Havells India Limited

Information Security Policy

Version 1.3

Document Scope

This document shall be applicable to all employees /Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Chief Information Security Officer (CISO) shall distribute this policy to all employees working handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. General

1.1. Management intent

The Information Security policy document defines Havells' position on information security. Havells' management has documented this policy to set a clear corporate direction and demonstrate support for, and commitment to information security. This objective of this policy is to describe the security requirements for Havells' information and information assets.

Havells' management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the Information Security Management System (ISMS) by:

a) Establishing an Information Security (IS) policy;
b) Establishing roles and responsibilities for information security;
c) Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
d) Ensuring that measurable ISMS objectives are established;
e) Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
f) Deciding the criteria for accepting risk and acceptable levels of risk;
g) Ensuring that ISMS audits are conducted; and
h) Conducting management reviews of the ISMS.

1.2. Policy Objective

The Havells Information Security Policy (HISP) provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage the information security in Havells. Havells shall secure information by:

a) Establishing and organizing an information security governance framework and ensuring that it is aligned with business objectives and regulatory mandates;
b) Developing and maintaining an effective Information Security Management System (hereinafter referred to as 'ISMS') consisting of an information security policy document, supporting policies and a risk management framework (to identify, measure, prioritize and treat risks);
c) Creating and maintaining a security-conscious culture in Havells and the third parties supporting Havells' operations; and
d) Taking appropriate actions for any violations of the HISP.
e) Continous improvement of the information security management system

2. Abbreviations

Abbreviation	Meaning
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
CIO	Chief Information Officer
BCFO	Business Chief Financial Officer
CIA	Confidentiality, Integrity and Availability
CISO	Chief Information Security Officer
DR Plans	Disaster Recovery Plans
HR	Human Resources
IPR	Intellectual Property Right
ISC	Information Security Council
ISMS	Information Security Management System
IST	Information Security Team
IT	Information Technology
MR	Management representative
NDA	Non-disclosure Agreement
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
RA	Risk Assessment

3. Definitions

Keyword	Definition
Authentication	A process to positively verify the identity of a user, device, or other entity in a computer system, often as a perquisite to allow access to resources in system.
Authorization	A process to provide a permission to access a specific resource or function.
Confidentiality Agreements	A legal agreement between two or more parties that is used to signify that a confidential relationship exists between the parties.
Control	A means of risk response, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.
Information Asset	A definable piece of information stored and/or processed in any manner, which is recognized as valuable to the business, including the systems processing the information. These information assets are classified into information assets, paper assets, people assets, physical assets, services assets, and software assets.
Asset Register (AR)	This is the register / inventory of all assets required for the functioning of all processes under each department. Each department is to maintain this register with them as a part of the ISMS mandatory activities. This will be reviewed annually.
Information Security	A process of safe-guarding information assets from unauthorized access, modification, use, disruption, and destruction to ensure confidentiality, integrity, availability, and non-repudiation of information.
Information Security Event	An event that is caused due to any action on an Information Asset. For example, deleting a key file from a critical business system.
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Intrusion	An uninvited and unwelcome entry into a system by an unauthorized source.
Key Management	In cryptography, it is the creation, distribution, and maintenance of a secret key. It determines how secret keys are generated and made available to both parties; for example, public key systems are widely used for such an exchange. If session keys are used, key management is responsible for generating them and determining when they should be renewed.
Logical Access	Connection of one device or system to another using software.
Media	The physical material which stores computer information.
Mobile computing	Generic term describing ability to use technology, that is not physically connected, or in remote or mobile (non-static) environment.

Keyword	Definition
Network	A configuration of communication equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to each other.
Non-Disclosure Agreements (NDA)	A legally binding document which protects the confidentiality of ideas, designs, plans, concepts, or other commercial material.
Password	A protected, generally computer encrypted, string of characters that authenticates a user to the system.
Policy	An overall declaration of management intent for information security. It states what needs to be done to foster information security goals and objectives of Havells. It contains managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected.
Remote Access	Ability to get access to a computer or a network from a remote distance.
Security breach	Violation of any security policy or procedures.
Software	Generic term used for Operating systems, firmware, databases, web servers, applications, services / daemons, drivers etc.
Source Code	The actual program, as written by the programmer, which is compiled into machine code which the computer can understand.
Special Interest Group	A Special Interest Group (SIG) is a community with an interest in advancing a specific area of knowledge, learning or technology where members cooperate to affect or to produce solutions within their particular field, and may communicate, meet, and organize conferences.
Strategic Partners	Strategic Partners are third parties providing key business-enabling services to Havells.
Teleworking	Involves the use of telephones and computers to enable an employee to work at a location other than their regular workplace.
Third Parties	Third party refers to any entity (distributors, sales agents, equipment support partners, suppliers, vendors, etc.) with whom Havells engages in a business relationship to deliver product and services to its customers.
Threat	An intention or a determination to inflict harm (or something unpleasant) on an Information Asset.
User	User shall mean an individual accessing information assets and information processing facilities of Havells. It shall include Havells and third parties' employees including strategic partners.
Virus	Form of a malicious code which is potentially disruptive.
Vulnerability	A weakness of an asset or a group of assets that can be exploited by a threat.

4. Policy structure

The structure of policy resembles the structure of the ISO 27001:2022 standard for Information Security Management Systems (ISMS).

a) Section 1 through 3 of this policy define the management intent, abbreviations, and definitions of terms

& framework;

b) Section 4 defines the structure of the policy;
c) Section 5 through Section 18 of this policy covers domains and controls as mentioned in ISO 27001:2022 standard; and
d) Annexure in this policy have been defined to ensure compliance with the clauses of the ISO 27001:2022 standard.

5. Information Security Policy

Control Objective

Havells Information Security Policy provides management direction and support to ensure protection of Havells' information assets, and to allow access, use and disclosure of such information in accordance with appropriate standards, laws, and regulations.

5.1. Policy Control

5.1.1. Policy Statement

The information assets of Havells shall be protected from information security threats, whether internal or external, deliberate, or accidental, such that the confidentiality of information is maintained, integrity of information can be relied upon, availability of information is ensured and all legal, regulatory, statutory, and contractual obligations are met.

5.1.2. Policy Scope

The scope of the policy covers all business functions, where the changes made to the IT infrastructure and IT applications.

5.1.3. Policy Enforcement

It is the responsibility of the IT team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Havells Information Security Policy.

All employees and/or third party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy.

5.2. Review of Information Security Policy

Havells Information Security Policy shall be reviewed at least annually and at a time of any major change(s) in the existing environment affecting the policies and procedures. Havells Information Security Policy shall be reviewed in consultation with relevant stakeholders and approved by the CIO and CISO after consulting with Management/Board/ITPC. The reviews shall be carried out for assessing the following, but not limited to:

a) Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture, regulatory and / or legal requirements, emerging threat landscape; and

b) Effectiveness of the policies.

5.3. Consequence for Non-Compliance

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.

b) Employees and third parties who breach this policy shall be subject to disciplinary action.

Refer: Zero Tolerance Policy

5.4. Exceptions

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy.*

Refer: Security Exception Management Policy.

6. Information Security Organization

Control Objective

Havells Information Security policy defines appropriate authority and responsibilities to manage information security in Havells. The information security organization has been designed to ensure structured co-ordination of information security related activities.

Responsibility

It is the responsibility of the Information Security Council (ISC) and Chief Information Security Officer (CISO) to manage the information security organization within Havells. CIO and CISO shall be responsible for creating and maintaining any guidelines/procedures required for adhering to information security policy.

