- Wireless networks deployed within HUDCO premises shall be approved before implementation. Controls such as secure configuration, encryption and authentication are to be implemented for wireless networks. Management of wireless networks shall be integrated into the overall network security management.
- HUDCO shall ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need.
- HUDCO shall deny access to those wireless devices that do not have such a configuration and profile.
- HUDCO shall detect and classify mobile Wi-Fi devices such as Laptops, iPads, Mobile devices and other portable devices. Where a specific business need for wireless access has been identified, HUDCO shall configure wireless access on client machines to allow access only to authorized wireless networks.
- HUDCO shall regularly scan for unauthorized or misconfigured wireless infrastructure devices.
- Network vulnerability scanning tools shall be configured to detect wireless access points connected to the wired network. Identified devices shall be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points shall be deactivated.
- HUDCO shall use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise. In addition to WIDS, all wireless traffic shall be monitored by a wired IDS as traffic passes into the wired network.
- HUDCO shall ensure wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.
- It shall be ensured that remote access (for e.g. Virtual Private Network (VPN), perimeter firewalls, etc.) to HUDCO Network over an un-trusted network is integrated into the overall network security management.
- All single points of failure within the HUDCO network shall be identified and the risks in such a design shall be assessed. Where possible, failover technologies should be in place to address network failure.

- Load balancing solution shall be implemented for critical network devices in order to ensure effective performance from the devices.
- It shall be ensured that arrangements for back-up of network technologies caters to:
    - The need to recreate 'current' configuration quickly and accurately if such information is lost (where 'current' refers to the last known configuration before failure);
    - Changes in configuration; and
    - Secure storage of this configuration information.
- Logs generated by critical network devices shall be analyzed to identify threats and exceptions.
- Network security may be monitored to provide immediate response to threats.
- Requirements of flow of traffic between HUDCO Networks are to be identified and documented. Inbound and outbound traffic passing through these networks shall be filtered and/or routed via HUDCO managed security technologies such as firewall and/or IDS/IPS.

27.1.2 Security of network services

- A firewall shall be implemented at each connection to an un-trusted network, and between semi-trusted and trusted/highly trusted networks.
- Defense-in-depth through placement of IDS/IPS solution shall be implemented to further control the traffic passing through these networks. These solutions have to be regularly updated with current signatures / characteristics of threats
- Deny-all rule is to be implemented i.e. all services are disabled by default and services are enabled selectively on a case-by-case basis as per requirement.
- Network services, protocols, ports not required for business purposes shall be disabled or turned off. Only services that are formally approved will be activated.
- List of approved services are to be identified, documented and approved which shall be enabled on the network.
- It is required that network traffic is constantly monitored and if any unapproved service is found to be enabled, it is disabled.
- Known insecure protocols such as File Transfer (FTP) and Telnet are not to be permitted on HUDCO-managed network technologies. For exceptions to this requirement, business justification and information security committee approval shall be obtained. It shall be ensured that

mitigating security controls are implemented to address the risks associated with these protocols.

- The consideration given to the security and business implications of interconnecting HUDCO and third-party networks are required to include the following:
    - Vulnerabilities in the information systems where information is shared between different parts of the organization;
    - Appropriate controls to manage information sharing; and
    - Restricting access to information relating to selected individuals, e.g. personnel working on sensitive projects.
- Usage of network sharing protocols (like SMB V1) should be minimized.

27.1.3 Segregation in networks

- It shall be ensured that network is addressed from a well-defined block of IP addresses so that the edge filters at egress points may block inbound traffic to the infrastructure.
- Network is to be segmented into subnets based on function and possibly location.
- Each of the networks shall be further segregated into separate VLANs based on business and security requirements.
- It shall be ensured that that HUDCO network is classified into zones as Web, Application, or Database. Following criterion shall be used for classifying zones:
    - Level of trust associated with each network; and
    - Sensitivity of information stored on or passing over the network.
- Publicly accessible systems, that is, HUDCO systems accessible from an un-trusted network (e.g. Web Servers) shall be located on an HUDCO semi-trusted network
- State-full inspection shall be implemented to allow only approved connections into the trusted and highly trusted networks.

27.2 Information Transfer

27.2.1 Information transfer policies and procedures

- Information owner is to be responsible for defining the recipient parties. It shall be ensured that the information is to be exchanged across the function based on business requirements.
- Personnel shall not discuss sensitive information over phone or with a colleague when in a public place unless they have taken precautions of not being overheard or intercepted.

27.2.2 Agreements on information transfer

- It shall be ensured that an agreement for the exchange of information/ software between HUDCO & third parties is established and well documented.
- Exchange agreements shall be addressed in the following security considerations:
    - Management responsibilities for controlling and notifying about transmission, dispatch, and receipt;
    - Electronic Information is to be shared only on organization e-mails;
    - Electronic Information is to be encrypted when sent over e-mail;
    - Information in paper form shall be sent through approved courier agency;
    - Responsibilities and liabilities in the event of information security incidents, such as loss of data;
    - Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; and
    - Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations.

27.2.3 Electronic Message

The following are prohibited/ deemed unacceptable use of HUDCO email resources:

- Sending emails that exhibit the following characteristics:
    - Attachments with file extensions which are susceptible to malware. E.g. .exe, .vb, .vbs and .com
    - Attachments that contain non-business-related information like music or video files
    - Containing malware
    - Information construed as spam or phishing
    - Emails that are deemed unacceptable by the HR or similar function
    - Distributing hoaxes and chain emails
    - Unless specifically delegated to a particular user, user should not intercept, or disclose emails intended for someone else within or outside HUDCO

  - Engaging in any form of mail spoofing, including attempting to send mail such that its origin appears to be another user or machine, or a non-existent machine
  - Sending, forwarding and/or replying to a large list of recipients concerning non-business-related matters.

- All use of HUDCO email resources is subject to the organization's content filtering rules.
- The Email system of HUDCO are not to be used for creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or/and national origin etc. Employees who receive any email with a content of this nature from any other employee are required to report the matter to information security committee.
- Employees shall exercise utmost caution when sending any email from inside HUDCO to an outside network. Sensitive information is not to be forwarded via any means, unless that email is critical to business and is encrypted.
- Any special privilege is to be approved by Head – Information security. It shall be ensured that the logs of any such activity is forwarded to the Information Security committee.
- Non-business email accounts shall not to be used to receive or send HUDCO information.
- Users who receive spam or phishing emails shall to promptly inform Information Security committee and report the same.
- Users owning HUDCO provided email accounts are to be fully responsible for the content of email originated, replied or forwarded from their account to other users within or outside HUDCO.
- Users shall exercise caution in providing their email account or other information to websites or any other Internet forum like mailing list or social networking website.
- Virus or other malware warnings and mass mailings from Organizations Email System shall be approved by department heads/managers before sending. These restrictions should also apply to the forwarding of mail received by HUDCO employee.
- HUDCO employees have no expectation of privacy in anything they store, send or receive on the company's email system. The Organization may monitor messages without prior notice.
- Only HUDCO approved instant messaging services are to be used.

28 Systems Development, Acquisition and Maintenance

28.1 Security requirements of information systems

28.1.1 Information security requirements analysis and specification

- Based on business need, requestor (management or business users) is required to submit their requirements on a predefined template, based on their understanding of their functionality need, to the IT Department.
- Respective department heads have to evaluate this proposal after performing a feasibility study. This study should include:
    - Current deficiencies.
    - Expected benefits.
    - Functional requirements to be provided by the software.
    - Alternate off-the-shelf products and solutions available in the market; and
    - Estimated cost in terms of manpower required and other software / hardware required for developing the solution.
- Project managers and other department heads shall be kept in loop information security committee to ensure security & compliance of the proposal.
- The feasibility study report is to be analyzed in terms of cost & benefit and any of the following decisions may be made
    - Develop the product (in-house or outsourced).
    - Buy a Commercial Off-The-Shelf (COTS) product.
    - Buy the product and customize or reject the request.
- Project managers and department heads are required to assess the interoperability of the proposed solution with the existing application & environment.

