GHCL LIMITED

INFORMATION SECURITY POLICY

Doc. No. ISP/003

Revision No. 003

Publish Date: 1-Apr-24

Table of Contents

1. Objective

The objective of this policy is to provide guidance and a framework to ensure that GHCL Limited (hereafter, referred to as GHCL) information assets are provided comprehensive protection against breaches of confidentiality, failures of integrity, and/or interruptions to their availability.

This policy aims to minimize the risk of damage by preventing security incidents, reducing their potential impact and ensure the business continuity at GHCL. The information security policy (ISP) establishes a framework for implementation and compliance of information security within GHCL. GHCL IT Security team shall provide a strategic direction to demonstrate the importance of information security to business processes. This direction shall be adopted, propagated, and maintained by GHCL.

ISO 27001 Clauses Addressed:

A.5.1.1 – Information Security Policy Document

A.5.1.2 – Review of the Information Security Policy

2. Scope & applicability

The scope of this policy includes the following:

- Information assets: All information assets (data) either owned by GHCL or entrusted to the company by a client under an agreement which specifically details GHCL's responsibilities for that data and includes:

Information assets held, processed, or stored on the premises of GHCL

Information assets held, processed, or stored at approved off-site premises or locations.

- Supporting assets: All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described above, including:

Premises: e.g., offices, laboratories, workshops, data centers, storage facilities and recovery sites

Hardware: e.g., servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices

Software: e.g., operating systems, off-the-shelf software applications and software applications developed by third parties for GHCL

Company Personnel: e.g., permanent, temporary, full time and part time employees, authorized contractors, and any third-party users of GHCL's information systems

- Documentation and Records: All policies, processes, procedures, work instructions and records related to management, use, control and disposal of the information assets and their supporting assets as detailed above.

This policy shall apply to all employees, contractors, and third-party users within GHCL.

3. Policy

3.1 General requirements:

3.1.1 GHCL shall be committed to the protection of all its information assets, as defined within the scope of this policy.

3.1.2 GHCL shall define and maintain a comprehensive inventory of all assets, including all information assets and supporting assets. Each information asset shall have a designated asset owner, custodian, and users. The asset inventory shall be periodically reviewed and updated.

3.1.3 GHCL shall define and document a formal access control policy to ensure that all information assets, and their supporting assets, are protected to ensure that their confidentiality, integrity, and availability is maintained. Access to information assets and supporting assets shall be in accordance with GHCL's physical & logical access control policies.

3.1.4 GHCL shall define and document a formal data classification and handling policy to ensure that all information assets are classified and handled adequately in accordance with their classification scheme requirements. This policy also provides guidance on the appropriate levels of personnel screening or clearances necessary to access information of different classifications.

3.1.5 GHCL shall define and document a formal acceptable usage policy to ensure that all personnel, contractors, and third-party users are aware about how information assets and supporting assets should be used in an acceptable manner. This policy shall detail the acceptable methods of use of information processing systems, networks including for e.g., the internet and the telephone systems- and other resources within the scope of this policy.

3.1.6 GHCL shall perform periodic risk assessments on all information assets in accordance with its risk assessment procedure. The documented results of risk assessment shall be reviewed to understand the level of risk to information and to supporting assets, and appropriate controls shall be implemented to address any unacceptable risks that have been identified.

3.1.7 GHCL shall have a formal mechanism for handling and responding to information security incidents and shall define and document an information security incident management policy. The policy shall include identification, reporting, investigation, resolution, and closure of information security incidents.

3.1.8 GHCL shall ensure that information security requirements are considered within its business continuity and recovery practices such that the security of its information assets is not compromised even when faced with a wide variety of unplanned business interruptions.

3.1.9 GHCL shall also ensure that its information security policies and practices are in line with regulatory, legislative, and legal and other applicable requirements. \

3.2 Management direction for information security:

3.2.1 GHCL shall provide management direction and support for information security in accordance with business requirement(s) and relevant laws and regulations.

3.2.2 A set of supporting policies and procedures for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties.

3.2.3 GHCL shall maintain a security awareness program for all employees and suppliers to ensure that staff awareness is refreshed and updated as necessary.

3.2.4 Suppliers (third-party contractors, vendors, external consultants, etc.) shall be required to undertake information security awareness sessions for their staff engaged with GHCL and submit records of the same to ORG.

3.2.5 GHCL management shall review the defined policies and procedures on a periodic basis, or in the event of any significant changes within the company, to ensure their continuing suitability, adequacy, and effectiveness.

3.2.6 The review shall include assessing opportunity for improvement of policies and approach to manage information security in response to changes to organizational environment, business circumstances, legal or regulatory conditions.