Policy Controls

6.1. Internal Organization

6.1.1. Management responsibilities

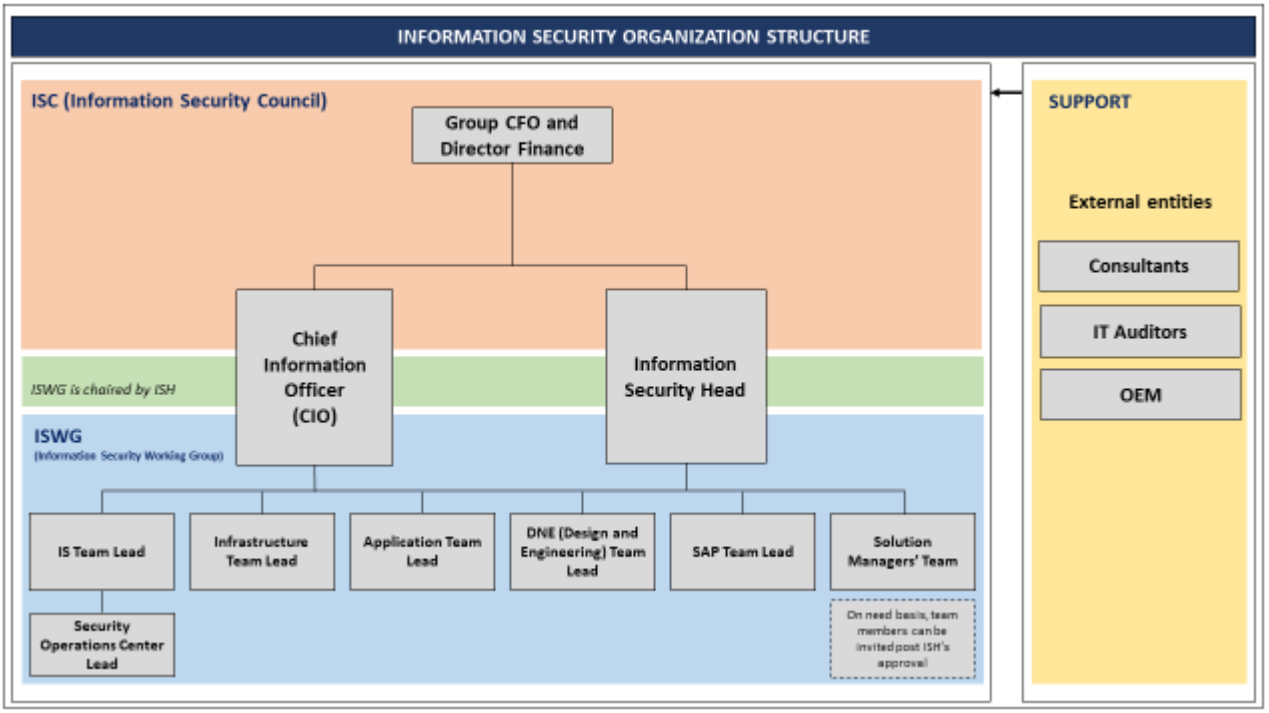
The management shall commit to implement, manage, monitor, and improve on an ongoing basis an organization wide information security framework. The management shall provide the direction and necessary support for the implementation and maintenance of the information security framework within Havells.

6.1.2. Information security co-ordination

The information security organization is responsible for the information security within Havells and supporting and maintaining information security activities.

6.1.3. Information Security roles and responsibilities

The governance framework for information security management system is defined below and includes the key roles and responsibilities during development and implementation of ISMS.



Refer: ISMS Manual

6.1.4. Authorization process for information processing facilities

Employees owned like laptops are not allowed to connect into corporate network. In specific cases, based on IT usage, employee is allowed to access corporate network and applications through Virtual Desktop Infrastructure (VDI) service after necessary approvals from user's manager and DC / IS lead.

Refer: Acceptable Usage Policy

6.1.5. Confidentiality Agreements

Requirements for confidentiality or non-disclosure agreements, reflecting Havells' needs for the protection of information shall be identified and maintained.

Refer: Code of Conduct, IT policy and respective agreements signed or as applicable on the employees at the time of joining

6.1.6. Contact with Authorities

Havells shall maintain contact with authorities including but not limited to law enforcement authorities, regulators, fire department, and emergency services. The contact details of these agencies shall be maintained and displayed at prominent places.

Refer: Physical Security Management Policy

6.1.7. Contact with Special Interest Group

CIO and CISO shall maintain appropriate contact with special interest groups and authorized information security forums for receiving and distributing updates on new vulnerabilities, security threats, regulations and/or risks pertaining to industry vertical of Havells.

6.1.8. Independent review of information security

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

6.1.9. Information security in project management

Project Managers shall ensure that information security aspects shall be integrated into the project management.

The project management team shall ensure that information security risks are assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle. Further, information security risks associated with the execution of projects, such as security of internal and external communication aspects are considered and treated throughout the project life cycle;
Refer : Project management Policy

6.2. Supplier / External Parties

6.2.1. Identification of risks related to supplier / external parties

The risks to Havells' information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

6.2.2. Addressing information security in supplier/third party agreements

Agreements with third parties involving accessing, processing, communicating, or managing Havells' information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements. Agreements/contracts shall be defined to ensure the inclusion of following, but not limited to:

a) Havells shall draw and sign formal written contracts / digital contracts / confirmation via email with all the third-party service providers. These contracts shall include the Service Level Agreement (SLA) identified, defined and agreed on for the respective service wherever applicable;
b) The third parties (wherever applicable) shall adhere to the Havells' Information Security Policy;
c) All the third parties to be on boarded or contract renewal of existing third parties from the date of implementation of policies shall comply with Havells' Information Security policy.

Refer: Third Party Security Policy

6.2.3. Monitoring, review and change management of supplier services

Monitoring, review and change management of supplier services should ensure the information security terms and conditions of the agreements are complied with, information security incidents and problems are managed properly and changes in supplier services or business status do not affect service delivery.

To maintain an agreed level of information security and service delivery in line with supplier agreements, the Havells shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

6.2.4. Managing information Security in Information and communication technology (ICT) supply chain.

To maintain an agreed level of information security in supplier relationships, Havells shall define and implement the processes and procedures to manage the information security risks associated with the ICT products and services supply chain.

Havells shall consider below aspect to address information security within ICT supply chain in addition to the general information security requirements for supplier relationships

i. defining information security requirements to apply to ICT product or service acquisition;
ii. requesting that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation;
iii. implementing a monitoring process and acceptable methods for validating that delivered ICT products and services comply with stated security requirements;
iv. defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers

Refer: Third Party Security Policy

6.2.5.Information security for use of cloud services

The Havells shall define Processes for acquisition, governance, use, management and discontinuation/migration of any cloud service or cloud service provider in accordance with the organization's business requirement wrt to information security management.

The Havells shall consider below aspects:

a. all relevant information security requirements associated with the use of the cloud services;
b. cloud service selection criteria
c. scope of cloud service usage;
d. roles and responsibilities related to the use and management of cloud services;
e. which information security controls are managed by the cloud service provider and which are managed by the organization as the cloud service customer;

f. how to obtain and utilize information security capabilities provided by the cloud service provider;
g. how to obtain assurance on information security controls implemented by cloud service providers;
h. how to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers;
i. procedures for handling information security incidents that occur in relation to the use of cloud services;
j. its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks;
k. how to change or stop the use of cloud services including exit strategies for cloud services.

b.

Refer ; Havells Cloud policy

7. Asset Management

The clauses in asset management establish the requirement of controls that need to be implemented for protecting assets of Havells. Assets of Havells shall be identified and shall receive comprehensive protection.

Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Asset Management Policy.

Refer: Asset Management Policy

7.1. Responsibility for assets

Commercial Head at each location (in conjunction with Administration function) shall be responsible for maintaining the IT asset register

Commercial Head at each location in conjunction with Functional and Administration function shall ensure that the assets are secured against physical and environmental threats.

HO Assets controller shall also ensure that the IT asset inventory is updated on as and when basis / periodically for all Havells locations.

7.2. Inventory of information and other associated assets

Commercial Head or other designated person at particular location is accountable for maintaining the IT asset inventory (workstations, printers, scanners, UPS) being used or managed at their respective locations. The IT Asset Inventory shall include details about the asset such as asset date of purchase, asset ownership and cost of assets.

Refer: Asset Management Policy

7.3. Acceptable use of information and other associated assets

Rules for acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented by Havells .

The Havells has defined acceptable usage policy to address this requirement

Refer : Acceptable usage policy

7.4. Return of assets

To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement, personnel and other interested parties as appropriate shall return all the Havells assets in their possession upon change or termination of their employment, contract, or agreement.

Refer: Asset Management Policy, HR policy and acceptable usage policy.

7.5. Classification of information

At Havells, Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.

Refer : Information classification, data masking and PII policy.

7.6. Labelling of information

At Havells, as per the information classification scheme adoption, labelling of information shall be implemented after notification of DPDP Act implementation guidelines/rule.

Refer : Information classification, data masking and PII policy.