28.2 Security in development and support processes

28.2.1 Secure development policy

- Security requirements shall be incorporated during the design phase.
- Security checkpoints within the project milestones shall be reviewed & documented.
- It is required that the developers ensure of ensuring industry best practices and application security standards such as Open Web Application Security Project (OWASP) is adhered during development process.
- Version control is to be followed and repositories it should be secured.

28.2.2 Restrictions on changes to software packages

- Vendor-supplied software packages should not be modified as far as possible without consulting the vendor.
- Any requirement for change to such software shall be controlled and undergoes the change management procedure.
- If changes are essential, then original software are to be retained, and changes could be applied to a clearly identified copy.

28.2.3 Secure system engineering principles

- Secure information system engineering procedures based on security engineering principles shall be established, documented and applied to in-house information system engineering activities.
- It is required that the security is designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility.
- New technology is to be analyzed for security risks and the design shall be reviewed against known attack patterns. These principles and the established engineering procedures are to be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process.
- It shall be ensured that they are also regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.
- The established security engineering principles shall be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources.

28.2.4 Secure development environment

- Segregation between different development environments e.g. test, development and production is to be ensured.
- Restriction on access to development environment should be on a need to know basis.
- Data movement from and to the development environment shall be controlled.

28.2.5 Security in system files of operational systems

Security policies will be defined to ensure that the distribution of system software files and system configuration data is controlled and monitored to ensure their integrity and availability and to stop authorized access. The

Operational system files must also be kept separate from development and test systems.

28.2.6 Securing application services on public networks

All information involved in application services passing over public networks undertaken by HUDCO shall be protected from any fraudulent activity, contract dispute, unauthorized disclosure, and modification and/or destruction

28.2.7 Outsourced development

- Information systems acquisition shall be done as per the approved procurement policy.
- Upon evaluating the feasibility study, Project Managers and Department Heads need to move forward with information systems acquisition by reaching out to the various vendors with the required functionality document.
- Project Managers and the purchase committee are required to perform vendor evaluation.
- HUDCO's priorities, constraints, risk tolerance, and assumptions are to be established and used to support decisions associated with managing supply chain risks. HUDCO has to establish and implement the processes to identify, assess and manage supply chain risks.
- Cybersecurity supply chain risk management strategy/ process shall be identified, established, assessed, managed, and agreed to by organizational stakeholders.
- Suppliers and third-party service providers of information systems, components, and services shall be identified, prioritized, and assessed using a cyber-supply chain risk assessment process.
- HUDCO shall establish a comprehensive vendor risk assessment process and implement controls that are proportionate to the identified risk and materiality. This process shall aim to:
    - mitigate concentration risks
    - prevent or address conflicts of interest
    - reduce risks associated with single points of failure
    - ensure compliance with applicable legal, regulatory requirements, and standards for customer data protection
    - maintain high availability to ensure uninterrupted customer service effectively manage supply chain risks.
- Information Systems that is to be acquired, shall be evaluated based on the following:

- Feasibility to business requirement
- Vendor commitment;
- Vendor support;
- Commercial considerations;
- Technical skills; and
- Ability to meet information security requirement

- Appropriate validation controls (input and output) and information processing controls are built into the software.
- Adequate cryptographic & key management controls are constituted in the software to provide appropriate protection of data.
- The software code is assessed internally to check for the security vulnerabilities
- Upon vendor finalization, as part of the acquisition checklist, IT Department requires to confirm that the vendors provide the following minimum requirements:
  - Software details (Module/Suite purchased).
  - Authentication (User ID, LDAP/Active Directory).
  - Hardware requirements (Server, RAM, Client Requirements).
  - Architecture (Client-server/Web/Virtualization).
  - Network Requirements (LAN/WAN, firewall, Port, Protocol details).
  - Database requirements.
  - Supporting documentation (Software Manuals).
- Software acquired should be updated in the asset register, detailing the name, vendor, license details (license number and date of expiry) and support service details (service contact, location and escalation matrix).
- Information security questionnaire to be duly filled by the vendor as per Third Party Risk Management Procedure.

28.2.8 System security testing

- It is required that HUDCO ensures thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities.
- New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.

- For in-house developments, such tests are to be initially performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected.
- User acceptance testing is then to be undertaken to ensure that the system works as expected.
- It is required that new application & services before deployment in production have a vulnerability assessment scan report which is made available by the vendor.

28.3 Test Data

28.3.1 Protection of test data

- All test data, temporary accounts and temporary passwords including personal identifiable information (PII) shall be removed from the systems prior to deploying them into the production environment. Further, generic accounts wherever possible shall be removed.
- The test environment shall be managed under the same general control environment as the production environment.
- Test data shall be selected carefully, and protected and controlled.

29 Suppliers Service Delivery Management

29.1 Monitoring and review of supplier services

- Service reports and evidences provided by the supplier have to be reviewed at regular intervals.
- Review of supplier audit trails and records of security incidents, operational problems, failures, fault logging and disruptions shall be done regularly.
- Respective departments in consultation with the Legal and Purchase Department, are required to review the service level agreement in case of any exceptions to the SLA. The following aspects shall be considered during the review:
    - Problems related to the services;
    - Identification of the service trends;
    - If the service levels do not meet agreed SLA, then actions taken for improvement;
    - Changes to scope of services;
    - Acceptable range of service levels;
    - Changes to monitoring or reporting procedures; and
    - Changes in penalty structure.

- Any change to the service is to be agreed, documented and approved.

29.2 Managing changes to supplier services

Significant changes to supplier's services shall be informed to the Information system committee. Such changes are:

- Take into account criticality of business system and processes involved
- Be accompanied by re assessment of risks.

Changes to the contracts with the suppliers are to be reviewed and approved in accordance with the policy.

30 Project Management

- HUDCO shall adopt a consistent and well-defined project management approach for IT projects undertaken by the organization. This approach shall include appropriate stakeholder participation to ensure effective monitoring and management of project risks and progress.
- When adopting new or emerging technologies, tools, or upgrading the existing technology stack, HUDCO shall follow a standardized enterprise architecture planning methodology or framework.
- The adoption of new or emerging technologies shall align with HUDCO's overall Business/IT strategy and risk appetite. It should support the secure and resilient creation, use, or sharing of information across the organization.
- HUDCO shall maintain an enterprise data dictionary to enable seamless data sharing across applications and information systems, fostering a common understanding of data.
- HUDCO shall ensure that software applications are adequately maintained and supported by software vendors, with formal agreements in place to enforce this requirement.
- HUDCO shall obtain the source codes for all critical applications from their vendors. Where obtaining of the source code is not possible, HUDCO shall put in place a source code escrow arrangement or other arrangements to adequately mitigate the risk of default by the vendor. HUDCO shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.
- HUDCO shall obtain a certificate or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. Such a certificate or a written confirmation shall also be obtained whenever material changes to the code, including upgrades, occur.
- Any new IT application proposed to be introduced as a business product shall be subjected to product approval.

31. Data Migration Controls

The data migration process is mandatory for smooth transition from the legacy systems to the new system for business continuity after Intellect going live. The migration process will facilitate transfer of data without any loss when it is migrated to the new system and at the same time will ensure the integrity of the data migrated by means of performing various integrity checks before and after migration. The migration would provide the business an option to clean up the existing data.

HUDCO shall have a documented data migration strategy specifying a systematic process for data migration, ensuring data integrity, completeness and consistency. The document shall, inter alia, contain provisions pertaining to signoffs from business users and application owners at each stage of migration, maintenance of audit trails, etc.

32. Straight Through Processing

- In order to prevent unauthorized modification of data, HUDCO shall ensure that there is no manual intervention or manual modification in data while it is being transferred from one process to another or from one application to another, in respect of critical applications.
- Data transfer mechanism between processes or applications must be properly tested, securely automated with necessary checks and balances, and properly integrated through "Straight Through Processing" methodology with appropriate authentication mechanism and audit trails.

