Information Security Policy

Date: 22-05-2023

Document Status: Approved

Version: 2.1

Document Owner: Corporate IT

#	Version No.	Date	Change Description
1	1.6	22/02/2022	New policy
2	2.0	13/01/2023	Section 6 added, clause for role-based trainings added in section 8, Information handling guidelines added in section 15, privilege access review frequency changed from quarterly to monthly in section 16.2, Section 16.3 updated, CCTV recording details updated in section 17.1, Section 21 – USB policies updated, Section 22 updated, Section 23 – policies for source code protection and outsourced development added, Clauses for confidentiality and data protection added in section 31, data masking clauses added in section 37.1
3	2.1	22/05/2023	Section 1.4 – Context regarding Godrej group added; clauses added for interested parties, section 3 – clauses added for monitoring and review of KPIs, section 16.1 – system lock duration updated, section 16.3- Password policy updated, section 36.1 – clauses for maintaining compliance to IT Act and CERT-In guidelines added

Policy Approval				
#	Name	Designation	Approval Date	Signature
1	Vijay Kumar Kannan	Head – Business Transformation and Digital IT, Godrej Consumer Products Limited	26/01/2023	DocuSigned by: Vijaykumar Kannan FCCE1DB6FF8E48C...
2	Sumit Mitra	Head – Group HR, Godrej Industries Limited and Associate Companies	01/02/2023	DocuSigned by: E54D014EAA7A4D9...
3	V Swaminathan	Head – Corporate Audit & Assurance, Godrej Industries Limited and Associate Companies	25/01/2023	DocuSigned by: 48B90E284B93436...
4	Divya Murthy	Head – Group & Corporate Legal, Godrej Industries Limited and Associate Companies	29/01/2023	DocuSigned by: Divya Murthy 3986F2F3395A48E...

Table of Contents

1. Introduction

Godrej Industries Limited and Associate Companies (GILAC) intends to follow process-based approach to design, implement, improve and maintain information security across all group companies. GILAC looks at information security as a strategic issue and has therefore set up a Group Chief Information Security Officer (CISO) role to be primarily responsible for implementing and monitoring the GILAC's information security policies & processes. This entails creation of a framework which will govern the entire information security aspect.

Information Security is the protection of Information and Information Assets, from a wide range of threats in order to safeguard business and profits. It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information Security Management System (ISMS) is an overall management system, based on a business risk approach, to establish implement, operate, monitor, review, maintain and improve information security. ISMS is a systematic approach to manage sensitive company information so that it remains secure. It encompasses People, Process and Technology.

It provides the following **benefits** to GILAC:

- Protects the GILAC's information assets
- Manages and minimizes risk exposure
- Enhances customer satisfaction that improves customer retention
- Builds a culture of security
- Keeps confidential information secure
- Allows secure exchange of information
- Ensures meeting legal obligations
- Provides consistency in the delivery of service or product

1.1. Five design principles for Security at GILAC

- Information Security is everyone's business
- Ensure all regulatory requirements are fulfilled – in compliance and in spirit
- Ensure Segregation of duties (e.g. design/ implementation v/s validate)
- Zero Trust in all aspects of Information Access
- Inculcate a strong Security mind-set

1.2. General Requirements of ISMS

People, process, and technology are critical to GILAC for the conduct of its operations. By establishing, documenting, implementing, monitoring, reviewing and maintaining ISMS, GILAC has greater confidence in its personnel. Also, the information security framework offers better assurance to its business partners and customers.

1.3. Scope of ISMS

Information Security Policy is applicable to:

- All employees, contractors, third-parties, outsourced partners and personnel associated with GILAC whether in India or out of India.
- All information Assets which include, but are not limited to: software assets, physical assets, paper assets, service assets, people assets and assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.
- Godrej Industries Limited and Associate Companies (GILAC) includes the following entities:
    - Godrej Industries Limited (GIL)
    - Ensemble Holdings and Finance Limited (EHFL)
    - Godrej Consumer Products Limited (GCPL)
    - Godrej Agrovet Limited (GAVL)
    - Godrej Tyson Food Limited (GTFL)
    - ASTEC Lifesciences Ltd (ASTEC)
    - Creamline Dairy Products Limited (CDPL)
    - Godrej Properties Limited (GPL)
    - Godrej Housing Finance Limited (GHFL)
    - Godrej Finance Limited (GFL)
    - Godrej Capital Limited (GCL)
    - Pyxis Holdings Limited (PHL)
    - Godrej Investment Adviser's Private Limited (GIAPL)

1.4. Context of the organization

GILAC are a group of companies within Godrej Group. GILAC has significant interests in consumer goods, real estate, agriculture, chemicals and financial services through its subsidiary and associate companies, across 18 countries. The combined market cap of GILAC's publicly listed entities is in excess of USD 15 billion. Ranked as the 2nd most trusted Indian brand, an annual revenue of USD 5 billion, and an estimated 1.1 billion customers across the world that use one or another Godrej product every day, the Godrej Group is amongst India's most diversified and trusted conglomerates.

GILAC intends to manage its internal and external issues that may affect the information security objectives of the Company. These issues include but are not limited to the following:

- Compromise in confidentiality, integrity and availability of information
- Non-compliance to legal, regulatory and contractual obligations
- Risks involved in online business
- Third party risks with respect to information security (i.e. Outsourced vendors, contractors, IT and cloud services, suppliers, etc.)

GILAC identifies all the relevant interested parties i.e. Senior Management, employees, vendors, contractors, service providers, suppliers, customers, legal and regulatory authorities, etc. through risk assessment exercise and also ensures that needs and expectations of these parties are also taken into consideration.

2. Policy

GILAC has documented an Information Security Policy (ISMS Policy, this document) that outlines all the information security objectives to be met by GILAC. The information security policy of GILAC addresses several domains including security at people, technology and process levels. Also, there are supporting process and procedure documents available for various aspects of information security.

The Information Security policy of GILAC shall be reviewed and updated at least annually or at major changes and communicated to all the users in the organization. In addition to the internal stakeholders, relevant sections of the ISMS Policy may be shared with external parties, on approval from CISO. The policy ensures that GILAC's information is protected and provides assurance to GILAC's customers and business partners.

The policy statement is as follows:

Information assets are important business assets to GILAC and needs to be appropriately protected in order to preserve trust and confidence of customers, Business partners and regulatory authorities in GILAC, ensure business continuity and maximize return on investments and business opportunities.

At GILAC, the management views information security as a critical business driver. Management understands the business risks associated with ineffective information security management. The management at GILAC is committed to the governance, implementation, systematic operation, maintenance and improvement of the Information Security Management System (ISMS). The management expressly supports the following activities associated with effective information security management:

- *Information Risk identification and their treatment to acceptable levels or risks*
- *Establishing information security policy and procedures.*
- *Compliance with statutory and regulatory requirements*
- *Establishing roles and responsibilities for critical activities associated with information security management.*
- *Providing sufficient resources to develop, implement, operate, and maintain the ISMS.*
- *Periodic review of Information Risk & ISMS and its management*
- *Conduct necessary programs for creating and increasing awareness about ISMS.*
- *Achieve global standards in Information Security Management.*

3. Objectives

The objectives of the GILAC Information Security policy are:

- To strengthen internal control and prevent threats to the GILAC's information, thereby ensuring the appropriate protection of information assets of GILAC through regular monitoring.