7.7. Information Archival or Deletion

Information archival/discard/deletion will be inline with company's retention policy/applicable statutory provisions. Refer acceptable usage policy

a) Selecting the deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirement and relevant laws and regulation
b) Recording the results of deletion as evidence

Where third parties store the organization's information on its behalf, the organization should consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

Refer : Asset management policy and acceptable usage policy

7.8. Data Masking

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements, the Havells IT team shall implement data masking as per the access control policy and business requirements, taking applicable legislation into consideration.
Where the protection of sensitive data (e.g. PII) is a concern, the organization should consider hiding such data by using techniques such as data masking, pseudonymization or anonymization.

Refer: Document classification, data masking and PII policy.

7.9. Data Leakage Protection

To detect and prevent the unauthorized disclosure and extraction of information by individuals or Systems, the Havells IT team shall implement data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

The Havells IT team shall implement necessary DLP tools to address this requirement.

The Havells should consider following to reduce the risk of data leakage

a) monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);

b) Identifying the sensitive information (e.g. personal information, product design, pricing)

c) acting to prevent information from leaking (e.g. quarantine emails containing sensitive information).

Data leakage prevention tools should be used to:

d) identify and monitor sensitive information at risk of unauthorized disclosure (e.g. in unstructured data on a user's system);

e) detect the disclosure of sensitive information (e.g. when information is uploaded to untrusted third-party cloud services or sent via email);

f) block user actions or network transmissions that expose sensitive information (e.g. preventing the copying of database entries into a spreadsheet).

8. Human Resources Security

The human resources security section of this policy defines the information security requirements that need to be incorporated in the human resource processes and to communicate information security roles and responsibilities prior, during and post-employment.

Responsibility

It is the responsibility of the IT and HR team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the policy.

Refer: Human Resource Security Policy

8.1. Pre-employment

8.1.1. Screening

All employees of Havells shall be subjected to pre-employment screening, which shall include the background verifications as identity check (for e.g. passport or similar document), educational background check (original certificate/degree of claimed academic and professional qualification).

8.1.2. Terms and Conditions of Employment

The HR department shall ensure that the terms and conditions of employment include confidentiality, NDA, and information security clauses.

8.1.3. Confidentiality or Non-disclosure agreements

The HR department shall ensure that Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

8.2. During Employment

8.2.1. Roles and Responsibilities

All employees shall ensure to maintain confidentiality, integrity and availability of Havells' information, information assets and/or information processing facilities;

8.2.2. Information security awareness, education, and training

The IT department shall ensure that the information security awareness, education, and training is provided to all the employees of Havells.

8.2.3. Disciplinary Process

A formal and uniform disciplinary process shall be maintained by HR, for all employees violating the information security policy and procedures.

Refer: Zero Tolerance Policy, HR policy/SOP

8.3. Employee Separation or Change of Employment

Employee Separation or Change of Employment

The HR department shall ensure that separation/ change of employment responsibilities of the employees is clearly defined, assigned, and communicated to them. The HR department shall formalize and document a separation process including the return of all issued assets such as corporate documents, equipment, mobile computing devices, software, access cards, manual and/ or any other asset that is the property of Havells.

8.3.1. Return of assets and removal of access rights

The HR department shall ensure that at the time of separation/change of employment or transfer of employee, assets belonging to Havells shall be returned by the employee. HR department shall also communicate to IT department regarding the removal of access rights of employees.

Refer : HR security policy

9. Physical and Environmental Security

The physical and environmental security section of this policy defines appropriate security controls required to protect information assets and information processing facilities of Havells from physical and environmental threats.

Responsibility

The administration department shall be responsible for the implementation of controls defined for physical and environmental security section of this policy.

Refer: Physical Security Management Policy

Policy Controls

9.1. Physical Security Controls

Appropriate security controls shall be designed and implemented to prevent unauthorized physical access, damage, and modification to Havells' information processing facilities and to protect information assets of Havells.

9.1.1. Physical Security Perimeter

The administration department shall define physical security perimeter for head office and other locations such as manufacturing plant where information assets of Havells are located.

9.1.2. Physical entry

The administration department shall ensure that secure areas are protected by appropriate entry controls and access points.

9.1.3. Securing offices, rooms and facilities

The admin department shall design and implement physical security for offices, rooms and facilities. The physical entry shall be restricted by bio-metric access / physical access card systems to prevent unauthorized access.

9.1.4. Physical security monitoring

Administration department shall ensure that premises shall be continuously monitored for unauthorized physical access. Physical security guards shall be deployed at entry / exit gates, loading /unloading area and other areas to monitor the unauthorized access. The CCTV cameras are installed at all entry /exit gates, reception area, equipment area and office area. Further, physical movement is monitored through BMS room where all CCTV camera feeds are displayed and monitored.

9.1.5. Protecting against physical and environmental threats

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure is designed and implemented. The periodic emergency

evacuation drills are conducted by admin team to review the emergency preparation and to increase awareness of the employees.

9.1.6. Working in secure areas

Security measures for working in secure areas are designed and implemented. The secure areas are provisioned with fire sensors, smoke detectors, fire exit signs, manual and automatic fire suppressant, emergency lights, emergency exit doors and continuous monitoring by trained staff etc.

Refer: Physical Security Management Policy

9.2. Equipment Security

Adequate controls shall be designed and implemented for equipment security to prevent loss, damage, theft, or compromise of information systems processing Havells' information and to prevent interruption to Havells' activities.

9.2.1. Equipment siting and protection

IT and other respective team shall ensure that IT equipment is sited securely and protected against unauthorized access, environmental and physical threats.

9.2.2. Security of assets off-premises Control

Admin and IT team shall ensure that off-site asses are protected to prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.
The following guidelines should be considered for the protection of devices which store or process information outside the organization's premises:

a) not leaving equipment and storage media taken off premises unattended in public and unsecured places;
b) observing manufacturers' instructions for protecting equipment at all times (e.g. protection against exposure to strong electromagnetic fields, water, heat, humidity, dust);
c) when off-premises equipment is transferred among different individuals or interested parties, maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment. Information that does not need to be transferred with the asset should be securely deleted before the transfer.
d) protecting against viewing information on a device (e.g. mobile or laptop) on public transport, and the risks associated with shoulder surfing

refer : Acceptable usage policy 2.5

9.3. Utilities

9.3.1. Supporting utilities

The Havells should ensure that all the offices and facilities are protected from power failures and other disruptions caused by failures in supporting utilities (electricity, UPS, Battery , DG, Air-conditioning etc.).

The Havells depend on utilities to support their information processing facilities. Therefore, the organization should:

a) ensure equipment supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications;
b) ensure utilities are appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
c) ensure equipment supporting the utilities is inspected and tested regularly to ensure their proper functioning;
d) if necessary, raise alarms to detect utilities malfunctions;
e) if necessary, ensure utilities have multiple feeds with diverse physical routing;
f) ensure equipment supporting the utilities is on a separate network from the information processing facilities if connected to a network;

9.3.2. Cabling security

Cables carrying power, data or supporting information services should be protected from interception, interference or damage to prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

At Havells, the following guidelines for cabling security should be considered:

a. power and telecommunications lines into information processing facilities being underground where possible, or subject to adequate alternative protection, if cables are underground, protecting them from accidental cuts (e.g. with armoured conduits or signals of presence);
b. segregating power cables from communications cables to prevent interference
c. use of fiber-optic cables
d. labelling cables at each end with sufficient source and destination details to enable the physical
a. identification and inspection of the cable.

10.Communications and Operations Management

Control Objective

The communications and operations management section of this policy defines the controls that shall be implemented to prevent unauthorized access, misuse or failure of the information systems and processing facilities. Confidentiality, integrity, and availability of information processed by or stored in the information systems shall be ensured.

Responsibility

IT team shall be responsible for implementation and maintenance of controls defined in the communications and operations management section of this policy.

Policy Controls

10.1. Operational Procedures and Responsibilities

10.1.1. Documented Operating Procedure

a) The operating procedures shall be documented, maintained, and made available to employees who require them; and
b) All operating procedures shall be centrally located and shall be easily accessible on a 'need to know' basis.

10.1.2. Change Management

a) All changes that could impact confidentiality, integrity or availability of information processed by or stored in the information systems and processing facilities, shall follow the documented change management process;
b) All relevant changes must be authorized and approved by change approval board (CAB); and
c) All approved changes on the critical systems shall be tested prior to implementing them on the production systems. In case of any exceptions, approval shall be taken from the respective department heads/solution managers.