33. Conduct of Vulnerability Assessment (VA) / Penetration Testing (PT)

- For critical information systems and/or those in the De-Militarized Zone (DMZ) having customer interfaces, VA shall be conducted at least once every six months, and PT at least once every 12 months. Additionally, HUDCO shall conduct VA/PT for such information systems throughout their lifecycle (pre-implementation, post-implementation, after major changes, etc.).
- For non-critical information systems, a risk-based approach shall be adopted to determine the requirement and periodicity of conducting VA/PT.
- VA/PT shall be performed by appropriately trained and independent information security experts/auditors.
- In post-implementation scenarios (e.g., IT project/system upgrades), VA/PT shall be conducted in the production environment. Under unavoidable circumstances, if PT is conducted in a test environment, HUDCO shall ensure that the version and configuration of the test environment closely resemble the production environment. Any deviation must be documented and approved by the ISC.
- HUDCO shall ensure that identified vulnerabilities and associated risks are addressed promptly by implementing necessary corrective measures and ensuring sustained compliance to prevent the recurrence of known vulnerabilities, such as those listed in the Common Vulnerabilities and Exposures (CVE) database.

- HUDCO shall establish a documented approach for conducting VA/PT, covering scope, coverage, vulnerability scoring mechanisms (e.g., Common Vulnerability Scoring System), and all related aspects. This approach shall also apply to HUDCO's information systems hosted in a cloud environment.

34. Cyber Crisis Management Plan

- The Cyber Crisis Management Plan (CCMP) aims to ensure a systematic, coordinated, and effective response to cyber incidents that may disrupt HUDCO's operations, compromise sensitive data, or impact stakeholders. The plan focuses on minimizing the impact of such incidents and ensuring rapid recovery to normalcy.
- The Information Security Policy shall take into consideration, inter alia, aspects such as the objectives, scope, ownership and responsibility for the Policy; information security organisational structure; exceptions; compliance review and penal measures for non-compliance of Policies. HUDCO's shall also put in place a Cyber Security Policy and Cyber Crisis Management Plan (CCMP).
- Effective CCMP shall accomplish the following goal:
    - Develop and implement a tailored strategy for managing the cyber incident and crisis communication
    - Protect and enhance reputation through diligent crisis management and communication
- Cyber Crisis Management Plan is the ability and readiness to manage business interruptions in order to provide continuity of services at a minimum acceptable level and to safeguard the HUDCO 's financial and competitive position. CCMP addresses the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. The categories covered in the Cyber Crisis Management Plan are:

    - Organization of crisis management
    - Crisis management procedure and lifecycle
    - Crisis management and communication guidelines
    - Cyber Security Threats
    - Sharing of information on cyber-security incidents with RBI
    - Cyber Security Incident Reporting Form
    - Guidelines for handling digital evidence

34.1 Purpose of CCMP

The purpose of a Cyber Crisis management Plan (CCMP) is to enable HUDCO to recover or maintain its activities in the event of a Cyber Crisis affecting normal business operations. The CCMP aims at establishing a formal response structure with representation from key stakeholders to assist the HUDCO effectively responding to a crisis and ensure recovery and restoration of its affected systems within the expected time duration, thereby minimizing business impact.

Effective CCMP shall accomplish the following goal:

- Develop and implement a tailored strategy for managing the cyber incident and crisis communication.
- Protect and enhance reputation through diligent crisis management and communication

34.2 Scope of Cyber Crisis Management Plan

This cyber crisis management plan is a well-defined and documented plan of action for use at the time of a crisis leading to adverse consequences like non availability/ downtime of systems typically covering key personnel, resources, services and resulting actions.

34.3 Crisis Management Team

Crisis Management Team (CMT) of HUDCO is established for seamless coordination and decision making in the event of cyber crisis.

a) The CMT shall consists of the following officials:
b) Chairman and Managing Director (CMD)
c) Head (IT)
d) Chief Information Security Officer (CISO)
e) Heads of the concerned departments related to the crisis
f) Information Security Team members

In case of any crisis related to the availability of information assets, BCP will be invoked. In case the crisis affects confidentiality and integrity, cyber crisis management plan (CCMP) shall be invoked. While invoking the CCMP, whenever there is a need to establish business continuity, BCP shall be invoked under CCMP.

The Crisis Management Team shall ensure the following:

- Ensure that HUDCO procures relevant threat intelligence feeds (through implementation of SOC and advice Financial Institution on corrective actions required to comply with the advisories/threat feeds.
- Meet periodically (at least annually) to discuss the efficacy of the formulated Crisis Management Plan.
- Analyze the crisis situation and its impact on the business
- Take the decision of invoking the cyber crisis management plan basis the identified incident and assessing the criticality of incident. CMT will co-ordinate with respective heads and inform the affected departmental heads.
- Adhere to all process activities of the CCMP
- Provide guidance to relevant stakeholders to ensure recovery from the cyber crisis
- Ensure adequate evidence collection and investigation for the crisis management

- Discuss lessons learnt from past crisis and consequently improving the cyber security controls, Cyber Security Policy and Cyber Crisis Management Plan.
- Formulate the crisis resolution team when the Cyber Crisis Management Plan is invoked. Prioritize the activities for handling of crisis. This cyber crisis resolution team shall help to decide the strategy and steps required for incident response
- Determine the scope of investigation of root cause and impact on Financial Institution when a cyber crisis occurs.
- Co-ordinate with various regulators / governing bodies / agencies such as CERT-In, RBI, Cybercrime cell of Police etc. depending on the nature and severity of the crisis.
- Arrange external assistance in cases where the internal crisis management team cannot handle the crisis.

34.4 Crisis Management Procedure

34.4.1 Detection and initial Reporting

An incident can be reported by anyone in HUDCO environment; however, it is typically reported by one of the following persons/ groups involved in managing and monitoring resources/ services:

1. IT Department officials
2. Security Operations Centre (SOC) Team
3. Network and System Support (NSS) Engineers
4. Web/System/Network / Database Administrator
5. Administration (Physical Security) Team
6. CISO
7. Head of the business unit
8. End Users including Customers and Suppliers

All security incidents or violations of security policies that an end user is aware of, witness or is informed should be reported to IT Department and CISO.

34.4.2 Defining Crisis

After analysis of the information and the circumstances, CISO in consultation with IT Department Head shall classify the incident as a Cyber crisis.

34.4.3 Invocation of Crisis

- CISO, in consultation with the IT Head, shall declare the Crisis and request for convene the CMT meeting.

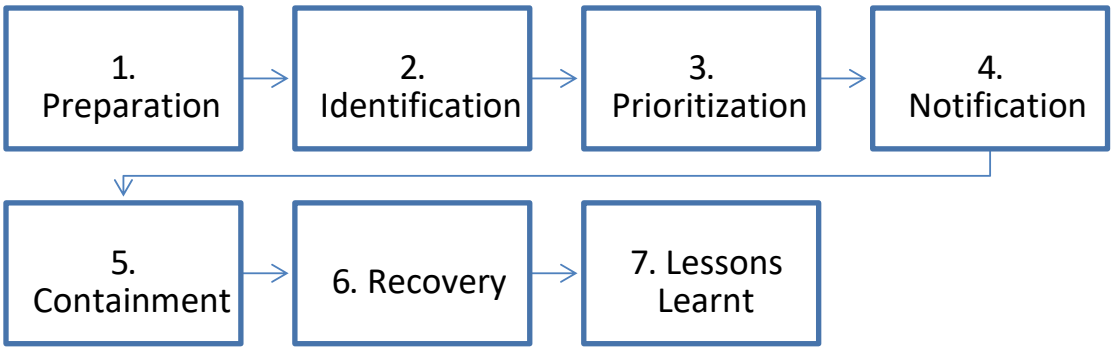
- CMT will co-ordinate with respective departments for cyber crisis management plan invocation.
- CMT shall inform the crisis resolution team. It is the responsibility of the crisis resolution team to carry out the mitigation plan and remediate the cyber crisis.