- To ensure the confidentiality, integrity and availability of information assets of GILAC through maintenance of asset registers and risk assessment.
- To continually strengthen and improve the overall capabilities of the Information Security Management System of the GILAC. This shall be assessed based security metrics designed for the organization and risk treatment methodology.

GILAC tracks the performance of its Information Security objectives and effectiveness of Information Security management system through defined Key Performance Indicators (KPIs). Also it reviews, monitors and reports the same to senior management on periodic basis and takes appropriate corrective action.

4. Consequence Management and Non-Compliance

- All violations of security policies, standards and/or guidelines are subject to disciplinary action. The specific disciplinary action depends upon the nature of the violation, the impact of the violation on informational assets and related facilities, etc. Violations will be handled as per the existing HR processes and could range from verbal reprimand, to termination of employment/contract and/or legal action.
- If a department or function is unable to comply with any requirements detailed within this policy, an exception shall be obtained. Such exceptions shall be documented and approved by the CISO or the Information Security Council indicating the rationale for the exception and the related risks.

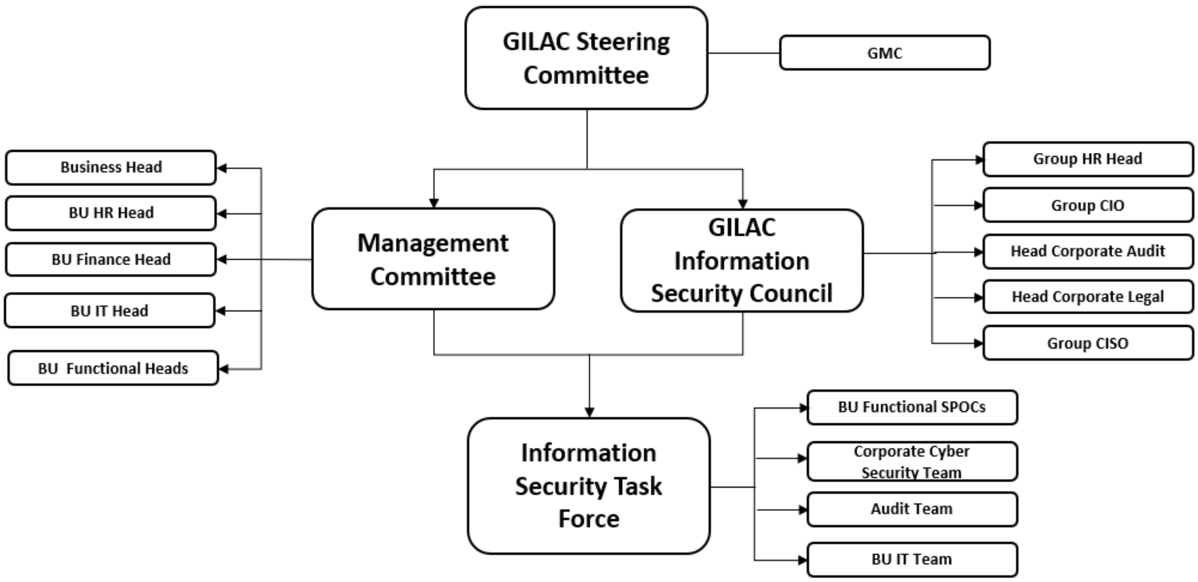
5. Leadership and Commitment

5.1 Security Organizational Structure

GILAC's top management demonstrates leadership and commitment with respect to Information Security Management. by delegating responsibilities to the Information Security Council. The organizational structure for Information Security comprises of four groups namely

- Steering Committee
- Management Committee
- GILAC Information Security Council
- Information Security Task Force

The organisation structure for Information Security is given as below:



GILAC Security
Organizational Structu

5.2 Roles & Responsibilities

<u>GILAC Steering Committee</u>

Steering Committee comprises of below core members:

- Global CIO
- GMC Members
- Corporate Audit Head

Steering Committee is responsible for discussing ongoing and new GILAC wide IT & Security initiatives, approval of these initiatives, approval of budget, approval and monitoring of projects, approval of changes to the organization structure and analyzing the IT & Security plans.

<u>GILAC Information Security Council</u>

Information Security Council is responsible for providing strategic inputs to the GILAC Steering Committee with regards to the Group wide IT and Security initiatives. It is also responsible for managing GILAC's cyber security posture by ensuring compliance to defined policies and procedures. The GILAC information Security Council comprises of:

- Group HR Head: - Ensure compliance to GILAC's policies and procedures by incorporating cyber security practices, and guidelines across the HR function.

- Corporate Audit Head: - Ensure the control objectives, controls, processes and procedures of GILAC Information Security Management System are in conform to the standard, effectively implemented, working as expected, and properly maintained.
- Group CISO: - Ensure compliance to GILAC's policies and procedures across all Business Units, ensure updating of Cyber Security policies and procedures according to changing threat landscape, facilitate Cyber Security awareness initiatives across GILAC and its customers, merchants and agents, managing the Group Security Operations Center
- Corporate IT Head: - Ensure compliance to GILAC's policies and procedures by incorporating cyber security practices, and guidelines in various stages of IT development, implementation, operation and retirement across the organization.
- Corporate Legal Head: - Ensure compliance to legal and regulatory requirements with respect to Information Security and IT across all Business Units, Advise on legal and contractual agreements with customers and third-party vendors.

<u>Management Committee (MC)</u>

Each BU (Business Unit) has its own 'Management committee' comprising of :

- BU Head
- BU HR Head
- BU Finance Head
- BU IT Head
- Other BU Functional Heads

Management Committee is responsible for:

- Ensure compliance to GILAC's policies and procedures by incorporating cyber security practices, and guidelines in various stages of IT development, implementation, operation and retirement across resp Business Unit.
- To oversee risk management framework to identify and deal with financial, model, operational, information security and cyber risks, and risks associated with the strategic direction, new products and change initiatives of the BU.
- The oversight of risk appetite and risk tolerance appropriate to each BU
- To review the BU's risk policies, risk reports and breaches of risk tolerances and policies
- To review the effectiveness of the BU's risk control/mitigation tools and risk management functions
- To monitor the effectiveness of controls across key risk types and controls to manage regulatory obligations and compliance risks across key functions

<u>Information Security Task Force</u>

Information Security Task Force is responsible for implementation of GILAC policies and procedures. The GILAC Information Security Task Force comprises of:

- BU SPOCs: - Responsible for implementation of GILAC policies and procedures by incorporating cyber security practices, and guidelines in various stages of IT development, implementation, operation and retirement across resp Business Units.

- BU HR: - Responsible for implementation of GILAC's policies and procedures by incorporating cyber security practices, and guidelines across the HR function.
- Cyber Security Team: - Development and ongoing maintenance of cyber security policies and procedures; Identify, access and monitor cyber security incidents; conduct cyber security related awareness campaigns across GILAC; Identification and mitigation of Cyber Security vulnerabilities.
- Audit Team: - Conduct internal audits and vendor/third-party assessments to ensure the control objectives, controls, processes and procedures of GILAC Information Security Management System are in conform to the standard, effectively implemented, working as expected, and properly maintained.
- IT Team: - Responsible for implementation of GILAC's policies and procedures across the entire GILAC IT infrastructure.