Refer: Change Management Policy

10.1.3. Segregation of Duties

a) Duties and areas of responsibilities of employees shall be adequately segregated to reduce the opportunities for unauthorized or unintentional modification or misuse of the information assets;
b) Where segregation of duties is not possible, approval of the departmental head shall be obtained prior to allocating responsibilities to the employee. Also, appropriate compensatory controls such as monitoring of activities, audit trails, management supervision and independent reviews shall be implemented; and
c) Team lead within Havells are required to ensure that no employee in their team is responsible for multiple duties such that it could lead to the circumventing of existing security controls.

10.1.4. Separation of Development, Test and Production Environment

a) The production environment shall be logically and physically separated from the development and test environments;
b) Access to production, development and test environments shall be provided based on segregation of duties;
c) All test data, temporary accounts and temporary passwords shall be removed from the systems prior to deploying them into the production environment. Further, generic accounts wherever possible shall also be removed;
d) The test environment shall also be managed under the same general control environment as the production environment; and
e) All production logs shall be generated and monitored periodically to detect unauthorized activity.

Refer : system acquisition and development policy

10.2. System Planning and Acceptance

10.2.1. Capacity Management

a) Projections of future capacity requirements for the existing and / or new systems / applications shall be planned by the following:
   i. Asset owners of the existing systems / applications;
   ii. Team leads requiring the new system / application.
b) Projections of future capacity requirement shall consider new business and system requirements of Havells;
c) Capacity planning shall specifically provide for capacity enhancements required for security- related logging;
d) System / application / network administrators shall monitor the capacity utilization and project the future capacity requirements to ensure that adequate processing power and storage are available;
e) Capacity thresholds shall be defined for critical information systems, for planning and provisioning additional capacity; and
f) Additional capacity shall be provisioned as and when the information systems reach the defined thresholds.

10.2.2. System Acceptance / Security testing in development and acceptance

a) Acceptance criteria for new information systems, upgrades and new versions shall be defined;
b) Suitable tests, functional test as well as security test of the systems shall be carried out during development and prior to acceptance;
c) Security clearance shall be obtained from IT team before any new information systems, upgrades and / or new versions are accepted;
d) In case of integrated systems consisting multiple elements, security architecture must be approved

by IT team; and

e) User Acceptance Testing (UAT) shall be conducted prior to the deployment of the systems in the production environment.

Refer ; System acquisition and development policy, change management policy.

10.3. Protection against Threats

10.3.1. Controls against Malicious Code

a) The email administrator shall implement email content filtering and virus protection software at the email gateway/ server;
b) Identified malicious attachment shall be quarantined and deleted at the email gateway/server end;
c) Users will get notification about the quarantined emails
d) Users shall not open any files/documents attached in an email from unknown, suspicious, or untrustworthy sources. Attachments with extensions such as '.exe', '.vbs', '.com', '.bat' etc. should be blocked by an anti-virus engine;
e) Users shall not open any files attached to an e-mail whose subject line is questionable or unexpected;
f) Users should send such suspicious email to soc@havells.com for verification and after confirmation from SOC they should open such emails;
g) Users shall delete chain/junk e-mails and not forward or reply to any of the chain/junk mails. These types of e-mail are considered Spam, which is unsolicited and intrusive that clogs up the network;
h) Users shall exercise caution when downloading files from the Internet and should download only from a legitimate and reputable source. Verify that an anti-virus program checks the files on the download site;
i) USB ports shall be blocked for all users, except those where the approval from HOD of the department, CISO / CIO has been received to activate the USB port;
j) Antivirus Protection/ EDR Tools shall be used to protect systems from internet based threats;
k) Internet security and data protection tool shall be installed to protect from Internet threats and data protection;
l) Advanced threat protection tool shall be installed in endpoint for zero day attacks;

10.3.2. Threat intelligence

Information relating to information security threats shall be collected and analyzed to produce threat intelligence.

The Havells Information security team shall implement various advanced security tools to collect, analyze and report threat intelligence.

For threat intelligence, the Havells information security team shall consider below aspetcs

a) Information about existing or emerging threats should be collected and analyzed to

i. facilitate informed actions to prevent the threats from causing harm to the organization.
ii. reduce the impact of such threats.

b) Threat intelligence should be considered in below 3 scenarios:
   i. Strategic threat intelligence: exchange of high-level information about the changing threat and scape (e.g., types of attackers or types of attacks);
   ii. Tactical threat intelligence: information about attacker methodologies, tools and technologies involved;
   iii. Operational threat intelligence: details about specific attacks, including technical indicators.

c) Threat intelligence should be:
   i. relevant (i.e., related to the protection of the organization
   ii. insightful (i.e., providing the organization with an accurate and detailed understanding of the threat landscape);
   iii. contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations);
   iv. actionable (i.e. the organization can act on information quickly and effectively).

d) Threat intelligence activities should include
   i. identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence collecting information from selected sources, which can be internal and external

Refer: Acceptable Usage Policy

10.4. Backup

Backup & restoration management is the process of ensuring that the information generated while conducting business, is available at all times. The backup & restoration management process also ensures that in the event of a disaster, this information can be restored with minimum data loss.

To implement an effective backup & restoration management process, Havells needs to ensure that data is regularly backed up. Restoration shall also be performed on a periodic basis to ensure the integrity and availability of backed up data. Backup and restoration activities shall be scheduled periodically.

Refer: Backup and Restoration Policy

10.4.1. Information Backup

The backup team shall maintain backup calendar in adherence to backup policy which should be reviewed and approved by Backup lead on half yearly basis. In case the backup activity fails, the Backup Administrator should perform root cause analysis, prepare a corrective action plan, and report the issue(s) to respective. A manual backup is recommended in this case.

Refer: Backup and Restoration Policy

10.5. Network Security Management

Network access controls must be designed to manage and protect information integrity and availability on

networks from authorized and unauthorized connections.

Refer: Network Security Policy

10.5.1. Network security

Adequate controls shall be implemented to protect the network from threats and to maintain security of the systems and equipment using the network.

Suitable information security controls shall be implemented in the infrastructure and systems where Havells provides hosting services.

Refer: Network Security Management Policy

10.5.2. Security of Network Services

Security features, service levels and management requirements of all IT network services included in network services agreement shall be identified.

Non-essential services shall be disabled on all information systems. However, these services, if approved by Security Team, shall be enabled by implementing alternative mitigation controls.

Refer: Network Security Management Policy

10.5.3. Segregation of Networks

The Havells network team considers managing the security of large networks by dividing them into separate network domains and separating them from the public network (i.e. internet).

The domains can be chosen based on levels of trust, criticality and sensitivity (e.g. public access domain, desktop domain, server domain, low- and high-risk systems), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units).

The segregation is done using either physically different networks or by using different logical networks.

The perimeter of each domain is well-defined by network team. If access between network domains is allowed, it is controlled at the perimeter using a gateway (e.g. firewall, filtering router).

Wireless access network for guests is segregated from those for personnel if personnel only use controlled user endpoint devices compliant to the organization's topic-specific policies.

Refer ; Network Security management policy

10.5.4. Web filtering

To protect systems from being compromised by malware and to prevent access to unauthorized web resources, the Havells IT team shall control access to external websites to reduce exposure to malicious content.

The Havells shall consider blocking the access to the following types of websites:

a. websites that have an information upload function unless permitted for valid business reasons;
b. known or suspected malicious websites (e.g. those distributing malware or phishing contents);
c. command and control servers;
d. malicious website acquired from threat intelligence
e. websites sharing illegal content.

Refer: Acceptable usage policy

10.6. Media Handling

10.6.1. Storage Media

a) Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the Havell's information classification scheme and handling requirements
b) Copying of data on removal devices such as USB/external drive etc. is prohibited unless approved by the competent authorities. However, for a business requirement, removable media shall be issued only after the approved "Exception Document";
c) Removable media shall be secured and sanitized before its issue to the user;
d) Proper records shall be maintained for the issuance and return of removable media;
e) All removable media shall be stored in secure environment in accordance with manufacturer's specification;
f) Employee shall get proper authorization from the IT department if removable media are required to be taken out of office premises;
g) In the event of loss of removable media, the user shall inform the IT department immediately; and
h) Company Information movement and data access at all channels i.e. Internet, Email, USB shall be monitored by IT team.

Refer : Asset Management policy, Physical security management policy

10.6.2. Secure Disposal or reuse of equipment

a) Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
b) Disposal shall be done only by authorized users and a record shall be maintained of the media disposal; and
c) The previous contents of any re-usable media that are to be removed shall be erased in such a way so that it cannot be recovered. Such disposals shall be authorized by IT department.