34.4.4 Crisis Resolution and Post crisis Communication

It is the responsibility of the crisis resolution team to carry out the mitigation plan and remediate the cyber crisis. The CMT shall remain active till the time crisis is resolved completely and recovery of business operations is ensured. Upon crisis resolution, CMT shall drive the post crisis communication amongst stakeholders.

34.4.5 Cyber Crisis Response Methodology

The various stages for responding to the cyber crisis are pictorially represented in figure below-



34.4.6 Preparation

The preparation phase in the HUDCO will focus on training, access to resources, and threat awareness for incident handling personnel. In addition to incident handling processes, some vital areas into which Financial Institution should be well trained but not limited to be:

- System hardening
- Threat Modelling
- Online monitoring and analysis of System logs
- Penetration Testing tools and techniques
- Forensic readiness as per the Information Security Policy and Cyber Security Policy
- Network devices and Firewalls
- Cyber resilience exercises such as DDoS simulation testing, phishing campaigns etc.

    - Incorporation of learning out of cyber resilience exercise in crisis management plan
    - Periodic testing of Cyber Crisis Management Plan Below guidelines shall be used for crisis readiness:
- Contact information for team members and others within and outside the Financial Institution (primary and backup contacts), including law enforcement and other crisis resolution team. Information will include phone numbers, email addresses, and instructions for verifying the contact's identity
- On-call information for other teams within the organization, including escalation information.
- Crisis reporting mechanisms, such as phone numbers, email addresses, and/or online forms that users can use to report suspected incidents.
- Cell phones to be carried by team members for off-hour support and onsite communications.
- "War room" for central communication and coordination: If a permanent war room is not necessary or practical, the team should create a procedure for creating a virtual environment for crisis management

34.4.7 Triggers for Incidents:

- Observation of certain symptoms and anomalies in the functioning of systems, networks and processes.
- Alerts noticed on the Financial Institution's security tools such as Security Incident and Event Management (SIEM).
- Infection, attack or intrusion or malfunctioning of a system or reported loss of damage to information assets/systems
- Alerts are received from external organizations such as CERT-In and other regulatory teams/ security agencies.

34.4.8 Symptoms of incidents and response actions:

The general symptoms indicating occurrence of incident noticeable by all types of users, source of detection, response actions required and persons responsible for the actions.

Following activities should be performed as a part of this phase:

1. Ensure all activities, results and decisions taken are logged for future analysis.
2. Ensure that evidence is gathered, stored securely and monitored continuously.
3. Conduct analysis to understand if the event is a possible cyber security incident or a false alarm.
4. If it is confirmed to be a cyber-security incident, classify the incident as per the incident classification criteria, communicate the result to CMT

5. Based on the events reported to the CMT and the pre-defined criteria for crisis, CMT shall classify the incident into a crisis and invoke the Crisis Management Plan.
6. In cases of a crisis, CMT shall also assign an initial crisis rating which is subject to change through the crisis.
7. CMT shall execute their defined responsibilities during the crisis invocation phase
8. CMT shall arrange for the following key activities:
    - Analyze system/network anomalies and events occurred
    - Analyze the incident based on the data/alerts available
    - Retrieve logs from affected systems from log sources such as local logs, syslog, active directory and alerts from security devices such as firewalls, IDS/IPS etc. for at least 3 months to conduct detailed analysis of incident in later phases.
    - Raw logs are essential for further investigations and as evidence in legal proceedings. Retrieval of logs and their safe storage should be a priority of the teams responding to the crisis
    - Logs shall be analyzed for at least 24 hours prior to incident
    - This analysis has to be reported back to the CMT within 60 minutes of a crisis being declared. The analysis shall also contain possible means to contain the crisis. (Note that RBI has given a window of two – six hours for initial incident reporting)
    - In case no suspicious event is found within afore mentioned time, analysis should be conducted for broader time frame.

34.4.9 Notification

Internal Stakeholder Notifications:

IT Head and CISO who will be actively participating in the recovery procedures would be notified over telephone. Other end users, if affected, would be notified either through direct mail or through respective Head-of-departments (who would be informed over telephone). Communication would include the details of affected services (Application, web portals, email service or overall network connectivity), cause of disruption and approximate time required for resuming operations.

External Stakeholders Notifications:

- Leadership team would be briefed on the situation.
- Company spokesperson would be identified and briefed of the situation.
- Company statements would be prepared and issued to the media and other organizations, if required.
- Media coverage broadcast would be organized and facilitated, if required.
- Changing events associated with the emergency would be continually adapted.

Regulatory bodies i.e. CERT-In/RBI, NCIIPC etc. would be duly notified about the crisis within defined time from the initial incident detection, if such crisis adversely affects external entities.

34.4.10 Containment

Two major containment strategies that may be utilized for handling the crisis are:

Immediate containment:

In this scenario the host (or hosts) is removed / isolated from the network. This is a standard procedure for malware and hosts that are generating malicious traffic

1. In this scenario, both the source and the affected systems have to be isolated from the Financial Institution's network.
2. An isolation can be performed by one or more of the following:
   - Physically disconnecting the network connection of the affected system
   - Logically isolating the affected system or the network segment. The scenarios may include isolating from internet, other critical segments, user segments, etc.
   - Disabling a user's login
3. Decision to isolate should be taken based on the initial understanding of compromise, business continuity procedures, sufficiency of disaster recovery plan
4. In case it is a challenge to isolate the systems or the need for isolation is not felt, all business and non-business transactions should be analyzed by the business teams for a period of at least 24 hours prior to the crisis or till the root cause of crisis is ascertained.
5. If required, the CMT should take a call to invoke BCP crisis to ensure switchover to DR site to run the business operations smoothly.

Delayed Containment:

- This strategy is used by crisis resolution teams that are trying to gather additional evidence by observing bad actors in progress before containing the event. This is an advanced strategy that will not take place unless under an extreme circumstance. However, in the event of a vital production machine, it may not be possible to immediately remove it from the network for containment.
- This strategy is used by crisis resolution teams that are trying to gather additional evidence by observing live patterns before containing the event.
- This is an advanced strategy that will not take place unless under an extreme circumstance or when the further relay of transactions or messages can be contained.
- The delayed containment strategy needs to be carefully performed, as an attacker could escalate unauthorized access or compromise other systems. Even in delayed containment, there should be certain level of initial

containment such as isolating the affected segment but delaying the containment of the affected systems

- The containment strategies shall be decided based on the business impact.

34.4.11 Recovery

Immediately on the escalation of the incident to a crisis, Departments will implement their contingency plans. The response action will be initiated in consultation with CMT, if the situation has wider ramifications and warrants response at the Financial Institution level. The War Room will be activated by CMT.

The response plan outlines the indications of different types of Cyber Crises generally noticeable by users, System Administrators and tool-based detection mechanisms and Response actions.

The steps necessary to mitigate crisis will vary with respect to nature and severity

34.4.12 Lessons Learnt

After successful mitigation and recovery from crisis, the following is required to be undertaken (before closing the incident) for future reference/precaution:

1. Perform a post-crisis analysis as well as the crisis response adopted at the organization and department level.
2. Evaluate and perform assessment of the attack from the technical point of view in order to fine-tune and optimize the eradication mechanism.
3. Document lessons learnt from the crisis and prepared crisis report, including infrastructure protection improvements from the post crisis.
4. Following activities should be performed as a part of lessons learnt:
    - Prepare a lesson learnt document which should contain details of the affected system, how was the access gained, how much was the damage and potential damage if cyber crisis management plan was not invoked
    - Identify trends/patterns with previous attacks
    - Identify areas of concern
    - Analyze what preventive action can be taken to reduce the likelihood of such crisis in the future
    - Identify and make improvements in the information and cyber security controls implemented
    - Identify and make improvements in the information and cybersecurity risk assessment frameworks
    - Update the security event/incident/vulnerability database
    - Identify and make improvements in the cyber crisis management plan

5. Confirmation of the treatment of the crisis shall be recorded and sent to as part of post crisis activity. Detailed root cause analysis (RCA) shall be captured by the department Heads.