6. Contacts with relevant authorities

- The organization shall identify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.
- Contacts with authorities shall also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

7. Risk Management

- Risk assessment exercise shall be conducted at least **annually** to identify and evaluate various information security risks faced by GILAC and to prioritize the required controls based on the business impact and the likelihood of risk occurring.
- Respective BUs will be responsible for identifying risks, developing a plan, tracking and treating the risks for their resp assets.
- Business Head shall be responsible for signing off any identified risks that are accepted.
- Status of Identified risks and corresponding treatment plan shall be reviewed by the management committee on **annually**.

8. Training and Awareness

- Online training and awareness programs shall be conducted **annually** for all employees based on current Cyber Security Threat Landscape. Relevant records shall be maintained for reporting purpose.
- Mandatory online trainings shall be assigned to newly joined employees with respect to organizations polices, standards and guidelines. Trainings with respect to cyber security awareness shall also be mandated.
- Organization shall identify and assign role-based security trainings for roles that require specific knowledge and expertise as part of their day-to-day operations.

- Completion and attendance shall be mandated where required and possible consequences shall be defined for non-adherence by the respective BU HR Teams.
- An overall assessment of the employee's understanding where required shall be conducted at the end of an awareness, education, and training course to test knowledge transfer.

9. Documentation

- GILAC shall document all the information required by the standards, and requirements of its Information Security Policies which are necessary for the effectiveness of the information security management system.
- All supporting policies and procedures shall be reviewed **annually** and revision history shall be maintained.
- All the documented information of GILAC in paper or electronic form shall be created and updated appropriately with identifications and descriptions such as title, date, author, version no., change details and review frequency.
- All the documented information shall be available when needed. The distribution, access, retrieval, use and storage of information documents shall be properly maintained and monitored.

10. Internal audit

- **Annual** Internal Audits shall be carried out to provide information on whether ISMS conforms to GILAC's own requirements for its Information Security, the requirements of the standards and to evaluate effectiveness of the IT general controls. Corrective actions shall be taken in case of any non-conformity to the requirements.
- The effectiveness of the corrective action taken shall be reviewed and changes shall be made to the information security management system, if required.
- All the information documents related to the detection of non-conformity and rectifying shall be retained as evidence.
- The GILAC shall plan, establish, implement and maintain an audit program that takes into consideration the importance of the processes concerned and results of previous audits.
- The audit criteria and scope shall be defined. Such audits need to be performed as per the Internal Audit Plan approved by the Audit Head. Information Security Council can consider the internal audit findings and recommend the action plan to remediate the same.
- The Audit Head reports the findings and the remediation steps recommended to resp BU IT Heads and the Head of Corporate IT.

11. Management Review

Information Security Council shall review the Information Security posture of the GILAC periodically to assess adequacy and effectiveness of the information security policy. Members of this committee shall review the following:

- Information incidents
- Feedback on information security performance
- Information security gaps and risk assessments outputs
- Security improvement plan
- Status of corrective actions implemented

12. BYOD Security Policy

- Any GILAC Staff, intern who intends to access GILAC's infrastructure shall be allowed only Mobile/Tablet Devices. Any service provider and third-party contractor, who intends to access Godrej Corp IT's infrastructure shall be allowed only 1 mobile/tablet device.
- BYOD program does not support personal devices (mobiles/tablets) using customized, "rooted", or "jail broken" versions of operating systems. The device must have a licensed version of the Operating System installed.
- Users shall erase all information and software related to any previous employment, before using their device under this policy for the first time.
- In case, the device user is transferred, or retired / contract expired, or device is lost, the user shall notify IT team for de-registration of device and wiping off entire GILAC data stored on the mobile device (smart phones, tablets, etc.)
- IT Team shall at a minimum ensure that adequate security measures are implemented to ensure compliance to GILAC ISMS Policy.
- Access to the GILAC's network and business applications shall be restricted to only approved devices that meet a predetermined minimum-security configuration.
- Users are advised to keep their personal data separate from business data on their personally owned device in separate directories to reduce the possibility of disclosure.
- Organization shall have the right to seize and forensically examine any personally owned device believed to contain, or to have contained, GILAC's data where necessary for investigatory or control purposes.
- GILAC IT team shall have the right to enforce technical security controls such as access control, malware protection software and encryption.
- By acceptance of the BYOD policy, employees agree to disclosure and/or monitoring of device internet usage.
- Users of employee-owned devices shall be subject to a comprehensive and targeted security awareness campaign so that they clearly understand and can comply with the acceptable use policy.
- Users (GILAC Staff, interns, service providers and third-party contractors etc.) at a minimum shall ensure that they:
    1. Operate the device in compliance with Information Security Policy.
    2. Users shall obtain written approval from their respective Supervisor/ Head of the department to access confidential or classified information using external devices.

3. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
4. Immediately contact GILAC IT Team and their immediate Supervisor/ Head of the department if the mobile device is lost, stolen, damaged, destroyed, compromised, or non-functional.

- Control wireless network and service connectivity: Wi-Fi connectivity shall be turned off when not in use, and users shall only connect their devices to trusted networks. Devices shall be set to prompt users before connecting to networks so that users aren't unknowingly connecting to unsafe networks.
- Never store confidential data on a device: Users shall avoid saving any sensitive data like password, personal, financial data on their devices. This precaution ensures that confidential data is safe even if a device gets compromised.
- Employees shall not install freely available mobile applications from unauthorized sites which may collect data on the device.
- Employee shall never access or use GILAC systems or company data through a device in a way that breaches any of other GILAC policies.
- On last working day of an employee, all company data (including work emails), and any software applications provided for business purpose, shall be removed from the device. If this cannot be achieved remotely, the device must be submitted to IT Department for wiping and software removal.

13. Acceptable Use Policy

Refer 'Information Systems Acceptable Use Policy'

14. Human Resource Security

14.1. During Recruitment

- HR Team shall be responsible for performing background verification checks prior to recruitment of employees or engagement of staff on contract basis.
- Information security responsibilities for all staff and third-party personnel shall be specified in terms and conditions of employment.
- All staff and third-party personnel shall sign the Code of Conduct at the time of joining.
- The contractual agreements with employees and contractors shall state their and GILAC's responsibilities for information security. Terms and conditions of employment shall:
    1. state that information security responsibilities extend outside normal working hours and premises and continue after employment has ended.
    2. explain the employee's legal responsibilities and rights
    3. include a non-disclosure / confidentiality clause

14.2. During Employment

- All staff and third-party personnel shall agree to perform their security responsibilities and comply with the requirements specified in the security policies.
- All staff and third-party personnel shall be responsible for protection of any sensitive information and assets assigned to them.
- All staff and third-party personnel shall use information processing systems and data residing on systems for authorized business purposes only.
- All staff and third-party personnel shall report any suspected information security incident or weaknesses to his/her reporting manager and Cyber Security team.
- The Cyber Security team shall ensure relevant cyber security awareness education and training (upon hire as part of induction and subsequently periodic) for all staff of GILAC and where relevant, third-party personnel.
- The Cyber Security team shall monitor, review and measure the effectiveness of cyber security awareness through internal compliance and awareness tests.
- The Business IT Head shall report all information security breaches committed by any employee to the HR head for taking necessary disciplinary actions against them.