Refer : Asset Management policy, Physical security management policy

10.7. Exchange of Information

10.7.1. Information Transfer

a) Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
b) Appropriate security controls (such as technical controls, contractual / agreement requirements) shall be implemented to transfer business information with stakeholders;
c) Users shall ensure that business sensitive information such as 'Confidential', 'Internal use' or 'Public' are handled / treated appropriately as per its sensitivity and criticality;
d) Employees shall share business sensitive information internally or externally to authorized personnel and intended recipient only; and
e) Employees shall not share business sensitive information on social media, public forums, and business conferences, unless authorized.

Refer: Acceptable Usage Policy

10.7.1.1. Physical Media in Transit

a) Documents and removable media carrying confidential information shall be transported using only the services of an authorized courier agency; and
b) It shall be ensured that the courier agency involved in the transport signs a non-disclosure agreement.

10.7.1.2. Electronic Messaging

a) Adequate technical controls shall be designed and implemented to prevent interception, modification and interruption of the information transmitted through email system;
b) Formal guidelines shall be established and communicated to all employees for the use of email system;
c) Employees shall not use any unauthorized web-mail services or portals for the exchange of information.

Refer: Acceptable Usage Policy

10.8. Logging and Monitoring

10.8.1. Logging

a) IT department shall ensure that logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.
b) IT department shall ensure that the audit logs recording the critical user-activities, (including users who accessed restricted data, administrator access), exceptions and security events (like creating or deleting system level objects) shall be enabled and stored. The audit logs shall assist in future investigations and access control monitoring. Audit logs for strictly critical information assets must

be immediately available for a minimum of six months at any given point in time;

c) All logs (including inventory logs) shall be monitored and analyzed for any possible unauthorized use of information systems;
d) Security controls shall be built to ensure the integrity of logs;
e) It shall be ensured that the system administrators do not have permissions to erase or de-activate logs of their own activities;
f) Access to audit trails and logs shall be provided to authorized individuals only.

10.8.1.1. Protection of Log Information

a) Log information shall be protected against unauthorized access, alterations, and operational problems. Access to logs shall be provided on 'need-to-know' and 'need-to-have' basis.
b) Audit logs recording exceptions and other security relevant events shall be produced and kept securely to assist in future investigations and access control monitoring.

10.8.1.2. Administrator and Operator Logs

a) Information systems shall be configured in such a way that the system administrator and system operator activities are logged;
b) These users shall not have access rights to access administrator and operator logs;
c) Administrator and operator logs shall be reviewed at specified intervals.

10.8.2. Monitoring of the activities

Networks, systems and applications is monitored by Havells SOC team for anomalous behavior and appropriate actions taken is taken to evaluate potential information security incidents.

Havells Information Security team has deployed the SIEM solution for monitoring of anomalous behavior, security incidents, rule /Policy violations, unauthorized access attempts and cyber-attacks. Server, network, applications are integrated with SIEM solution for their logs analysis based on the pre-defined rules and generated alerts for any violations. All such security alerts are monitored, notified, analyzed, and resolved in close co-ordination with respective process / domain owners of IT team.

SLA for response and resolution of SOC incidents have been defined and followed up.

10.9. Clock Synchronization

a) Network Administrator should identify Domain controller / authentic NTP which serves as common source, to synchronize the time with a standard time source to Indian Standard Time (IST);
b) The date / time format should be uniform on the systems, network devices and network security devices.

10.10. Configuration management

Configurations including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed by Havells IT team. Standard templates/ hardening documents for the secure configuration of hardware, software, services and networks should be defined:

Network systems, including operating systems, equipment and applications must be hardened in accordance to Hardening Document using publicly available guidance (e.g. pre-defined templates from vendors and from independent security organizations).
This must include:

a) Removing or disabling all unnecessary services;

b) Removing or disabling all unnecessary (including default) accounts;

c) restricting access to powerful utility programs and host parameter settings

d) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity

e) Relevant patching applied in a timely and appropriate manner;

f) Logs are maintained and reviewed where practical;

g) Backups are maintained where appropriate;

h) Applying relevant baseline device configuration templates; and

i) Following best practices and standards where appropriate

Refer : Hardening checklist document

11. Access Control

Control Objectives

The access control section of this policy defines the access controls that need to be implemented and maintained to protect information assets against unauthorized access. The policy intends to establish adequate controls for user access management, networks access, operating system security and mobile computing.

Responsibility

It is the responsibility of the IT department to implement and maintain the controls defined in the access control section of this policy. Procedures to perform this shall be documented in access control policy and password management policy.
Refer: Access Control Policy

Policy Controls

11.1. Access control

To ensure authorized access and to prevent unauthorized access to information and other associated assets, rules to control physical and logical access to information and other associated assets are established and implemented based by IT team on business and information security requirements.

To achieve this, Access control policy and procedures are documented, implemented, and reviewed to protect information assets against unauthorized access based on the business and information seuirty requirements. The procedure shall consider the security requirements of business applications, segregation of access control roles, etc.

11.1.1. Access to Network Services

All network access controls must be based on the following principles:

a) Limit user access on need-to-know basis;

b) Provide users with the minimum of privileges required for their job;

c) Require requests for access to a system be authorized by the information owner or other approving authority;

d) Access to Havells' wireless network shall be granted to guests or vendors after appropriate business approvals;

e) For "Guest" network, access shall be granted to users for one day after appropriate business approvals;

f) For "Vendor or Third party" network, access shall be granted to them for a maximum of 3 months, after appropriate business approvals; and

g) Users having access to network devices shall be reviewed bi-annually.

Refer : Access control Policy, Physical security management policy.

11.1.2. Application and Information Access Control

Logical access to the application software shall be restricted to authorized users only. The appropriate security controls shall be used to restrict access to the application systems of Havells. All applications shall be tested for information security requirements and be compliant to *Havells Systems Acquisition and Development Policy*.

Clearance from the CISO / designated personnel by CISO / CAB shall be obtained prior to deploying systems/application/network equipment in the production environment.

11.1.3. User Access Management

The allocation of access rights to information systems and services shall be done in accordance with the User Access Management procedure. The procedure shall encompass all stages in the life-cycle of user access, from the initial registration to the final de-registration of users, including allocation and authorization required for privileged access rights.

11.1. Identity Management

The 'User' registration and de-registration, for granting / revoking access shall be done in accordance with the User Access Management procedure. The following shall be implemented: -

a) A unique user ID shall be created for all the users having access to the information systems;
b) Departmental Heads shall approve the access request prior to the creation of user IDs of the users;
c) Any user shall not approve his or her access. Segregation of duties shall exist between the request and approval for authorization;
d) Assigning of access privileges including administrator rights to the user shall only be in accordance with the user's role and appropriate approval. The access shall only be used for legitimate business purposes and shall be removed when no longer necessary;
e) The identity of a user shall be determined by a combination of user-name and domain; and
f) Audit trails for all requests for addition, modification or deletion of user accounts / IDs and access rights shall be maintained.

Refer: Access Control Policy

11.2. Authentication information

To ensure proper entity authentication and prevent failures of authentication processes, allocation and management of authentication information is controlled by a management process, including advising personnel on the appropriate handling of authentication information.
Havells IT team has documented and implemented password management policy to address this requirement.

11.2.1. Password Management

Passwords are strings of characters that are input to a system to authenticate an identity and/or authority and/or access rights. Appropriate technical specifications for password management, shall be implemented on the information systems and applications:

a) Employees shall be provided unique credentials (username and password) to access Havells IT

Systems;

b) Employee shall change the default password at first logon;
c) Password shall always be memorized, easy to remember and difficult to guess;
d) Passwords shall be at least twelve characters in length with complexity;
e) Users shall change their password regularly at least once every 60 days; and

Refer: Password Management Policy

11.2.2. Password Use

Employees shall: -

a) Keep their user IDs and corresponding passwords confidential and refrain from sharing them with others;
b) Change their passwords whenever there is any indication of a possible compromise of the system or password;
c) Change passwords for new IDs after first use manually or automatically as systems allow;
d) User's account should be locked out for minimum 15 minutes or till administrator enables the user;
e) Account after more than five invalid logon attempts.

Refer: Password Management Policy

11.3. Privilged Access Rights

Creation and allocation of privileged user accounts / IDs on the information systems shall be authorized according to the user access management procedure. The procedure shall ensure the following: -

a) Privileges shall be allocated to individuals on a 'need-to-have' basis in strict adherence to the authorization process for privilege access;
b) A record of all privilege accounts used on the information systems shall be maintained;
c) Changes made to privileged accounts shall be logged; and
d) The logs shall be reviewed at a specified periodicity.
e) Privilege accounts w.r.t Network devices will be managed via TACAS
f) Privilege Identity Management (PIM) tool is implemented for secure and effective management of privilege access.