6. IT Department, in consultation with CISO Office, shall implement measures to strengthen the infrastructure configuration to protect such crisis in future. Any physical and environmental security controls to be implemented/ enhanced for this purpose, shall be the responsibility of facilities/ building management department.

7. Share incident report with CERT-In, RBI, etc., as required. This activity will be performed by CISO.

35. Cyber Attack Life Cycle

The steps in a cyber-attack lifecycle are explained below:

Step-1: Intelligence gathering or reconnaissance:

During this phase of cyber-attack, criminals, cybercriminals or hackers carefully study their victims and plan their attacks, often using social engineering, phishing, email address harvesting, and other tactics to research, identify, and select targets. They also use various tools to scan networks for vulnerabilities, services, and applications that can be exploited

Step 2: Initial Exploitation:

The attacker determines the malware payload and the method that will be used to deliver it. For example, data files or web pages can be weaponized with exploits that are used to target the victim's vulnerable software and delivered via an email attachment or drive-by download. A drive-by download delivers advanced malware or an exploit in the background, without the user's knowledge, usually by taking advantage of a vulnerability in an operating system, web browser, or other third- party application. The attacker generally has two options for exploitation:

- Social engineering is a relatively simple technique used to lure someone into clicking a malicious link or opening a malicious executable file, for example.
- Software exploits is sophisticated technique since they essentially trick the operating system, web browser, or other third- party software into running an attacker's code. This means the attacker has to craft an exploit to target specific vulnerable software on the endpoint. Once exploitation has succeeded, an advanced malware payload can be installed.

Step-3: Command and Control (CnC):

Communication is the lifeblood of a successful attack. Attackers must be able to communicate with infected systems to enable command and control, and to extract stolen data from a target system or network. This communication can also be used by the attacker to move laterally, targeting other systems on the victim's network. Thus, the initially infected target may only be the first entry point that enables lateral

movement toward the attacker's ultimate objective. CnC communications are generally stealthy and can't raise any suspicion on the network. Such traffic is usually obfuscated or hidden through techniques that include the following:

- Encryption with SSL, SSH, or some other custom application.
- Circumvention via proxies, remote desktop access tools, or by tunneling applications within other (allowed) applications or protocols.
- Port evasion using port hopping to tunnel over open or nonstandard ports.
- Fast Flux (or Dynamic DNS) to proxy through multiple infected hosts, reroute traffic, and make it extremely difficult for forensic teams to figure out where traffic is really going.

Step-4: Privilege escalation:

Once a target endpoint has been infiltrated, the attacker needs to ensure persistence (resilience or survivability). Various types of advanced malware are used for this purpose, including the following:

- Rootkits are malware that provides privileged (root-level) access to a computer
- Boot kits are kernel-mode variants of rootkits, commonly used to attack computers that are protected by full disk encryption.
- Backdoors enable an attacker to bypass normal authentication procedures in order to gain access to a compromised system and are often installed as a failover, in case other malware is detected and removed from the system.
- Anti-AV software may also be installed to disable any legitimately installed antivirus software on the compromised endpoint, thereby preventing automatic detection and removal of malware that is subsequently installed by the attacker. Many anti-AV programs work by infecting the master boot record (MBR) of a target endpoint.

Step-5: Data Exfiltration:

Attackers have many different motives for an attack and data exfiltration including data theft, destruction of critical infrastructure, hacktivism, or cyber terrorism. This final phase of the attack often lasts months or even years, particularly when the objective is data theft, as the attacker uses a low-and- slow attack strategy to avoid detection

Type of Threats

Threat	**Possible reason for attack**
Unsophisticated attackers	The possible reason for such a threat is due to existence of the Bank over the internet and having a vulnerability

Sophisticated attackers	The possible reason for such a threat is due to existence of the Financial Institution over the internet and having information of value
Threat	**Possible reason for attack**
Corporate espionage	The possible reason for such a threat is an attempt to gain access to trade secrets through dishonest means
Organized crime	The possible reason for such a threat is to achieve financial gain
State-sponsored attacks and advanced persistent threat	The possible reason for such a threat is due to the type of work the Bank does and the value of its Intellectual Property

35.1 Cyber Attack Prevention Strategies

Cyber resilience is defined as the ability of HUDCO to anticipate, withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact caused due to cyber-attacks. Below are the practices to be followed to withstand Cyber-attacks:

Test preparedness to withstand cyber attacks

IT Department in co-ordination with CISO shall participate in drills. These exercises and tests shall be conducted at defined intervals.

35.2 Cyber Security Preparedness indicator

The adequacy of and adherence to cyber resilience framework is assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators will be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The aim is to identify the controls, measure the effectiveness, identify the areas of concern and then establish a plan to close the gaps (from cybersecurity perspective). The awareness among the stakeholders including employees may also form a part of this assessment

35.3 Security Operation Center (SOC)

The objective is to setup the SOC at the earliest. SOC will enable continuous monitoring and be able to combat against the ever-changing threat landscape. Proactive monitoring and management capabilities will be the key features of SOC. Quick detection and rapid response are the key factors which would strengthen the governance aspect of cybersecurity. In order to achieve this, the key enablers of SOC are:

- Monitor, analyze and escalate security incidents
- Develop Response - protect, detect, respond, recover
- Conduct Incident Management and Forensic Analysis

- Co-ordination with relevant stakeholders within the FI /external agencies

HUDCO will ensure that HUDCO's SOC is integrated, operated and 24*7 monitored, equipped with set of tools such as, Security Information and Event Management (SIEM), Threat Intelligence Platforms (TIP), and all other tools that are required to comply to the scope and service levels.

36. Secured Cloud Services

- Cloud services follow a shared responsibility model for security and compliance. It is advised to thoroughly examine these models and implement appropriate security policies and measures for testing, staging and backup environments hosted on cloud services
- Check public accessibility of all cloud instances in use. Make sure that no server/storage is inadvertently leaking data due to inappropriate configurations.
- Implement least privilege principle for access control with granular permission to cloud resources
- Enable cloud native security controls along with logging for critical cloud resources and ensure continuous monitoring
- Ensure User Accounts have Multi Factor Authentication (MFA) with strong password policy along with a procedure / standard for disabling of the account when an administrator / user leaves an organisation.
- HUDCO should clearly document the Cloud service models and services procured.
- HUDCO should establish a well-defined cloud security framework that incorporates the following security layers:

    - Physical and Logical Security
    - IT Infrastructure Security
    - Application and Process Security
    - Data and Information Security
    - Cloud Security Management

- **Identity and Access Management:** HUDCO should define controls for access to data hosted on the premises of the cloud service provider. This includes obtaining specific information on the hiring and oversight of privileged administrators and establishing robust controls over their access.
- **Authentication and Authorization:** HUDCO's Password Policy should be adhered to for all authentication requirements. Role-based authentication should be implemented when necessary, and separate identities must be maintained in a multi-tenant environment.
- **Data Residency:** The cloud service provider must ensure that HUDCO's data resides exclusively in data centre's within India. All processing should be performed in India, and no data, including backups, should be transmitted outside India's legal jurisdiction.
- **Data Segregation:** HUDCO should define robust controls for data segregation in multi-tenant cloud environments.

- **Data Security:** Policies and procedures must be established and maintained to ensure the confidentiality, integrity, and availability of HUDCO's data across all system interfaces and business functions. Strong encryption mechanisms should be employed for data at rest and in transit to prevent unauthorized disclosure, alteration, or destruction.
- HUDCO should establish clear controls for logging, monitoring, and auditing data.
- Risk-based Vulnerability Assessments and Penetration Testing should be conducted regularly to identify and remediate potential threats.
- A collaborative governance structure and processes between HUDCO and the cloud provider should be defined during the design and development of service delivery. These processes should address service risk assessment and management protocols and be included in service agreements.
- HUDCO should ensure effective Business Continuity and Disaster Recovery measures for cloud-based solutions.