14.3. Termination and Change of employment

- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
- All physical and logical access privileges shall be revoked immediately when an authorized user no longer requires access to information or systems as part of their job, or when they leave GILAC. In case access needs to be retained, the same shall be approved by the HR team and resp BU SPOC.
- In the case of a contractor provided through an external party, the termination process is undertaken by the external party in accordance with the contract between the organization and the external party.
- Upon termination of employment/contract/agreement, internal staff and third-party personnel shall:
    1. Return Assets that belong to GILAC
    2. Confirm that they have destroyed all copies of information owned by GILAC.
- The activities performed by a staff / third party may be subject to additional monitoring at the time of termination or change of employment, on communication from respective Business representative (BU Head or BU SPOC). The department representative shall assume ownership and responsibility for monitoring related activities in co-ordination with IT.

15. Asset Management Policy

There shall be documented standards and procedures for managing the asset lifecycle.

15.1. Ownership of Information Assets

- All Information assets (hardware and software) shall be identified and have an asset owner.
- An asset custodian shall oversee and implement necessary safeguards to protect the assets per the classification level defined by the asset owner.
- Asset reconciliation and verification shall be performed on **bi-annual** basis.

15.2. Asset Register

- Business heads or Business SPOCs shall develop and maintain an asset register containing all assets within their business function.
- The asset register shall contain at a minimum, the asset type, asset location, owner, custodians and name of the function/processes that use those assets.
- The asset register shall also maintain the CIA rating for all assets and accordingly label them as per the Asset Classification Scheme. (Refer Asset Management procedure for asset classification categories).
- Asset rating shall be reviewed on periodically as part of **annual** Risk Assessment exercise.

15.3. Information Classification and Handling

- The Information Classification scheme shall be used to define an appropriate level of protection or special handling required for an information asset.
- The level of protection shall be commensurate with the classification level of the data.
- The classification of the information shall be consistent with the business value of the data.
- Information shall be classified using GILAC's Information Classification Scheme as tabulated below:

Information Classification Guidelines

Classification Category	Category Description
CONFIDENTIAL	This classification applies to the most critical business information assets, which are intended strictly for use within GILAC for limited authorized users. Its unauthorized disclosure could adversely impact its business, its shareholders, its business partners and/ or its customers, leading to legal and financial repercussions and adverse public opinion.
RESTRICTED	This classification applies to any sensitive business information assets, which are intended for use within GILAC for some of the authorized users. Its unauthorized disclosure could adversely impact its business, its shareholders, its business partners, its employees and/or its customers
INTERNAL	This classification applies to information assets that are specifically meant for all employees of GILAC. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact the business, employees, customers, stockholders and/ or business partners.

PUBLIC	This classification applies to information assets, which has been explicitly approved by the management for release to the public.

Electronic Information Handling Guidelines

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
Creation/ Obtainment of Information	Shall be labelled at the time of creation/obtainment	Shall be labelled at the time of creation/ obtainment	Shall be labelled at the time of creation/ obtainment	Shall be labelled at the time of creation/ obtainment
Storage on static media	Shall be protected by password	Shall be protected by password	No Special requirements	No Special requirements
Storage on removable media	Shall be protected by password	Shall be protected by password	No Special requirements	No Special requirements
Printing and duplication	Printing permitted with explicit business need and approval from Business owner and infosec teams.	Printing permitted with explicit business need and approval from department head.	Printing permitted	No Special requirements
Read/Update/ Delete access to information	Shall be restricted to Information owners, relevant authority of groups	Shall be restricted to Information owners, relevant authority of groups	Access to delete/update information shall be restricted to authorized individuals, relevant authority or groups. Read access shall be provided to all users within the company	Access to delete/update information shall be restricted to authorized individuals. No special requirements for read access
Transmission to internal email ID	Encryption or password protection is required as mandated by the Information Owner	Encryption or password protection is required as mandated by the Information Owner	No special requirements	No special requirements
Transmission to external email ID	Shall not be emailed unless authorized by Information owner.	Shall not be emailed unless authorized by Information owner	Shall not be emailed unless authorized by Information owner	No special requirements

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
	Encryption or password protection is mandatory. While sending such data outside, reporting manager should be kept in Cc	Encryption or password protection is recommended		
Disposal of Information	Shall be degaussed and destroyed if media is not to be reused in future	Shall be deleted from the media	Shall be deleted from the media	No special requirements

Paper Information Handling Guidelines

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
Creation/ Obtainment of Information	Shall be labelled mandatorily at the time of creation/obtainment	Shall be labelled mandatorily at the time of creation/obtainment	No Special requirements	No Special requirements
Storage and Access	Shall be stored in appropriate location with restricted access Shall not be available to personnel without prior authorization from information owner	Shall be stored in appropriate location with restricted access Shall not be available to personnel without prior authorization from information owner	No Special requirements	Shall be available widely for public No Special requirements for storage
Duplication	Shall not be copied/scanned without permission from information owner Unattended coping/scanning should not be done	Unattended coping/scanning should not be done	Unattended coping/scanning should not be done	No Special requirements
Mailing	Mailing allowed as per permission of relevant authority or	Mailing allowed as per permission of relevant authority or	Mailing allowed as per permission of relevant	No special requirements

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
	information owner only Classification marking shall be visible on the envelope.	information owner only Classification marking shall be visible on the envelope.	authority or information owner only Inter-office mailing of documents is permitted	
Disposal of Information	Shall be shredded	Shall be shredded	Shall be shredded	No special requirements

15.4. Asset Retention and Disposal

- Information owners shall define types of records and their retention requirements.
- Records which are no longer active shall be archived for a period of time as set forth in the GILAC Data Retention Schedule.
- Information shall be disposed when no longer needed subject to its retention schedule and approval by asset owner.
- Hardware assets and electronic records shall be disposed in a secure manner in accordance with the Asset Disposal guidelines.
- All assets destroyed in compliance with this policy shall require 'e-waste certificate' to be retained as per defined policy.
- Prior to disposal of system devices like Hard Drives, RAMs, etc., the same shall be sanitized by use of techniques like degaussing, low-level formatting, or physical destruction to ensure that data cannot be reconstructed.

15.5. Media Handling

- All media containing sensitive data shall be stored in a secure safe, which shall be fire resistant and free of toxic chemicals.
- Access to media library and media safe shall be restricted to authorized persons only.
- Prior to disposal of removable media, all data shall be securely deleted, or the media shall be destroyed.
- All incoming/outgoing media transfers shall be authorized and shall be checked against a gate pass.
- Removable media shall be scanned for malware/anti-virus prior to providing read/write access.

