QRG Investments and Holdings Limited

Information Security Policy

Version 2.0

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	QRG Investments and Holdings Limited Information Security Policy
2.	Document Code	QRGIHLISP
3.	Date of Release	October 22, 2022
4.	Document Superseded	
5.	Document Approvers	Board of Directors

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	October 22, 2022
1.0	NA	No Change	October 04, 2023
2.0	February 06, 2024	As per RBI Master Directions, Nov,23.	February 06, 2024

Table of Contents

1. General

1.1. Management intent

The Information Security policy document defines QRG Investments and Holdings Limited ("QRGIHL") position on information security. QRGIHL' 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 QRGIHL' information and information assets.

QRGIHL' 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 QRGIHL Information Security Policy (QRGIHLISP) provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage the information security in QRGIHL. QRGIHL 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 QRGIHL and the third parties supporting QRGIHL' operations; and
d) Taking appropriate actions for any violations of the QRGIHLISP.

2. Abbreviations

Abbreviation	Meaning
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
CIO	Chief Information Officer
CIA	Confidentiality, Integrity and Availability
DR Plans	Disaster Recovery Plans
HR	Human Resources
IPR	Intellectual Property Right
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.

Keyword	Definition
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.
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 QRGIHL. 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 QRGIHL.
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 QRGIHL 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 QRGIHL. It shall include QRGIHL 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 27001:2013 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 are aligned to the domains and controls as per clauses A.5 through A.18 in the ISO 27001:2013 standard in the similar sequence; and
d) Annexure in this policy have been defined to ensure compliance with the clauses of the ISO 27001:2013 standard.

5. Information Security Policy

Control Objective

QRGIHL Information Security Policy provides management direction and support to ensure protection of QRGIHL' 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 QRGIHL 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

QRGIHL Information Security Policy is applicable to information and information assets of QRGIHL.

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

5.2. Review of Information Security Policy

QRGIHL 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. QRGIHL Information Security Policy shall be reviewed in consultation with relevant stakeholders and approved by the CIO 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 QRGIHL' IT and/or handle, process or manage information/information assets of QRGIHL, 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.

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.

6. Information Security Organization

Control Objective

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

Responsibility

It is the responsibility of the CIO to manage the information security organization within QRGIHL. CIO 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 commitment to information security

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 QRGIHL.

6.1.2. Information security co-ordination

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

6.1.3. 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

6.1.4. Confidentiality Agreements

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

6.1.5. Contact with Authorities

QRGIHL 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.

6.1.6. Contact with Special Interest Group

CIO 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 QRGIHL.

6.1.7. Independent review of information security

QRGIHL' 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.

6.2. External Parties

6.2.1. Identification of risks related to external parties

The risks to QRGIHL' 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 security in third party agreements

Agreements with third parties involving accessing, processing, communicating, or managing QRGIHL' 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) QRGIHL 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 QRGIHL' 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 QRGIHL' Information Security policy.

7. Asset Management

The clauses in asset management establish the requirement of controls that need to be implemented for protecting assets of QRGIHL. Assets of QRGIHL 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.

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 QRGIHL locations.

7.1.1. Inventory of assets

The Company shall maintain Inventory of IT Assets. The IT Asset Inventory shall include details about the asset such as asset date of purchase and cost of assets as at book value.

8. 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 QRGIHL 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.

8.1. Physical Security Controls

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

8.1.1. Physical Security Perimeter

The administration department shall define physical security perimeter for head office where information assets of QRGIHL are located.

8.2. Equipment Security

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

9. 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

9.1. Operational Procedures and Responsibilities

9.1.1. Documented Operating Procedure

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

9.1.2. 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.

9.1.3. 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 QRGIHL 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.

9.1.4. 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.

9.2. System Planning and Acceptance

9.2.1. 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 QRGIHL;
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.

9.2.2. System Acceptance

a) Acceptance criteria for new information systems, upgrades and new versions shall be defined;
b) Suitable tests 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.