37. Encryption Policy

The purpose of this Encryption Policy is to establish guidelines and best practices for the encryption of sensitive data at HUDCO, ensuring the confidentiality, integrity, and availability of data in transit and data at rest. This policy outlines the requirements for encrypting data during transmission over networks and when stored in various storage components, including cloud storage volumes, databases, and file storage. As well as transmission via API's. The policy aims to protect HUDCO's and its clients' data from unauthorized access, interception, and tampering, thereby mitigating the risk of data breaches and maintaining a high level of data security.

- Confidentiality, integrity, authenticity and non-repudiation of secret/confidential information shall be maintained through appropriate encryption techniques when information is stored in information systems, media/devices or accessed /transmitted over networks.
- HUDCO shall put the appropriate encryption system for: -
    - Data in Transit: Data that is being transmitted over a network between two communicating parties, such as data sent and received via APIs, web applications, and other communication channels.
    - Data at Rest: Data that is stored on storage systems, databases, or other storage media, whether on-premises or in the cloud.
- The technical standards and contractual requirements for the storage and transmission of encrypted data should be defined.
- Cryptographic Controls should be used for ensuring the confidentiality and integrity of confidential and secret information stored on devices and storage media.
- Cryptographic controls should be used in compliance with all relevant legislations and regulations.
- Secure processes should be employed for key generation, distribution, revocation, and storage wherever electronic certificates are used.

- Management of critical servers or security devices should be done over secure channels using encryption techniques.
- Access to secure storage of media should be controlled by authentication (passwords, biometrics, keypad) etc. Minimize distribution of sensitive information, including printouts that contain sensitive information.
- Removable media encryption software should be used to encrypt and password-protect the data in portable devices.
- Data transmitted over all networks should be encrypted using the approved cryptographic algorithms based on information classification.
- HUDCO should use electronic signatures or message authentication codes to verify the authenticity, non-repudiation, and integrity of stored or transmitted sensitive or critical information.
- A list of encryption standards and hashing techniques should be created, approved, and maintained.
- All passwords shall be encrypted using non-reversible hashing techniques in password files.
- Protect passwords in storage for verification purposes using a strong cryptographic hash function that utilizes a random salt.
- Physical and environmental controls should be implemented to protect cryptographic systems and assets.
- It shall be ensured by owners of mobile devices that no official data is stored in the privately used mobile device. Regular backups shall be taken for devices carrying important, sensitive or critical business information. It shall be ensured that employees using mobile devices are trained and made aware of the risks and also the controls that have to be implemented.

Encryption Key Management

- An approved Key Management procedure shall be established which should outline guidelines for Key Generation, Key Distribution, Key Installation, and Key Lifecycle Management.
- Key management is a critical aspect of encryption and data security, focusing on the secure generation, distribution, storage, rotation, and disposal of encryption keys. Encryption keys are essential for both data in transit and data at rest encryption. They play a central role in converting plaintext data into ciphertext during encryption and vice versa during decryption. Effective key management is crucial to ensure the confidentiality, integrity, and availability of encrypted data and to protect against unauthorized access to sensitive information.
    a. Key Generation: Key generation involves creating cryptographic keys using random number generators or cryptographic algorithms. The strength of encryption relies on the randomness and complexity of the generated keys.
    b. Key Distribution: Securely distributing encryption keys to authorized users or systems is a crucial step in key management. This process ensures that only intended recipients can access and use the encrypted data.
    c. Key Storage: Safeguarding encryption keys is paramount to prevent unauthorized access to the keys and, consequently, the encrypted data. Key

storage should follow industry best practices, such as hardware security modules (HSMs) or secure key management systems.

d. Key Rotation: Regularly changing encryption keys is known as key rotation. This practice reduces the window of opportunity for attackers to exploit stolen or compromised keys and enhances overall data security.
e. Key Revocation: In cases of suspected key compromise or unauthorized access, key revocation allows administrators to invalidate and replace compromised keys.
f. Key Escrow: Key escrow involves securely storing encryption keys with a trusted third party to facilitate data recovery in exceptional situations, such as when authorized users lose access to their keys.

Acceptable Encryption Algorithms

HUDCO will use Encryption Algorithm as per CERT-in/ RBI guidelines as applicable for Application used, for ex AES (Advance Encryption Standard), Triple DES

Roles and Responsibilities of stakeholders, Enforcement of Policy: - Application owner/ system integrator will be responsible for enforcement of policy.

Data Leak Prevention Strategy

To ensure the protection of HUDCO's data against leakage.

- The HUDCO shall develop data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.
- The Data loss/leakage program shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.
- Data security and protection should be ensured at the vendor managed facilities as well.
- Restrict Access of external devices to avoid unauthorized transfer of official data.

Preventing Execution of unauthorized Software

To ensure installation and usage of only approved software's in the HUDCO. The HUDCO will define controls to protect its operations systems / information processing facilities against malicious software and virus attacks to ensure availability of IT services without interruptions. All application/ software deployment (on all systems within HUDCO environment) shall be managed using a centralized solution. Financial Institution shall deploy tools to monitor latest released security patches by vendors of the HUDCO.

Secure Configurations

HUDCO's systems shall be configured for security, reliability and stability and all such configurations should be documented. Systems should follow standard naming conventions for efficient identification in configuring and in problem solution

- HUDCO should maintain the Guideline and Documents to apply baseline security requirements/configurations to all Categories of devices (endpoints /workstations, mobile devices, operating systems, Databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and reviewing periodically.
- All critical device (such as firewall, network switches, security Devices, etc.) configurations and patch levels should be periodically evaluated for all systems in the bank's network Including in Data Centers, in third party hosted sites.
- Secure Configuration Documents should be tested in the test environment prior and approved before releasing it in production.
- Secure configuration documents should be created based on the OEM's and industry practices, at a minimum for the following:
    a. Endpoints
    b. Operating systems
    c. Web servers
    d. Application servers
    e. Database servers
    f. Security devices
    g. Network devices
- Secure configuration documents should be reviewed on change of version, based on learnings from security incidents or once in a year.

38. Data Classification

Below is the detailed classification of the definitions listed above based on data sensitivity for both HUDCO and its clients:

38.1 Public Data (HUDCO and Clients):

Definition: Data that is meant for public consumption and does not contain sensitive or confidential information.

Classification: Non-Sensitive

Access Controls: No access restrictions; publicly accessible.

Examples (HUDCO): Publicly available marketing materials, press releases, general website content.

Examples (Clients): Publicly available product information, general announcements.

38.2 Internal Data (HUDCO and Clients):

Definition: Data that is intended for internal use within the organization and may include non-public operational information.

Classification: Internal Use Only

Access Controls: Limited access to authorized personnel within the organization.

Examples (HUDCO): Internal communications, non-sensitive internal reports, project status updates.

Examples (Clients): Internal documents shared with specific departments or teams.

38.3 Confidential Data (HUDCO and Clients):

Definition: Data that is sensitive and requires protection from unauthorized access or disclosure.

Classification: Confidential

Access Controls: Access restricted to individuals with a need-to-know basis and proper authorization.

Examples (HUDCO): Employee records, financial data, business plans, client contracts (if shared with HUDCO).

Examples (Clients): Customer personal information, financial records, proprietary information shared with HUDCO

38.4 Executive Data (HUDCO and Clients):

Definition: The most sensitive data that requires the highest level of protection due to its critical nature.

Classification: Executive

Access Controls: Restricted access with strict authorization and additional security measures (e.g., multi-factor authentication).

Examples (HUDCO): Intellectual property, trade secrets, financial reports, client contracts (if shared with HUDCO).

Examples (Clients): Proprietary algorithms, strategic plans.