Refer: Access Control Policy

11.4. Access Rights

The allocation of access rights to information systems and services shall be done in accordance with the User Access Management procedure. The procedure shall encompass all stages in the life-cycle of user access, from the initial registration to the final de-registration of users, including allocation and authorization required for privileged access rights.

11.4.1. Review of User Access Rights

a) User access rights shall be reviewed at regular intervals for users having access to systems/ applications by respective system owners;
b) Whenever there is a change in the role of a user or a transfer from one department / geography to another department / geography, access rights shall be revoked and reassigned on a "need-to-have" basis;
c) Authorizations for special privileged access rights shall be reviewed at regular intervals by respective system owners;
d) Changes to privileged accounts shall be logged for periodic reviews.

Refer: Access Control Policy

11.4.2. User Responsibilities for Access Management

All employees with access to information assets are required to understand their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

11.5. End Point devices

To protect information against the risks introduced by using user endpoint devices, Information stored on, processed by or accessible via user endpoint devices is protected by technological controls.

Following controls are considered for protecting the end point device:

a) Restriction of software installation (e.g. remotely controlled by system administrators)
b) Requirements for user endpoint device software (including software versions) and for applying

updates (e.g. active automatic updating)

c) Rules for connection to information services, public networks or any other network off premises (e.g. requiring the use of personal firewall);
d) Access control, restriction of local admin rights
e) Storage device encryption
f) Remote lockout, disabling, deletion
g) Protection against malware
h) The use of removable devices, including removable memory devices, and the possibility of disabling physical ports
i) MDM Capabilities
j) VDI
k) Data Leakage protection (DLP)

Refer : acceptable usage policy

11.5.1. Unattended User Equipment

All employees with access to information assets shall be made aware of the information security requirements

according to the clear desk and clear screen section, as defined by IT, for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Refer: Acceptable Usage Policy

11.5.2. Mobility (Mobile Device Policy)

a) Employees shall be allowed to remotely connect to Havells network using mobile computing device to access the business information, only after successful identification and authentication via VPN / VDI etc.;
b) Latest virus definitions shall be regularly updated on the laptops to prevent the corruption of information stored on these devices;
c) Regular training sessions shall be conducted for the employees, leveraging mobility, to increase their awareness on the additional risks resulting from this way of working and precaution that needs to be taken while using the device.

11.6. Clear Desk and Clear Screen

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted in order to reduce the risks of unauthorized access, loss of and damage to information during and outside normal working hours. Following shall be ensured:

a) Where appropriate, paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially during off-office hours;
b) Restricted and Confidential information and storage media shall be locked away (ideally in a fire-resistant safe or cabinet) when not required especially during off-office hours;
c) IT team shall implement the appropriate technological controls to lock the screen of the information systems when unattended beyond a specified duration.

11.7. Access restriction

To ensure only authorized access and to prevent unauthorized access to information and other associated assets, Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control

11.7.1. Information Access Restriction

a) Access to information and application systems shall be in accordance with this policy.
b) System administrator or the person performing the equivalent role shall be required to maintain the updated user access matrix with privileges assigned to the users.

11.7.2. Network Access Control

Logical access to the network equipment shall be restricted to authorized users only. The appropriate security controls shall be used to restrict access to the network systems of Havells. All network equipment's shall be tested for information security requirements. Clearance from the CISO / designated personnel by CISO shall be

obtained prior to deploying network equipment in the production environment. A network security assessment shall be conducted for the critical applications at regular intervals.

11.7.3. Operating System Access restriction

Adequate security controls shall be implemented on the information systems to restrict access to operating systems to authorized users only. The controls shall authenticate the authorized users and record the successful and failed system authentication attempts.

11.8. Secure Authentication

a) User IDs created shall not give any indication of the user's privilege level. For example, User ID shall not be created with names as admin, manager, supervisor, etc.;
b) Havells uses appropriate secure authentication mechanisms such as SSO and Multifactor authentication as per business requirement.

11.8.1. Session Time-Out

Operating systems and applications shall be equipped with session time-out control to lock the screen after 15 minutes of inactivity, unless defined otherwise.

11.9. Access to program source code

To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property, the Havells should ensure that access to program source code, development tools and software libraries is appropriately managed.
The Havells should consider below to control access to program source code

a. Access to program source code repository is restricted and is based on personal role
b. granting read and write access to source code based on business needs
c. updating of source code and associated items and granting of access to source code in accordance with change control procedure
d. not granting developers direct access to the source code repository, but through developer tools
e. maintaining an audit log of all accesses and of all changes to source code

11.10. Use of privileged utility programs

To ensure the use of utility programs does not harm system and application controls for information Security, The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.

The Havells shall consider following measures :

a. limitation of the use of utility programs to the minimum practical number of trusted, authorized users ;

b. use of identification, authentication and authorization procedures for utility programs, including unique identification of the person who uses the utility program;
c. authorization for ad hoc use of utility programs;
d. removing or disabling all unnecessary utility programs;
e. limitation of the availability of utility programs (e.g. for the duration of an authorized change);
f. logging of all use of utility programs.

11.11. Mobility and Teleworking

Appropriate security controls shall be implemented to ensure information security while using mobility and teleworking facilities as defined below.

11.11.1. Teleworking / remote working

Adequate teleworking security measures shall be established and implemented. At a minimum the following shall be ensured:

a) Establishing a secure communication channel between the tele-workers and the networks of Havells;
b) Use of appropriate authentication mechanism for authenticating those using the teleworking solutions; and
c) Revocation of authority, access rights and return of equipment when the teleworking activity ceases or when the employee exits from Havells.

12.Information Systems Acquisition, Development & Maintenance

The information systems acquisition, development and maintenance section of this Policy define the security requirements that need to be identified and integrated during the development and maintenance of information systems and services.

Responsibility

IT team shall be responsible for the implementation of this policy during the acquisition, development and maintenance of information systems and services.

Policy Controls

12.1. Induction of Equipment/Services/Software

The contract with partners/third party shall have provisions to ensure that the equipment/services/software they supply are “safe to connect” in the network.

The condition ‘safe to connect’ would encompass that:

a) Security clearance for equipment/services/software has been conducted;

b) All addressable security concerns have been addressed;

c) Non-addressable security concerns have been listed with remedial measures and precautions provided; and

d) Copies of test results / test certificates shall be maintained as per the business requirement.

Refer: Havells System Acquisition and Development Policy

12.2. Application security requirements

The Havells shall ensure that Information security requirements are identified, specified and approved when developing or acquiring applications.

Refer: Havells System Acquisition and Development Policy

12.3. Secure system architecture and engineering principles

To ensure information systems are securely designed, implemented and operated within the development life cycle, the Havells shall ensure that Principles for engineering secure systems are established, documented, maintained and applied to any information system development activities.

Refer: Havells System Acquisition and Development Policy.

12.4. Secure coding

The Havells application development team shall ensure that secure coding principles are applied to software development to ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.

The Havells shall implement below principles for secure coding

1. Planning and before coding include
    a. common and historical coding practices and defects that lead to information security vulnerabilities
    b. use of controlled environments for development
    c. qualification of developers in writing secure code
2. During coding
    a. secure coding practices specific to the programming languages and techniques being used
    b. using secure programming techniques, such as pair programming, refactoring, peer review, security iterations and test-driven development
    c. documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited
    d. prohibiting the use of insecure design techniques (e.g. the use of hard-coded passwords)
    e. conducting Static application security testing (SAST)
3. Review and maintenance
    a. source code should be protected against unauthorized access and tampering
    b. updates should be securely packaged and deployed
    c. reported information security vulnerabilities should be handled
    d. ensuring that external libraries are managed and regularly updated with release cycles

12.5. Secure development life cycle

To ensure information security is designed and implemented within the secure development life cycle of software and systems, Application development team shall establish and apply rules for secure development of applications and systems.
To achieve this, the following aspects should be considered:

a. separation of development, test and production environments;
b. guidance on the security in the software development life cycle:
c. security in the software development methodology;
d. secure coding guidelines for each programming language used;
e. security requirements in the specification and design phase;
f. security checkpoints in projects;
g. system and security testing, such as regression testing, code scan and penetration tests

h. secure repositories for source code and configuration
i. security in the version control;
j. required application security knowledge and training.