9.3. Protection against Threats

9.3.1. 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, 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;

9.4. 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, QRGIHL 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.

9.4.1. 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.

9.5. Network Security Management

Network access controls must be designed to manage and protect information integrity and availability on networks from authorized and unauthorized connections.

9.5.1. Network Controls

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 QRGIHL provides hosting services.

9.5.2. 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.

9.6. Media Handling

9.6.1. Management of Removable Media

a) 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";
b) Removable media shall be secured and sanitized before its issue to the user;
c) Proper records shall be maintained for the issuance and return of removable media;
d) All removable media shall be stored in secure environment in accordance with manufacturer's specification;
e) Employee shall get proper authorization from the IT department if removable media are required to be taken out of office premises;
f) In the event of loss of removable media, the user shall inform the IT department immediately; and
g) Company Information movement and data access at all channels i.e. Internet, Email, USB shall be monitored by IT team.

9.6.2. Disposal of Media

a) Media containing critical and sensitive information shall be disposed-off in a secure manner;
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.

9.7. Exchange of Information

9.7.1. Information Exchange Policies and Procedures

a) Appropriate security controls (such as technical controls, contractual / agreement requirements) shall be implemented to exchange business information with stakeholders;
b) Users shall ensure that business sensitive information such as 'Confidential', 'Internal use' or 'Public' as per the sensitivity and criticality;
c) Employees shall share business sensitive information internally or externally to authorized personnel and intended recipient only; and

d) Employees shall not share business sensitive information on social media, public forums, and business conferences, unless authorized.

9.7.2. 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.

9.7.3. 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.

9.8. Logging and Monitoring

9.8.1. Audit Logging

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

9.8.2. 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.

9.8.3. 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.

9.9. 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. 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.

Policy Controls

10.1. Access control policy

Access control policy and procedures shall be documented, implemented, and reviewed to protect information assets against unauthorized access. The procedure shall consider the security

requirements of business applications, segregation of access control roles, etc.

10.1.1. 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.

10.1.2. User 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.

10.1.3. Privilege Management / TACAS

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

10.1.4. 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 QRGIHL 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

10.1.5. 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.

10.2. 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.

10.2.1. 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.

10.2.2. 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.

10.2.3. 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.

10.3. 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 QRGIHL. All network equipment's shall be tested for information security requirements. Clearance from the designated personnel 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.

10.3.1. 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 QRGIHL' 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.

10.4. Operating System Access Control

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.

10.4.1. Secure Log-on

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) QRGIHL uses appropriate secure authentication mechanisms such as SSO and Multifactor authentication as per business requirement.

10.4.2. 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.

10.5. 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 QRGIHL. All applications shall be tested for information security requirements.

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

10.5.1. 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.

10.6. Mobility and Teleworking

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

10.6.1. Mobility

a) Employees shall be allowed to remotely connect to QRGIHL 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.

10.6.2. Teleworking

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 QRGIHL;
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 QRGIHL.

11. 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

11.1. 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.

12. 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 QRGIHL shall be responsible for the development and implementation of the controls defined in this policy.

Policy Controls

12.1. Incident Identification

A security incident could be defined as the act of violating the security policy. 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 users;

12.2. Reporting Information Security Incidents and Weaknesses

a) All employees shall report any IT related security incident or weakness to IT Helpdesk / SOC.
b) 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) 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) d) A dedicated email ID (itsupport.helpdesk@havells.com) has been created for the reporting such incidents to Cert-In / other agencies as may be applicable.

e) 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.

12.3. Learning from Information Security Incidents

a) The Incident Response Team at QRGIHL 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

12.4. 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.

13. Risk Assessment and Business Continuity Management

QRGIHL 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 QRGIHL 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 QRGIHLISP shall be reviewed at least annually or whenever significant changes occur in the organization.

Responsibility

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

Policy Controls

13.1. Risk Assessment and Business Continuity

QRGIHL 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.