39. Dark Web Monitoring

Dark Web Monitoring framework is critical to safeguarding sensitive organizational data and assets from potential cyber threats. Dark Web, being a hub for illicit activities, poses significant risks, including the sale of confidential information, credentials, and other exploitable data.

HUDCO's Dark Web Monitoring focuses on proactive measures to identify, analyze, and mitigate threats originating from this hidden online realm.

HUDCO will employ advanced tools and specialized service providers to continuously scan Dark Web forums, marketplaces, and other illicit platforms for any mentions of HUDCO’s sensitive data, employee information, or critical business operations. The policy outlines clear

protocols for identifying breached data, assessing risks, and initiating rapid incident response procedures. By integrating Dark Web Monitoring into the IS Policy, HUDCO demonstrates its commitment to staying ahead of emerging cyber threats, ensuring the resilience and security of its digital environment.

40. Social Media Policy

Guidelines for Social Media Activities in HUDCO

Introduction:

In modern age of online communications, '**Social media'** has become an integral part of our life. It is an ideal platform for sharing information, ideas, beliefs etc. In order to enable HUDCO to make use of this dynamic medium of interaction, a framework and guidelines for use of the social media has been formulated. These guidelines will enable HUDCO to create and implement its own strategy for the use of social media.

The guidelines/framework comprises of the following elements:

1. **Objective:** Why HUDCO needs to use social media
2. **Platform:** Tools available under social media
3. **Governance:** What are rules of engagement
4. **Communication Strategy:** How to interact with all the stakeholders
5. **Engagement:** How to create and sustain a community
6. **Institutionalization:** How to embed social media in organization structure

1. Objective:

HUDCO's Social Media Platforms/Handles will primarily aim to:

- Increase awareness about the company through online social sites/ channels and also explore further options in this field.
- Create wider audience base by addition of more members, generation of 'likes', retweeting important tweets / Facebook shares by official handles of HUDCO (as per guidelines received from Ministry) or by members.
- Showcase latest information in forms of videos / photographs / AVs etc.
- Provide platform for management to send messages for expressing greetings / opinions / reactions etc. when required and deemed fit to various stakeholders and the public at large.

2. Platforms:

The following social medial platforms are currently being used by HUDCO:

Name	Type	Remarks
Facebook	Social networking website	Official account https://www.facebook.com/HUDCO
X.com (Formerly Twitter)	Online news and social networking service where users post and interact with messages, known as "tweets".	Official account https://twitter.com/hudcolimited
YouTube	YouTube is a video sharing website that makes it easy to watch online videos. Videos can be created and uploaded on it and shared with others.	Official account https://www.youtube.com/hudcoltd
LinkedIn	LinkedIn is a business and employment-focused social media platform that works through websites and mobile apps. The platform is primarily used for professional networking and career development which allows jobseekers to post their CVs and employers to post jobs.	Official account https://www.linkedin.com/company/hudco-limited
Instagram	Instagram is a mobile, desktop and Internet based photo sharing application and service that allows users to share pictures and videos either publicly or privately to pre-approved followers.	Official account May be created

3. Governance:

3.1 Resource Governance:

A dedicated Social Media team including outsourced resources may be constructed to manage the engagement and keep abreast of the fast-paced development in media.

a) Roles and Responsibilities:

i) Official Social Media handles to be created, maintained only by PR Unit.
ii) PR Unit shall compile, edit & draft all content.
iii) Uploading / Response / Monitoring on Social Media Sites by PR Unit.
iv) There shall be one official account of HUDCO on each online social media platform which will be centrally managed by PR Unit.

v) EMPLOYEES will be encouraged to associate themselves with all official social media handles AND further be reminded to share / retweet / like posts and information to increase reach.

vii) EMPLOYEES shall abide by the guidelines regarding online media usage / online behavior as attached **Annexure-I**. The guidelines shall be modified as and when required.

b) Accountability:

The officials designated for engagement with citizen using the social media shall be covered under provisions in consonance with the RTI Act and the IT Amendment Act, 2008.

3.2 Account Governance:

i) Account Creation: A social media account establishes an organization's online identity. Wherever possible, the same name for the different social networking accounts may be adopted to ensure ease of search on the internet. The account name should not be more than 15 characters (e.g. Twitter).

ii) Login and passwords: Each new account requires a URL, user-name and/or email address and a password. A proper record of login ids and password must be maintained. This is critical as multiple people may be authorized to post on behalf of the department.

iii) Account Status: It is important to define whether the engagement may be undertaken through official accounts only or the officials may be permitted to use personal accounts also for posting official responses. It determines who says what on behalf of HUDCO and in what form it is published. It also outlines how each piece of published information is presented where it is published. The most important aspect is whether the responses are in Official or Personal Capacity.

3.3 Response Governance:

The major attraction of social media is the spontaneity and immediacy of response and feedback and those visiting the site would expect some kind of response within a pre-defined time limit.

i) All responses should be kept short and to the point.

ii) Accurate, complete, polite and prompt feedback mechanism to users via social media platforms.

iii) Employees are prohibited to respond in their personal capacity.

iv) Monitoring to be done using proper tracking mechanism to track conversations relating to HUDCO.

v) Moderating the sites to avoid spam, advertisements and inappropriate content. Tracking social media networks for relevant and related key words and respond to them to initiate positive conversations on social media sites.

3.4 Content Governance:

i) **Generating content:** creating stories / photo opportunities for audience interest. Content will have to be short & specified to the site on which it is being published.

ii) **Accessibility:** For wider participation, content availability should be in Indian languages and must not be limited to text alone. The content should follow the Government of India Guidelines for Website and adequately address challenges related to accessibility in Indian Languages as well as accessibility of content for differently abled.

iii) **Moderation:** The moderation should include matter related to copyright, rights to addition and deletion etc.

iv) **Records Management:** When any information is shared or guidance given online, it is necessary to ensure that all relevant digital records are captured, trail is generated, and records are managed appropriately. It is important that the rules regarding digital record keeping are stated upfront so that those seeking historical data are aware of statutes and limitations. Since most of the social media platforms are based outside India and are not governed by Indian Laws or managed and controlled by Indian regulations, there is a need to address information security and archiving. If required, HUDCO may (internally / through external social media services provider) work out Service Level Agreements for Complaint & Response Mechanism for:

- Content Storage
- Shared access of the content
- Archival mechanisms

v) **Data & Information Security Governance:**

HUDCO's communication to citizens via social media should follow the same data retention policy as its communication through other electronic and nonelectronic channels. Data portability compliance varies from one social media platform to another.

Provisions related to Personal Information & Security: Under the Information Technology Act 2000, the Central Government has enacted various rules and regulations which impact social media. Some of the most important in this regard are as follows:

a) The Information Technology (Reasonable Security Practices and Procedures & Sensitive Personal Data or Information) Rules 2011 defines provisions for personal information & security and what constitutes sensitive personal data. Sensitive personal data or information of a person means such personal information on which consists of information on relating to:

password; financial information such as Bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information.

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

b) For the purposes of protecting such sensitive personal data, the Government has mandated that any legal entity who is processing, dealing or handling sensitive personal data must implement reasonable security practices and procedures.

c) Further under the Information Technology (Intermediary guidelines) Rules 2011, since the said Government department who is providing social media facilities is an intermediary, it has to comply with the Information Technology (Intermediary guidelines) Rules 2011. Under Rule 3(4) of the said rules, the Government department shall act within thirty-six hours on receiving the written complaint form an affected person and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2).

d) Further the Government department shall preserve such information and associated records for at least ninety days for investigation purposes.

vi) Rules for Privacy and data collection:

It is important to ensure the protection of people from exposure to inappropriate or offensive material.

a) Since profiles on social network are linked more often to individuals and not organizations, for the organization's site / page, a separate work profile may be created which can then be linked to a general email address that is accessible to anyone in the team, enabling them to administer the social networks without compromising on individual privacy.

b) It is critical that social media policy for the organization is compliant with existing law governing data protection and privacy. Each department of the HUDCO may be recommended to practice additional protections to safeguard privacy of citizens while maintaining highest levels of transparency.