Refer: Havells System Acquisition and Development Policy

12.6. Outsourced Development

To ensure information security measures required by the Havells are implemented in outsourced system development, The Havells should direct, monitor and review the activities related to outsourced system development.

The following points should be considered for outsourced development:

a) licensing agreements, code ownership and intellectual property rights related to the outsourced content.
b) contractual requirements for secure design, coding and testing practices;
c) acceptance testing for the quality and accuracy of the deliverables;
e) provision of evidence that minimum acceptable levels of security and privacy capabilities are established (e.g. assurance reports);
f) provision of evidence that sufficient testing has been applied to guard against the presence of malicious content (both intentional and unintentional) upon delivery;
g) provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;
h) escrow agreements for the software source code (e.g. if the supplier goes out of business);
i) contractual right to audit development processes and controls;
j) security requirements for the development environment;
k) taking consideration of applicable legislation (e.g. on protection of personal data).

12.7. Test Information

To ensure relevance of testing and protection of operational information used for testing, Havells shall ensure that test information is appropriately selected, protected and managed.

Refer: Havells System Acquisition and Development Policy

13.Information Security Incident Management Control Objectives

The Information Security Incident Management section of this policy defines the controls required for early detection, reporting and resolution of security incidents and weaknesses.

Responsibility

IT team at Havells shall be responsible for the development and implementation of the controls defined in this policy.

Refer: Havells Incident Management Policy

Policy Controls

13.1. Information security incident management planning and preparation

The Havells IT team shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Refer: Havells Incident Management Policy

13.2. Assessment of and decision on information security events

The Havells IT team shall assess information security events and decide if they are to be categorized as information security incidents.

13.2.1. Incident Identification

A security incident could be defined as the act of violating the security policy and / or types of cyber security incidents defined as per Cert-In directions dated 28th April 2022. The following is an illustrative list of what actions can be classified as incidents: -

a) Attempts to gain unauthorized access to a system or its data; masquerading, spoofing as authorized users;
b) Unwanted disruption or denial of service;
c) Unauthorized use of a system for the processing, transmitting, or storing data by authorized/
d) Unauthorized access;

13.3. Response to information security incidents

Information security incidents shall be responded by Havells IT team to in accordance with the documented procedures. The documented procedures covers the SLAs for response time and resolution time for addressing information security incidents.

Refer: Havells Incident Management Policy

13.4. Information security event reporting

The Havells IT team shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. The information security incidents can be logged by dialing designated voice calling number or reporting an incident on designated email id as mentioned in the incident management policy.

Refer: Havells incident management Policy.

Reporting Information Security Incidents and Weaknesses

a) All employees shall report any IT related security incident or weakness to IT Helpdesk / SOC.
b) It is mandatory to report cyber incidents as mentioned in Annexure:- I of CERT-In direction. Cyber incident having material impact with respect to continuation of Business operation, financial loss, damage to company's reputation, legal labilities, and compromised of sensitive data/information shall be reported " to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents in accordance with the criteria defined under company's "ISMS (Information Security Management System) -Risk Management Policy"
c) As per SEBI amendment LODR (Listing Obligations and Disclosure Requirements) Regulations, 2015, Details of cyber security incidents or breaches or loss of data or documents shall be disclosed along with the Quarterly Report on Corporate Governance filed by the Company within 21 days of quarter end
d) A dedicated email ID (Cyberincident@havells.com) has been created for the reporting such incidents to Cert-In / other agencies as may be applicable.
e) Employees shall be made aware of the possible security incidents that could impact the information assets of Havells and their responsibilities for reporting the incidents or weaknesses they observe.

13.5. Learning from Information Security Incidents

a) The Incident Response Team at Havells shall establish a knowledge base for the information gained from the evaluation of all information security incidents.
b) The knowledge base shall be referred to for incident handling and as a learning source of information security incidents.
c) The learning from evaluation of information security incidents shall be documented / updated in respective tool to the possible extent

13.6. Collection of Evidence

Where a follow-up action against a person or organization after an information security incident involves legal action, (either civil or criminal) evidences shall be collected, maintained, and presented to the relevant authorities as per the company policy / DOA.

14.Risk Assessment and Business Continuity Management

Havells has defined and documented an appropriate method for Risk Assessment (henceforth defined as RA) that shall enable the organization to understand risks to its critical business processes, sites, IT, network infrastructure, and supporting resources including those provided by any third party providers.

The Business Continuity Management section of this Policy defines the intent of the Havells management to establish a business continuity plan to counteract or minimize interruptions to key business activities. The interruptions could be due to natural or manmade disasters, or technology incidents which might convert into disasters. The organization supporting business continuity plan shall have representation from all the business units which should ensure a structured development, implementation, exercising, review, and update cycle of the business continuity plan.

This section of the HISP shall be reviewed at least annually or whenever significant changes occur in the organization.

Responsibility

IT team at Havells shall be responsible for the development and implementation of the controls defined in this policy.

Refer: Havells Business Continuity Policy

Policy Controls

14.1. Risk Assessment and Business Continuity

Havells shall identify events that can cause interruptions to organizations key business processes e.g. equipment failure, human errors, theft, fire, natural disasters, and act of terrorism. They shall be followed by a risk assessment to determine probability and impact of such interruptions, in terms of time, damage, scale and recovery period.

14.1.1. Risk Assessment

a) Havells shall carry out RA for all critical business processes, support resources and sites at pre-defined frequencies. RA shall also be carried out for IT and network infrastructure to identify single points of failure;
b) IT shall conduct periodic (at least annual) risk assessment for the network and application risk assessment to examine the threats that can cause harm, loss, or damage to assets of the organization;
c) The risk assessment shall involve analyzing risk, assessing the controls already in place to address the risk and assessing the residual risk;
d) Based on the findings of the risk assessment, Havells shall prioritize and implement additional controls to reduce the exposure to threats to an acceptable level;
e) RA shall be reviewed on an annual basis;
f) Control implementation as well as risk arising out of control implementation shall also be reviewed

on an annual basis;

g) The ISC shall monitor the implementation of controls by the risk owners against risks arising out of the RA exercise.

Refer: Risk Management, Risk Assessment & Recovery Strategy Procedure

14.1.2. Maintenance of business continuity plan

Business continuity plan shall be reviewed and updated on an annual basis. In addition, the plan shall be updated if any changes to the operating environment occur, such as:

a) Facility changes;

b) Equipment changes;

c) Major changes to existing applications;

d) Off-site storage location changes;

e) Major software upgrades or installs; and

Changes to backup procedures.

14.2. Information security during disruption

a) Havells shall document business continuity plans. The CISO/ CIO and department heads at Havells shall own and maintain these plans. The business continuity plans shall cater to employee safety, L&R compliance, crisis management, crisis communication, business process recovery, IT and network recovery, information security, site emergency management, plan activation and deactivation steps;

b) The Havells shall plan how to maintain information security at an appropriate level during disruption

c) The Network recovery plans shall be owned and maintained by the respective department heads and signed off by CISO;

d) Havells shall carry out an on ground implementation of all business continuity plans, IT and Network recovery plans.

e) It would be the responsibility of respective department heads to ensure that documented business continuity strategies are implemented as defined in the plans. Department heads shall ensure implementation of the plans as and when the plans are reviewed and revised.

14.3. ICT readiness for business continuity

a) ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

b) The Havells shall ensure that

i. An adequate organization structure is in place to prepare, response and mitigate to disruption

ii. ICT continuity plans, including response and recovery procedures are in place

iii. The plans are regularly evaluated through exercise and tests

14.4. Testing, maintaining, and re-assessing business continuity plans

14.4.1. BCMS Exercising

a) IT head shall conduct DR tests at least on a bi-annual basis;
b) Respective department heads shall conduct walkthrough of business continuity plans as part of self-assessment exercise on an annual basis;
c) Exercising methodologies shall be clearly defined, where such exercises should be scoped, signed off by respective departmental heads (CIO), monitored for adherence to plan and reporting of results of the exercises to the ISC. The ISC shall review the test results at regular frequencies.;

14.4.2. BCM Monitoring

a) Department Heads shall carry out monitoring of the BCMS to ensure that the update and maintenance of the BCMS is being carried out effectively;
b) There shall be defined self-assessment, internal audit programs to check effectiveness of BCMS for all departments.