13.1.1. Risk Assessment

a) QRGIHL 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, QRGIHL 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 CIO shall monitor the implementation of controls by the risk owners against risks arising out of the RA exercise.

13.1.2. 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.

13.2. Developing and implementing continuity plans including information security

a) QRGIHL shall document business continuity plans. The CIO and department heads at QRGIHL 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, site emergency management, plan activation and deactivation steps;
b) The Network recovery plans shall be owned and maintained by the respective department heads and signed off by CIO;
c) QRGIHL shall carry out an on ground implementation of all business continuity plans, IT and Network recovery plans.
d) 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.

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

14.3.1. BCMS Exercising

a) IT head shall conduct DR tests at least on a bi-annual basis for critical applications and risk based approach for non-critical applications;
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 CIO. The CIO shall review the test results at regular frequencies.;

14.3.2. 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.

14.3.3. Corrective Actions and Preventive Actions

a) QRGIHL 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. Compliance

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

Responsibility

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

14.1. Compliance with Legal Requirements

14.1.1. Identification of Applicable Legislation

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.

14.1.2. 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 QRGIHL network environment. Record of all software licenses shall be kept and updated regularly.

14.1.3. Protection of Organizational 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;

14.1.4. 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.

14.1.5. Regulation of Cryptographic Controls

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.

14.2. Compliance with security policies and standards and Technical Compliance

14.2.1. Compliance with security policies and standards

a) IT team shall ensure that QRGIHL 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.

14.2.2. Technical Compliance Checking (May be introduced in due course)

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 designated person appointed by CIO during their initiation and prior to deployment in operational environment;

c) Technical compliance checking shall cover Vulnerability Assessments (VA) every half yearly (for Critical Application) or whenever any significant change happens in the system. For non-critical information systems, a risk-based approach shall be adopted to decide the requirement and periodicity of conduct of VA/PT.

d) Penetration testing should be done atleast annually for critical applications; this can be carried out internally or by independent experts specifically contracted for this purpose. Compliance testing should be conducted annually for restricted information assets.

14.3. Information Systems Audit Considerations

14.3.1. 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.

14.3.2. 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.

15. Network Security Policy

15.1. Introduction

a) QRGIHL, 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.

15.2. Communications and Operations Management

15.2.1. 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.

15.2.2. Network Security Requirements

Security of network assets of QRGIHL 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 QRGIHL network.

16. Document Management

- Any amendment to this policy/ procedure or issue of any guidance or circular etc. under this policy/ procedure has to be incorporated in the policy on an ongoing basis by the Management.
- This policy will be reviewed atleast every year by Board/ Committee.
- This procedure replaces any other procedure issued earlier by the Company to the extent specifically covered here. This policy should be followed both in letter and spirit.
- The Company is committed to continuously reviewing and updating policies and procedures-based on the Company's risk assessment and incorporating any regulatory requirement as maybe required.
- Any amendment to this procedure or issue of any guidance or circular etc. under this procedure has to be approved in writing by the approving authority.

****

Annexure A: Risk Assessment and Treatment

Objective

Security risks associated to information assets of QRGIHL 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 QRGIHL.

Risk Assessment

a) Information assets of QRGIHL shall be subjected to Risk Assessment in accordance with the Risk Assessment Methodology of QRGIHL. 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 QRGIHL. 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 QRGIHL.
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 bereviewed 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, QRGIHL 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 critical system and application including cloud 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.
e)

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

Network Hardening -

Network systems, including operating systems, equipment and applications must be hardened in accordance to Hardening Document. This must include:

a) Removing or disabling all unnecessary services;
b) Removing or disabling all unnecessary (including default) accounts;
c) Relevant patching applied in a timely and appropriate manner;
d) Logs are maintained and reviewed where practical;
e) Backups are maintained where appropriate;
f) Applying relevant baseline device configuration templates; and
g) Following best practices and standards where appropriate.

Maker-Checker Policy -

Maker-checker is one of the important principles of authorization in the information systems of financial entities. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information.