4. Communication Strategy:

i. Social media can only be used by HUDCO to communicate existing information and propagate official policy/information to the public.
ii. Social media handles to be made informative / interesting containing of more stories apart from regular news/event updates.

5. Engagement Analysis:

i. Regularly monitor and evaluate social media presence.
ii. Track conversations, links and blogs for Positive, Neutral or Negative sentiments. If, negative sentiments found, draft a plan to work out and neutralize.
iii. Respond to the queries after collection of information from the concerned.

6. Institutionalize social media:

i. rules may be established that all policy announcements will be undertaken simultaneously on traditional as well as social media.
ii. all-important occasions, documents as far as possible may be broadcasted using social media.
iii. all updates from the website should preferably be updated on social media sites.

7. Conclusion:

The Framework and Guidelines in this document have been formulated with a view to helping HUDCO to make use of social media platforms to engage more meaningfully with its various stakeholders.

Standard guidelines for Employees of HUDCO

1) Employees should be aware that Social Media platforms as Facebook / Twitter / Instagram are freely available and easily accessible platforms for the general public. Employees must therefore act responsibly and should not post / publish / comment / release any information that is considered confidential / sensitive / harmful for overall image of HUDCO.
2) Employees should use their best judgment in posting material that is neither inappropriate nor harmful to HUDCO.
3) Examples of inappropriate social media behavior include posting comments that are negative, defamatory, proprietary, harassing, and libelous or that can create a hostile work environment.

4) Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized spokespersons.
5) If employees encounter a situation / interaction while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner.
6) Employees should get appropriate permission before referring to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
7) Employees should be aware that Social Media platforms as Facebook / Twitter / Instagram are freely available and easily accessible platforms for the general public. Employees must therefore act responsibly and should not post / publish / comment / release any information that is considered confidential / sensitive / harmful for overall image of HUDCO.
8) Employees should use their best judgment in posting material that is neither inappropriate nor harmful to HUDCO.
9) Examples of inappropriate social media behavior include posting comments that are negative, defamatory, proprietary, harassing, and libelous or that can create a hostile work environment.
10) Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized spokespersons.
11) If employees encounter a situation / interaction while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner.
12) Employees should get appropriate permission before referring to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property. Social media use should not interfere with employee's responsibilities at HUDCO.

41. Defending against premeditated internal attacks

A member of staff may target confidential information or deface the organization web site, which could result in both financial loss and embarrassment so the policy for controlling such activity should include following measures.

- The access to information should be as per roles and requirements.
- The recruitment and hiring practices of the HUDCO should include following:

  Background checks.

  Confidentiality/ non-disclosure agreement.

Employee bounding to protect against losses due to theft etc.

42. Compliance

It is required that HUDCO define, document and maintains all the relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements for each of the information systems.

42.1 Compliance with legal and contractual requirement

It is required that Legal and Compliance function identifies the relevant legislation, regulations and compliance requirements for business operations.

Functional Heads are required to ensure that their function meet the requirement of the information and Cyber Security Policy and relevant controls.

42.2 Identification of applicable legislation and contractual requirements

- A list of all relevant statutory, regulatory and contractual requirements along with the individual responsibilities must be defined.
- Periodic reviews are to be carried out to ensure that the list of identified statutory, regulatory and contractual requirements along with individual responsibilities, remain up to date.

42.3 Intellectual property rights

- Software acquisition is to be carried out through known and reputable sources to ensure that the copyright is not violated.
- The HUDCO's management is required to provide its endorsement to the information identified as intellectual property. Intellectual Property Rights (IPR) is to be included in all the contracts, and is implemented to ensure, but not limited to:
- Compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be IPR.
- IPR including software or document copyright, design rights, trademarks, patents, and source code licenses are not infringed.
- Only licensed software is to be installed within HUDCO's network environment. Record of all software licenses is to be kept and updated regularly.
- On best effort basis, it shall be ensured that Intellectual Property rights for all applications or changes to applications provided by the third-party service provider should remain with HUDCO.

42.4 Protection of records

- Important records of an organization shall be protected from loss, destruction, unauthorized access, unlawful and unauthorized duplication, tampering and falsification, and in some cases retention of certain records for certain periods of

time is required by law. However, it is not possible or desirable to keep everything forever.

- It is required that the data protection and privacy is being ensured as required in the relevant legislation, regulations, and, if applicable, contractual clauses.
- PII or information that can be used on its own or with other information to identify, contact or locate a single person, mentioned in any document or over mail is to be treated as confidential.
- Data Loss Prevention solution shall be implemented in order to protect information from going out of the organization's boundaries undetected, wherever possible.
- Relevant legislation, regulation and contractual clauses for collecting, using and storing PII is to be identified.
- It is required that the purpose for which PII was collected is to be identified by the owner. Owner is required to conduct a self-review against the purpose and report any deviations for which appropriate action is to be taken based on a Root Cause Analysis (RCA).
- It is required that access to PII is available only to authorized personnel only. It shall be ensured that this authorization is provided by the business function.
- PII shall be stored on network drives and/or in application databases with strong access controls measures (for e.g. User IDs/password) and are made available only to those individuals with a valid and approved business need.
- All incidents involving data breaches which could result in identity theft shall be coordinated by information security committee for investigation and closure.
- If PII needs to be transmitted over the Internet, It shall be ensured that it is sent using encryption methods.

42.5 Privacy and protection of personally identifiable information

The data protection and privacy of (such as customer details, restricted data etc.) against unauthorized access, transmission, publication, damage, use, modification, disclosure and impairment is to be ensured at HUDCO by implementing adequate technical and administrative control.

42.6 Regulation of cryptographic controls

- It is required that cryptographic controls are to be used in compliance with all relevant agreements, laws, and regulations.
- The access to encryption key data shall be restricted to authorized administrators only. It shall be ensured that the activities of the administrators having access to such sensitive data are appropriately logged and monitored periodically.

Annexure I – Glossary

Term	Description
AMC	Annual Maintenance Contract
BCM	Business Continuity Management
BCP	Business Continuity Plan
CCTV	Closed Circuity Television
CD	Compact Disk
CISO	Chief Information Security Officer
COTS	Commercial Off-The-Shelf
CTO	Chief Technology Officer
DC	Data Center
DMZ	Demilitarized Zone
DRP	Disaster Recovery Plan
DVD	Digital Video Disk
ERT	Emergency Response Team
HR	Human Resource
ID	Identifier
IP	Internet Protocol
IPR	Intellectual Property Right
IS	Information Security
ISM	Information Security Manager
ISP	Information and Cyber Security Policy
IT	Information Technology
LAN	Local Area Network
PII	Personally Identifiable Information means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. E.g. Name, Address, Phone Number
HUDCO	Housing and Urban Development Corporation Ltd

Term	Description
RPO	Recovery Point Objective
RCA	Root Cause Analysis
RTO	Recovery Time Objective
SFTP	Secure File Transfer Protocol
SPI	Sensitive Personal Information means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSL	Secure Socket Layer
TPA	Third Party Assessment
UPS	Uninterrupted Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

Annexure II – References

Sr. No.	Circular Reference Number	Description
1.	ISO 27001:2013 Framework	It the requirements for establishing, implementing, maintaining and continually improving an information security management system.
2.	IT Act 2000	An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication.
3.	IT Amendment Act 2008	It is the substantial amendment to IT Act 2000.
4.	COBIT (DS5.2, DS5,3) and (DS5.2, ME2.5, ME2.7) for Information Security Policies	COBIT (as mentioned subparts) provides information regarding the policies for Information Security and review of the policies for Information Security.
5.	NIST SP 800-100 Information Security	A manual for the Information Security intricacies and techniques
6.	RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices-RBI/2023-24/107DoS.CO.CSITEG/SEC.7/31.01.015/2023-24	Dated 07th November, 2023