14.4.3. Corrective Actions and Preventive Actions

a) Havells shall ensure continual improvement of BCMS through the application of corrective and preventive actions;
b) The triggers for corrective and preventive actions can be from BCMS testing, changes in the organization, incidents, and audit observations from internal and third party audits;
c) The corrective and preventive actions taken shall be reviewed in self-assessments, internal audits, and management reviews.

14.5. Redundancy of information processing facilities

To ensure the continuous operation, Havells shall implement redundancy sufficient to meet availability Requirements.

The Havells should consider the following when implementing redundant systems:

a) contracting with two or more suppliers of network and critical information processing facilities such as internet service providers
b) using two geographically separate data centers with mirrored systems
c) using physically redundant power supplies or sources
d) having duplicated components in systems (e.g. CPU, hard disks, memories) or in networks (e.g. firewalls, routers, switches)

Where applicable, preferably in production mode, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

15. Compliance

The Compliance Policy provides direction to design and implement appropriate controls to meet legal, regulatory, statutory, and contractual obligations within different departments of Havells.

Responsibility

Concerned Business / Functional / IT Teams shall implement appropriate controls ensuring prevention of misuse of business information and facility.

Policy Controls

15.1. Compliance with Legal Requirements

15.1.1. Legal, statutory, regulatory and contractual requirements

a) A list of all relevant statutory, regulatory, and contractual requirements shall be maintained by the Legal department;
b) The list of applicable legislations shall be reviewed and approved at least once a year or whenever there is a change in any statutory, regulatory, contractual obligations.

15.1.2. Intellectual Property Rights (IPR)

Intellectual Property Rights (hereinafter referred to as 'IPR') shall be included in all the contracts, and shall be implemented to ensure, but not limited to:

a) Compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be IPR.
b) IPR including software or document copyright, design rights, trademarks, patents, and source code licenses are not infringed.
c) Only licensed software shall be installed within Havells network environment. Record of all software licenses shall be kept and updated regularly.

15.1.3. Protection of Records

a) The relevant business, legal and regulatory requirements shall be identified and documented for storing and segregate as per their criticality
b) The organizational records shall be maintained and stored in a secure manner to prevent any loss, destruction, or falsification. The retention period of these records shall be identified and recorded;
c) Respective department heads shall ensure the retention of organizational records such as CDRs backup, log storage, books of account, etc. in accordance with legislative, regulatory, and contractual requirements;
d) Data that is no longer required for business, legal and/ or regulatory purpose shall be securely disposed of;

15.1.3.1. Prevention of Misuse of Information Processing Facilities

Controls shall be implemented to prevent employees from accessing the information, information systems and/ or facilities for unauthorized purposes.

15.1.4. Use of cryptography

a) Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
b) Suitable procedure for compliance assurance shall be documented and maintained by the IT Team with support from the Legal and Regulatory departments.
c) Licensing requirements such as restrictions on export of encryption keys including remote access must be met.
d) Cryptographic keys must be managed in compliance as per the standard.

15.1.5. Privacy and protection of personally identifiable information (PII)

The Havells shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

The Havells should develop and implement procedures for the preservation of privacy and protection of PII.

Refer : Information classification, data masking and PII Policy

15.2. Compliance with security policies and standards and Technical Compliance

15.2.1. Compliance with security policies, rules and standards

a) IT team shall ensure that Havells information security policy and related procedures are implemented to meet the compliance requirements.
b) Security Team shall have the authority to perform compliance checks against each security policy, in accordance with the agreed procedures. The frequency of such compliance checks shall be performed according to the size of the facility or prior audit results.
c) If any non-compliance is found as a result of the review, Security Team shall:
   i. Determine the causes of the non-compliance;
   ii. Evaluate the need for actions to avoid recurrence of the same;
   iii. Determine and implement appropriate corrective action;
   iv. Review the corrective action taken.
d) Results of reviews and corrective actions carried out shall be recorded and these records shall be maintained.

15.2.2. Management of technical vulnerabilities

a) IT Team shall conduct technical compliance checking at periodic frequency either manually or with the assistance of automated tools;
b) IT department shall obtain a security clearance for all new projects, products, applications, services, etc. from the CISO/designated person appointed by CISO during their initiation and prior to deployment in operational environment;
c) Technical compliance checking shall cover penetration testing and vulnerability assessments every quarter or whenever any significant change happens in the system; this can be carried out internally or by independent experts specifically contracted for this purpose. Compliance testing must be

conducted at least once in a year for restricted information assets.

15.3. Protection of information systems during audit testing

15.3.1. Information Systems Audit Controls

a) Audit requirements on the operational systems shall be planned, documented, and agreed in order to minimize the risk of disruptions to business processes.

b) Copies of the system files shall be provided for appropriate protection till it is required.

15.3.2. Protection of Information Systems Audit

a) All information audit systems shall be protected to prevent their misuse.

b) The authorization process for acquiring, testing, and maintaining the audit tools shall be followed.

16. Network Security Policy

16.1. Introduction

a) Havells, in its constant endeavor to strengthen the security posture of the organization and to adhere to the legal and regulatory requirements, is focusing on security of its core network assets and operations. The Network Security Policy defines control to protect the network assets.

b) Network Security Policy defines control for all network assets, underlying infrastructure and various interfaces and interconnections with/ between the network assets.

16.1.1. Network Security Management

Suitable network security controls shall be implemented across the application, services and infrastructure layers of user, control, and management planes of the network.

16.1.2. Network Security Requirements

Security of network assets of Havells is significant and the communication network shall be protected against the threats to the network. It is important to ensure adequate security measures to protect the Havells network.

Refer: Network Security Management Policy

Annexure A: Risk Assessment and Treatment

Objective

Security risks associated to information assets of Havells shall be identified to determine the safeguards to be implemented to reduce the level of risk or to lessen the impact of a security breach. The objective of risk assessment shall be to identify the probability of the occurrence of threats, and their impact on the confidentiality, integrity, and availability of information assets of Havells.

Risk Assessment

a) Information assets of Havells shall be subjected to Risk Assessment in accordance with the Risk Assessment Methodology of Havells. As part of this exercise, risks shall be identified along with appropriate control measures to mitigate / minimize the risks.

b) Risk Assessment shall be conducted and reviewed at least once in a year to identify and analyses the associated risks and develop and implement adequate control measures.

c) Risk Assessment shall include:

i. Identification of the information assets used by different departments of Havells. The identified information assets shall be collated in the Risk Registers.

ii. Identification of the vulnerabilities and threats that shall expose the information assets to information security risks. A Gap Analysis shall be conducted to evaluate the existing control measures as compared to the control objectives.

iii. Analysis of the risks in accordance with the Risk Assessment Methodology and determination of the mitigation plan to reduce the level of risk.

d) All the identified control measures shall be put in place in addition to the controls defined in this policy or related procedures.

Risk Treatment

a) Risk Treatment Plan (RTP) shall be developed to mitigate / minimize the risks identified as a result of the Risk Assessment, in accordance with the Risk Assessment Methodology of Havells.

b) RTP shall elaborate the actions to be taken or the controls to be implemented to mitigate / Minimize the risks.

c) In cases where the management decides not to implement certain controls and accept the risks, Proper justification shall be provided, and such acceptable level of risks would be signed off / approved on email by the business. The risk signs off would be reviewed and approved, at least on an annual basis or on change of the business conditions and environment.

d) Regular monitoring shall be done to track the implementation of the controls as planned in the RTP.

Technical Risk Management

Risk Assessment

a) IT Team / SOC shall periodically conduct risk assessment to examine the threats to the network that can cause harm, loss, or damage to assets of the organization.

b) The risk assessment shall involve analyzing risk, assessing the controls already in place to address the risk and assessing the residual risk.

c) Based on the findings of the risk assessment, Havells shall prioritize and implement additional controls to reduce the exposure to threats to an acceptable level.

Technical Vulnerabilities

a) IT Team / SOC shall identify and document all technical vulnerabilities of information systems and evaluate the exposure to such vulnerabilities.

b) To do so, IT Team / SOC shall implement technical vulnerability management including: -
- Vulnerability monitoring,
- Vulnerability assessment and
- Vulnerability closure through implementation of appropriate controls to mitigate the risks.

c) . Vulnerability Assessment shall be carried out once in an year for all Equipment and their supporting components

d) Information systems with vulnerabilities leading to high risks shall be addressed on priority. Following shall be used as a reference for time periods of closing vulnerabilities/ gaps/ non-compliances.

Risk Category	Time Period for mitigation
Critical and High	30 days
Medium	60 days
Low	90 days