3.2.7 Based on the outcome of the reviews, additional policies could be issued and/ or existing policies shall be updated, as required. Policies that are identified to be redundant shall be withdrawn.

4. Organization of Information Security

Information security organization plays a key role in achieving information security objective of Confidentiality, Integrity, and Availability. Information security organization’s structure ensures:

Allocation of responsibilities

Accountability

Senior Management involvement and Commitment

4.1. Roles and Responsibilities

This defines roles and responsibilities related to establishing Information Security Organization.

Sr. No. Role Responsibility

1. ISMF

1. Provide leadership and commitment towards the protection of GHCL information assets.

2. Establish working groups or sub-committees to identify and develop strategic direction and recommendations.

3. Approve all policy matters related to information Security.

4. Approve the revisions to GHCL's information security policies.

5. Approve assignment of specific roles and responsibilities for information security across the organisation.

6. Ensure that information security management reviews are conducted periodically and decide acceptable levels of information security risks.

2. IT-Head

1. Identify information security objectives and align them to the corporate strategic plans.

2. Manage the development, update and implementation of security policies and related procedures to ensure ongoing maintenance of information security.

3. Coordinate information security efforts within ORG.

4. Maintain relationships with all appropriate internal and external stakeholders.

5. Ensure development of an effective information security awareness program to impart awareness to all the employees.

6. Manage the development, implementation and updating of risk assessment methodology to identify information security risks.

7. Develop, implement, and maintain an effective compliance monitoring and reporting program to monitor compliance with information security policies including a security review by an independent third party.

8. Report information security compliance to ISMF;

9. Communicate information security plans and programs to maintain information security awareness.

3. ISIT ISM

1. Administer the information security program and assess whether the program is implemented in accordance with information security policies and standards.

2. Review requested exceptions to information security policies, standards, and procedures.

3. Provide solutions, guidance, and expertise in IT security.

4. Maintain awareness of security status of sensitive IT systems.

5. Facilitate effective implementation of information security program, by:

- Preparing, disseminating, and maintaining information security policies, standards, guidelines, and procedures, as appropriate

- Collecting data relative to the state of IT security and communicating as needed

- Providing consultation on balancing an effective information security program with business needs

4 GHCL Employees, Contractors, Vendors & Third parties

1. Make themselves aware of and understand their information security requirements and responsibilities.

2. Make themselves aware of and understand ORG's Information Security Policies and related procedures.

3. Ensure adherence to & compliance with ORG's information security policies, procedures, and related guidelines.

4. Take all reasonable precautions to protect information assets against unauthorised access, use, disclosure, modification, duplication, or destruction.

5. Use information systems only as appropriate for their job responsibilities.

6. Use available mechanisms and procedures to protect their own data and company data under their control.

7. Assist and co-operate in the protection of information and information processing facilities.

8. Use information systems only for their intended purpose; and

9. Report security incidents and weaknesses.

5. Abbreviations

1. ISMF: Information Security Management Forum

2. ISIT: Information Security Implementation Team

3. ISM: Information Security Manager

4. SOP: Standard Operating Procedures

6. Exceptions

There may be instances where there is a justifiable business need to perform actions that conflict with GHCL's information security policies and procedures. To provide flexibility in such instances, this component of Information security policy shall be referred to get details of actions that are required to obtain a waiver from compliance to a specific policy.

Any person who identifies an exception to the information security policy that occurs to successfully complete business operations shall immediately forward the request to his / her reporting manager. The reporting manager shall analyse the request and will forward it to the function owner and IT-Head for approval. After the approval from the function owner and IT-Head, information security team shall review and validate the requirement and forward it to the IT team for implementation. At the minimum, following requirements shall have to be met when an exception is requested:

1. Requests for exceptions to policies shall have a justifiable business case documented and shall have the necessary approvals. The respective function owners shall approve exceptions prior to the action of the IT-Head/information security team.

2. Any exception approved shall be valid for a limited period, maximum of one year after which it shall be re-evaluated.

3. If policy exceptions are likely to circumvent existing, internal controls then "Mitigating Controls" or "Compensating Controls" shall be implemented and followed.

Any person who becomes aware of any loss, compromise, or possible compromise of information, or any other incident, which has information security implications, shall immediately inform his/her line manager or functional head, who shall initiate immediate action to prevent further compromise or loss. The functional head with support from the information security, compliance and HR teams shall be responsible for getting the incident investigated as per the defined procedure.

7. CHANGE LOG

1.	Type of Document	Policy
2.	Recommended by Audit & Compliance Committee	July 29, 2019
3.	Approved by Board of Directors	July 29, 2019
4.	Approved by IT head	November 1, 2023
4.	Reviewed by Managing Director	April 1, 2024
5.	Document Control	IT Department

For GHCL Limited

R S Jalan Managing Director