16. Access Control Policy

16.1. User Access Management

- A formal user registration and de-registration process shall be implemented to create user IDs and assign access privileges.
- A unique ID shall be assigned to each user of information system to hold them responsible for their actions. User Ids shall follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions shall cover all end users, contractors, consultants and vendors.
- A single user shall not be assigned more than one user ID on the same information system.
- The administrator of Information systems shall not grant a user, access to any system without the authorization of the user's supervisor or manager.
- The supervisors 0r managers shall revoke access rights of users in a timely manner who have either changed their job function or have been terminated.
- Generic user IDs where necessarily required as an exception shall be assigned to a nominated user post approval from the respective Business Head or Business SPOC. The nominated user along with the Business head shall maintain the accountability, by whom, when and for what the generic ID is used.
- All vendor supplied default user IDs shall be disabled or removed where possible.
- GILAC systems to be scanned to identify orphan IDs, dormant IDs, unauthorized IDs, etc. on a periodically as part of **quarterly** ID validation process. Same need to be deleted if not required. Exception to be raised for IDs which need to be retained with proper business justification.
- Access to information and information technology resources shall be controlled, monitored, and authorized based upon user's job function, need-to-know and need-to-perform criteria.
- The access to specific functionalities in information systems and level of access required at the granular level of read, modify & update, deletion shall be identified and documented. These requirements shall be translated into system profiles for the different classes of business users.
- Access privileges shall be assigned to a unique user ID that is mapped to an employee/Contractor based on individual's subscribed role, business need and security requirements.
- Role based access shall be provided based on the systems profiles defined by the system and business owners.
- The use of Group and shared IDs shall be restricted and if it is absolutely required to use shared IDs, mechanisms shall be established to ensure traceability/audit trails of usage to individual users.
- Request for change in the access right shall be documented and approved by the user's Manager or the respective Business SPOC.
- Audit trails for all requests for additions, modifications or deletions of individual accounts and access rights shall be maintained.
- Access rights shall be defined based on the least privilege principle and be approved by user's Manager or the respective BU SPOC.
- The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

- User access shall be reviewed and access shall be disabled if the account is found to be inactive for a period of Ninety (90) days or more. If the same cannot be disabled, exception shall be taken from the CISO or the Information Security Council and same shall be maintained.
- IT Operations shall enable user account lockout after five (5) unsuccessful attempts to logon to the system.
- Users shall be required to re-authenticate themselves after a specific period of inactivity.
- System lock duration shall be set to a maximum period of 5 minutes in case of system inactivity.
- Access review for critical applications shall be done on **quarterly** basis.

16.2. Privilege Access Management

- Privileged users must be authenticated using either two-step or two-factor authentication, wherever applicable. A quality password is required along with additional authentication such as biometric, tokens, OTP, authenticator, etc.
- The BU Head or BU SPOC shall approve the granting, modifications, and revocation of privilege accounts on respective information systems owned by that business unit.
- Documented approvals shall be appropriately stored and produced by BU SPOCs when requested for their resp BU assets.
- Privileges shall be assigned to user's identity.
- The use of privilege accounts such as root or administrator shall be discouraged.
- Controls to monitor and track activity of privilege accounts shall be implemented.
- The activity logs of privilege users have to be stored in remote systems to prevent tampering of these logs.
- Privileged access rights shall be reviewed **monthly.**
- When a privilege is granted on a temporary basis to a user, privileges shall be revoked after completion of that period.
- Changes to privileged accounts shall be logged.

16.3. Authentication Information Management

- Authentication information such as passwords or personal identification numbers (PINs) generated automatically shall be non-guessable and unique.
- The identity of a user shall be verified prior to providing a new or temporary authentication information
- Authentication information, including temporary authentication information shall be transmitted to users in a secure manner (e.g. over an authenticated and protected channel) and the use of unprotected channels for this purpose shall be avoided.
- Randomly generated temporary passwords shall be provided to a new user initially and a password reset shall be enforced upon first login.
- Vendor default passwords shall be changed prior to use.
- Passwords shall be secured during transmission and storage.

- Authentication information such as passwords shall be kept confidential and shall be shared only with authorized persons basis proper justification and approvals.
- The password policy shall address the following at the minimum:
  i. Password length should be a minimum of eight (8) characters for end users and ten (10) characters for privileged accounts.
  ii. Passwords should be complex, consisting of any 3 out of 4 characters – lowercase, uppercase, numerals and special character
  iii. Users shall be forced to change the passwords after first logon.
  iv. Domain users shall be forced to change their passwords at least every 90 days. Passwords should automatically expire if not changed within 90 days. Expired passwords for end user accounts should result in a forced password change upon next sign in. Users should not use last 5 passwords (password history).
  v. Privileged account passwords must be changed at least once every 90 days. Privileged Account Passwords should automatically expire if not changed within 90 days. Expired passwords for Privileged Accounts should result in an account lockout.
  vi. Default system privileged accounts such as root and administrator accounts are configured with 'password never expire' and the password shall be vaulted.

16.4. User Responsibilities for Access Management

- Users, contractors, consultants, etc. shall keep their passwords confidential and shall not share with any other individual.
- Users, contractors, consultants, etc. shall protect and/or report all unattended equipment appropriately.

16.5. Network Access Control

- Appropriate interfaces shall be created to segregate GILAC network from the networks owned by other organization and public networks.
- Users shall only be provided with access to the services that they have been specifically authorized.
- Only authorized users shall be permitted to establish remote connections to the network using secure channels.
- An equipment identifier shall be used to authenticate all equipment connecting to the network.
- Users connecting to the network shall be authenticated and their access attempts shall be logged.
- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

- User sessions shall be disabled after 15 minutes of inactivity so as to limit the connection time to sensitive network.
- Vendor shall provide details of their employees who shall need access to GILAC network. Access shall be granted to only those vendor employees whose details have been provided to GILAC.

16.6. Application Access Control

- Logical access to the application software shall be restricted to authorized users.
- Access to application functionalities shall be restricted based on business requirements.
- User access (except administrators) to data repositories shall be approved and recorded.
- Application accounts created for inter-application access shall not be used by individual users.
- Application Owners shall be responsible for management of access rights to their respect applications.
- Application access for critical applications shall be reviewed on a **quarterly** basis.

16.7. Segregation of Duties

- Access profiles for critical applications shall be designed to avoid potential segregation of duties conflicts.
- SoD reviews to be conducted on **quarterly** basis to identify potential SoD conflicts.

16.8. Remote Access

- Remote access shall not be provided to employees/vendors/contractors by default. Remote access to network shall require an appropriate management approval and a valid business need.
- Remote access request for third party vendor/consultant shall be raised by the GILAC employee responsible for the vendor /consultant engagement along with proper business justification. The request needs to be approved by BU SPOC and Cyber Security Manager.
- Remote user sessions shall be terminated after a maximum period of 15 minutes of inactivity.
- Unauthorized inbound and outbound connections to and from GILAC network shall be prohibited.
- Remote access to the network shall utilize approved VPN (Virtual Private Network) infrastructure and multi-factor authentication.
- All remote access to an internal network, whether through VPN, or other mechanism, shall be logged.

16.9. Access to third Party Users

- The designated manager within GILAC shall authorize and supervise access requirements for non-employees.
- Basic information Security principles such as least privilege, Separation of duties and defense in depth shall be applied.

17. Physical & Environmental Security Policy

17.1. Physical Security

- Physical access to offices and information processing facilities shall be properly controlled for employees, contractors and visitors to prevent unauthorized access or damage to information systems.
- Physical access provided to secure areas such as the Data Centers, Network room, Server rooms, Disaster recovery sites etc. to employees/vendors/visitors shall be reviewed on **quarterly** basis.
- Entry and exit to the premises shall be logged and monitored. In case of any major deviations/ suspected events noted, the same shall be notified to appropriate authorities.
- Facilities shall be classified into zones and physical safeguards for each zone shall be designed and implemented at a level appropriate to the classification of the zone.
- Appropriate physical security controls and monitoring capabilities shall be employed to detect and prevent disruptions to the information processing facilities.
- Offices and information processing facilities shall be manned reception area to control physical access to resp premises.
- CCTV cameras shall be installed at key locations of premises. Ensure that due diligence is exhibited during CCTV monitoring. CCTV recordings shall be retained for least for 1 month for Primary datacenter. For GodrejOne, recordings shall be retained at least for 10 days.
- Visitor details shall be verified and entered into a visitor register/ visitor management system. Details regarding laptops, pen drives, CDs/ DVDs, floppies etc. shall be entered.
- Every visitor shall be provided with a visitor badge and the visitor shall display the badge at all times in the GILAC premises.
- Access cards provided to vendors/consultants shall have limited floor access. Cards unused for more than 30 days shall be disabled.
- Visitor/Vendor personnel/third party personnel shall be escorted at all times inside the Datacenter or facilities housing critical information systems or equipment.
- All employees and visitors shall display the access card at all times on premises. Also, all employees and visitors shall use their access cards (employee identification badges, visitor badges etc.) to obtain entry and exit to the premises.
- Monitoring events and records for physical access (eg. access cards, biometric access, etc.) shall be stored for a minimum of three months or longer based on business and legal requirements.

17.2. Equipment Security

- Equipment shall be secured from potential threats to prevent loss, damage, theft or compromise.
- All cables, including power and telecommunication network cables shall be protected from damage or unauthorized interception.

- IT/ Network function shall ensure that any networking equipment, gateways, Wireless access points, telecommunication lines and cabling racks/ distribution points in the office area are not physically accessible to people other than IT/ Technical function.
- It shall be ensured that all areas, where loading and unloading of items are done, are monitored.
- Security personnel shall maintain an inward and outward register for all the incoming and outgoing materials.
- Delivery and loading areas shall be isolated and kept away from information resources. Delivery or loading shall not be permissible in restricted areas.
- All incoming IT equipment shall be inspected for hazardous and combustible materials at entry point to ensure the same is not allowed inside the premises.

17.3. Environmental Security

- Air-conditioning systems shall be installed to support information systems and equipment like server rooms, network rooms, and disaster recovery sites.
- Smoke detectors, fire detection and fire suppression equipment shall be installed in office premises and other sensitive areas for protection against any fire incidents.
- Necessary fire drills and trainings shall be conducted for all employees on a periodic basis in case of any emergency. Emergency evacuation drills shall also be conducted to ensure emergency evacuation.
- Appropriate temperature and humidity controls shall be implemented, monitored and maintained.
- Uninterruptible power supply (UPS) systems and generators shall be installed to support controlled shutdown or continued functioning of equipment supporting critical business operations
- Appropriate water/ moisture sensors shall be installed to detect water leakage and seepage
- Critical information systems, storage media, document and assets shall not be located in areas susceptible to water seepage or flooding, or near combustible materials.
- A preventive maintenance exercise for the utility equipment (electrical equipment, fire equipment, AC, UPS, water leakage detectors, etc.) including alarm systems is carried out at scheduled intervals ensuring their continued availability and integrity.

18. Change Management Policy

- A Change Advisory Board (CAB) shall be formed for approving and tracking critical changes.
- A change management process shall be documented and established that shall at least include types of changes, recording of changes, business and security approvals, impact assessment due to the change, testing the change, roll back procedures and post implementation review of changes.
- Changes to system components shall be adequately controlled and shall be carried out only after changes are validated, documented and approved by authorized individuals.

- The potential business impacts of changes shall be assessed (for e.g., in terms of the overall risk and impact on other components of the application)
- Changes shall be reviewed to ensure that they do not compromise security controls (e.g., by checking software to ensure it does not contain malicious code, such as a Trojan horse or a virus)
- Back-out positions shall be established so that the system or application can recover from failed changes or unexpected results
- Changes to the system or application shall be performed by skilled and competent individuals who are capable of making changes correctly and securely.
- Changes shall not be carried out directly in the production environment unless required during contingency (for emergency changes) with prior authorization.
- Any deviations from the implementation plan shall be recorded and approved by the Change Manager and informed to CAB.
- Status of Changes (e.g., successful, failed, cancelled, etc.) post activity shall be recorded and communicated to the change manager or change management team.
- The change manager or change management team shall ensure that status of all changes is informed and updated by resp activity SPOCs within the required timeframe.
- Record of changes shall be maintained for at least a period of 1 year.

19. Security Incident Management Policy

- Processes shall be implemented and documented to manage information security incidents including but not limited to incident detection, reporting, ownership, classification, investigation, resolution and closure.
- A formal incident management process shall be documented for timely detection, reporting and management of information security incidents within the organization’s computing environment.
- Security incidents shall be reported from all relevant sources, including users, audit process, SOC, advisory team, customers, etc.
- Escalation and communication processes and lines of authority shall be established
- All reported security events shall be analyzed before being classified as security incidents. Based on the learning from the incident, Cyber Security Team shall make necessary changes (if required) to security policies.
- The Cyber Security Team shall conduct periodic sessions to make staff and third-party personnel aware of the procedures for identifying different types of security events.
- All information security incidents shall be recorded in a log or equivalent (e.g. using an automated information security incident management system) and categorized according to their severity and type. GILAC shall classify incident based on incident classification criteria outlined in Security Incident Management Procedure.
- For critical incidents that need communication to be sent out to employees or customers should be done as soon possible.
- All reported security incidents shall be responded and resolved timely, and if not, then escalated as per the classification of security incidents.

- Cyber Security Team shall verify all reported security incidents for closure and conduct post-incident analysis by reviewing the appropriateness of actions taken for closure.
- Cyber Security Team shall investigate the cause of all reported security incidents. Wherever required, they shall also verify the implementation of recovery solutions.
- Cyber Security Team shall maintain a knowledge base of all security incidents and the identified solutions. This will help in providing quicker solution if the same or similar incident happens again.
- Cyber Security Team shall collect significant evidence for conducting necessary investigation. The events and logs shall be retained for a period as required by legal, regulatory or other compliance obligations.
- Cyber Security Team shall conduct post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future.
- Cyber Security Team shall perform Forensic investigations for incidents requiring investigation for legal purposes and /or severe information security incidents.
- All security incidents and breaches shall be discussed with management on **quarterly** basis.

20. Data Backup, Retention and Disposal Policy

- Information owners shall determine the backup and recovery requirements based on the criticality of information systems to prevent operational disruptions or data loss.
- Backup media shall be stored in a secure location in a off-site facility such as an alternate or backup site.
- Data recovery processes shall be tested for effectiveness on **annual** basis.
- Data backup shall be encrypted.
- IT operations team shall identify and establish appropriate processes to meet the backup and recovery requirements determined by information owners.
- Data retention period shall be defined and records shall be retained for the defined period. This shall be reviewed at least once in a year and updated with changes if any. Retention periods for data shall be decided based on the following,
    1. GILAC's business requirements,
    2. Legal or regulatory compliances,
    3. Contractual obligations.
- Records shall be maintained in a safe and secure environment. Records shall be protected from unauthorized access.
- All waste copies of sensitive information that are generated while copying, printing, or faxing shall be shredded using paper shredders/incinerators or shall be placed in locked bins clearly marked as containing confidential data.
- Storage media like floppy disk, hard drives, CDs, tape or optical media, zip disks, etc. shall be erased using a degaussing device or "disk-wiping" software before being discarded.

- If the data cannot be erased, then Media shall be physically destroyed prior to disposal in such a manner that data should be beyond retrieval.
- Non-disclosure agreement shall be signed between the Organization and external contractor for outsourcing disposal. Certificates of secure disposal shall be obtained from external contractor.

21. Data Security Policy

- GILAC shall implement mechanisms to prevent the accidental disclosure of email and attachments to unauthorized individuals by enforcing encryption between email servers (e.g. using Transport Layer Security (TLS) or equivalent).
- Email servers shall protect messages by using digital signatures to identify if email messages have been modified in transit.
- Users shall be educated in how to protect the confidentiality and integrity of email messages (e.g. by the use of encryption, digital certificates and digital signatures).
- Data Security solution (e.g. DLP, IRM, etc.) should be used to identify specific types of sensitive information, monitor channels of data leakage (vectors) and take actions to prevent this data from leaking.
- Data Security solution should be configured to monitor and control the flow of sensitive data using technical Data Security solution policies, defining:
    1. what data can and cannot be sent, posted, uploaded, moved or copied and pasted.
    2. where data can be transmitted.
    3. who can send and receive data (e.g. via email).
    4. how data can be shared.
- Data Security solution should be configured to include a register of keywords, electronic document characteristics and the specific types of sensitive information (sometimes referred to as pre-registration) that need to be protected from unauthorized disclosure.
- Data Security solution should be configured to detect sensitive data by using
    1. described content matching, which checks data against regular expressions, defined strings, keywords, patterns or dictionaries (a list of specific terms, keywords or key phrases);
    2. fingerprinting (indexing), which takes a cryptographic hash of a sample file or file contents to create a 'fingerprint', checking content against this fingerprint for complete or partial matches (i.e. to detect either the complete text or excerpts that match the sample document)
    3. machine learning, which uses algorithms and statistical techniques to determine if content is similar to test data, used to train the machine learning algorithm, used by the Data Security solution
    4. optional character recognition (image recognition), which analyses image files (e.g. screenshots or scanned documents) and extracts text to find matches for sensitive content.

- Data Security solution should be configured to monitor data leakage channels where sensitive data is in motion (e.g. data traversing a network such as the internet or private network), in use (e.g. data processed on endpoint devices) or at rest (e.g. data stored in file systems, databases, the cloud or endpoint devices)
- Backups should be encrypted to protect sensitive information, when:
    1. transmitted via a network to external storage facilities, particularly when engaging with a third party to support backup capabilities
    2. stored on physical media, to prevent unauthorized access in the event backups are lost or stolen in transit to an alternative location, such as an off-site storage facility
- Data processed by cloud services should be protected, which includes encrypting sensitive data by using the CSP default encryption solution, configuring customer-managed key encryption or implementing customer-supplied key encryption.
- USB shall be blocked for all end-users. In case of any deviation, policy change shall be pre-approved by the respective Business heads.
- Sensitive information shall not be kept for longer than it is required to reduce the risk of undesirable disclosure.
- Information shall be deleted from systems, applications, and services in accordance with business requirements and taking into consideration relevant laws and regulations.
- When using service suppliers for information deletion, evidence of information deletion shall be obtained from them.

22. Capacity Management Policy

- Systems capacity shall be monitored. Capacity monitoring data shall be analyzed to identify the trends and discrepancies on a regular basis, especially for critical systems.
- New business and system requirements, as well as the current and future trends for information systems usage shall be used to develop future projections for capacity requirements.
- GILAC shall identify the required actionable for capacity management to ensure effective performance of information systems and business processes. The action plan shall identify and consider the capacity requirements based on business criticality of the concerned systems, business requirements, Service Level Agreements, Memorandums of Understanding, and risk assessments.

23. System Acquisition, Development, Planning and Maintenance Policy

- GILAC shall ensure that cybersecurity requirements are included in the entire lifecycle of information systems & applications, whether acquired or developed, and integrated as early as possible.
- Security engineering principles should be established, documented and applied to information system engineering activities. Security should be designed into all architecture layers.

- The Cybersecurity function shall perform activities such as vulnerability assessments, configurations' review, for newly developed/acquired systems/applications. All findings shall be mitigated before going live in production environment.
- The Application team shall perform activities such as secure configuration, hardening and patching of new applications prior to go live.
- GILAC shall ensure that the development of new applications or updates to existing applications incorporate secure coding standards.
- Source code should be protected against unauthorized access and tampering. Access to source code should be restricted only to authorized personnel. Changes to source code should be recorded to maintain an audit trail.
- GILAC change management process shall be followed when attempting to perform system maintenance and updates.
- All Vendor and third-party contracts shall include the cybersecurity requirements for any product/system procurement.
- In case of outsourced system development, the organization shall communicate and agree requirements and expectations regarding licensing agreements, code ownership, secure design, secure coding standards, testing practices, etc. and continually monitor and review whether the delivery of outsourced work meets these expectations.
- Operational information used for testing purposes shall be appropriately protected.
- Same access control procedures shall be applied to test environments as those applied to operational environments.
- Usage of operational information shall be recorded to maintain an audit trail.
- Operational information shall be properly deleted from a test environment immediately after the testing is complete to prevent unauthorized use of test information.

24. Network Security Policy

- GILAC shall develop and approve baseline security standards for network devices.
- Firewall configurations and rules shall be reviewed periodically, and at least **quarterly** for sensitive systems.
- GILAC shall provide the necessary protection when browsing and connecting to the Internet, and restrict access to suspicious websites, file storage sharing sites, and remote access sites.
- Managing the access rights of third parties to the network shall be in accordance with the GILAC Access Management Policy.
- Strong authentication and encryption techniques shall be used to ensure the protection of wireless networks.
- Firewalls, Intrusion Prevention Systems (IPS), and DNS Security technologies shall be in place and updated periodically for proper logical and physical segmentation between internal corporate network and between external networks.
- GILAC shall apply network segregation between production environment and test & development environments.

- The use of physical network ports in all GILAC facilities shall be restricted by using Port Security or Port-Based Authentication technology to protect the network from the possibility of connecting unauthorized or suspicious devices without being revealed.
- GILAC shall restrict direct connection to the internet.

25. Secure Baseline & Vulnerability Management

- Secure Baseline standards shall be defined for all system components (endpoints/workstations, network devices, operating systems, databases, applications and other systems which require secure baseline) and shall be implemented across all systems.
- Applications and IT infrastructure shall be subject to periodic technical assessments like Application Security Review, Vulnerability Assessments and Penetration Testing.
- Cyber Security Team shall conduct periodic vulnerability scans as per defined cycle and share report with system owners for closure of findings.
- The vulnerabilities detected shall be remediated promptly so as to avoid exploitation of such vulnerabilities.
- Penetration testing of public facing systems as well as other critical applications shall be carried out by professionally qualified teams.

26. Security Patch Management Policy

- Security operations team, Server team, Network Administrators, Database administrators and Application administrators are responsible for identification and validation of all patch related issues concerning their domain of work.
- System owners shall be responsible for deployment of patches.
- Application and System owners shall ensure that all patches applicable to applications and systems used by GILAC are identified.
- Patches shall be tested in a test environment before being applied to production systems.
- Security Patch Management Process shall be followed to prioritize patches.
- IT Infrastructure team shall establish methods to protect information and systems if no patch is available for an identified vulnerability, for example, disabling services and adding additional access controls.
- Delay in security patch deployment shall be tracked.
- New devices shall be patched to the current patch level, as defined by the operating system vendor and supported by the application, prior to the device being connected to the production network.
- IT infrastructure team shall submit the patch management report on periodic basis to the respective Business Units.
- Respective system owners shall be responsible for patching of their systems.
- The Cyber Security Team shall track all security patch implementations using the patch dashboard or patch status report. This is to ensure that all patches are installed on all system and also to keep a track of patches which are not installed.

27. Audit Logging and Monitoring Policy

- Security logging, monitoring and reporting capabilities shall be implemented to detect security events within GILAC's network and information assets in accordance with applicable laws, regulations and industry standards.
- Logs of all critical servers, network devices and system components that support security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, etc.) shall be stored, reviewed and monitored to detect malicious activities.
- Critical Business applications and technical infrastructure shall be configured to enable event logging (standard format/syslog or equivalent).
- Critical Business applications and technical infrastructure shall generate appropriate event types (e.g. Object creation, login attempts etc.)
- The logs generated shall have relevant event attributes in event entries (e.g. IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name, etc.)
- All systems shall use a trusted source for date and time to ensure logs use accurate time stamps. The trusted time source shall be synched with global atomic clocks for accurate timing.
- Critical servers and network devices shall be configured to log / alert creation and deletion of system-level objects.
- Critical servers and network devices shall be configured to log / alert initialization, stopping or pausing of the audit logs.
- Security relevant logging shall be enabled at all times.
- Logs shall be protected against unauthorized access, misuse and modification. Sufficient storage space shall be allocated based on expected volume of logs.
- Security-related event logs shall be analyzed regularly to help identify anomalies. Anomalies detected shall generate alerts in SIEM (Security information and event management) tool. Various use-cases to be defined in SIEM to detect security events covering all possible threat landscapes.
- Security Operations Center (SOC) team shall monitor security alerts generated in the SIEM tool 24x7. Any incident identified or reported shall be handled as per Incident Management process.
- Information relating to information security threats shall be collected and analyzed to produce threat intelligence.
- User accounts shall be monitored regularly to detect any unwanted privileges, orphan accounts, and dormant accounts. Any accounts detected in violation of GILAC's policies shall be suspended or terminated.
- The logging of security-related events should be reviewed on **quarterly** basis to verify whether alerts are getting triggered in SIEM as per configured use-case.
- Audit logs shall be retained for at least one year and shall be readily available for last 3 months.
- The organization shall also subscribe and connect with special interest groups or other specialist security forums and professional associations with the aim to improve knowledge about best practices, receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities and stay up to date with relevant security information.

28. Network Time Protocol

- The real time clock of systems shall be set accurately to ensure the accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases.
- The real time clock of systems and communication devices shall be in sync with central NTP server. Further there shall be procedure that checks and corrects drift in the real time clock.

29. Anti-Virus Policy

- All servers, desktops and laptops shall have anti-virus agent installed. Infrastructure Team shall ensure that all new systems including desktops, laptops, and servers have anti-virus agent installed, pre-loaded and configured before provisioning.
- Anti-virus agent installation shall be password protected to ensure that end users cannot uninstall the agent. The anti-virus agent shall be configured in such a way that end users will not have privileges to change any settings or to disable the agent.
- Anti-virus agent shall be configured to scan the machine at least once every week. The scanning can be scheduled during non-peak usage hours.
- Anti-virus agent shall be configured to scan all removable disks before use.
- Anti-virus agent shall be configured to quarantine virus infected files if they cannot be cleaned.
- Access to websites and other resources on the internet known to host malicious content shall be prevented using the web content filtering tool. Antivirus software shall be installed on the Internet Proxy and if feasible configured to scan downloads/uploads for malicious code.
- GILAC shall employ anti-malware signature auto update features. After applying an update, automated systems shall verify that each system has received its signature update. The GILAC shall monitor anti-virus console logs to correct any systems that failed to be updated.
- Infrastructure team shall submit **monthly** reports on the status of the Anti-Virus protection to the Cyber Security Team.
- For external users (including consultants, vendors, customers, and service providers) who bring laptops/desktops into the Organization's premises, GILAC shall ensure the devices are scanned for viruses or compensating controls are in place to prevent the spread of viruses before allowing these devices access to GILAC network.
- Provisions shall be made for real-time triggering and monitoring of alerts related to virus/malware detection and necessary actions shall be taken to remediate the same.

30. Email Security Policy

- GILAC shall implement technologies to protect e-mail by analyzing and filtering e-mail messages, and block suspicious messages such as spam and phishing emails.
- Access to e-mail messages shall be restricted to GILAC employees, consultants & contractors only.
- GILAC shall ensure that email systems are only accessed by individual users via their user IDs.
- All emails sent from organization addresses to recipients outside of the organization shall carry the following disclaimer in English: **"DISCLAIMER: The information in this message is**

confidential and may be legally privileged. It is intended solely for the addressee. Access to this message by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, or distribution of the message, or any action or omission taken by you in reliance on it, is prohibited and may be unlawful. please immediately contact the sender if you have received this message in error.
GODREJ INDUSTRIES LIMITED AND ASSOCIATED COMPANIES".

- GILAC shall prohibit the System Administrator to access the e-mail contents of any employee without prior permission.
- GILAC shall ensure that GILAC's email is only used for business purposes.
- Multi-Factor Authentication shall be required to access the email service remotely or through a Webmail page.
- GILAC emails that contain classified information shall be encrypted.
- GILAC shall archive the emails and perform backups periodically and according to business requirements.
- Limits shall be defined for email attachments to ensure appropriate capacity management for each user's mailbox.
- A warning notice shall be displayed for emails being sent to recipients outside the organization.
- Incoming and outgoing email attachment shall be filtered at the email gateway. GILAC email gateway shall be protected against Advanced Persistent Threats and Zero Day attacks shall be implemented.
- Anti-virus software shall be configured to scan attachments in all emails. If a virus is found in an incoming SMTP mail, then the appropriate actions shall be taken to delete or quarantine the attachment.
- Third party vendors shall not be allowed to send emails to external domains.
- The organization shall prohibit:
    1. Automatic email diversion to external email addresses.
    2. Unauthorized private encryption of email or attachments.
    3. The opening of attachments from unknown or untrusted sources.
- GILAC shall disable the Open Mail Relay service.

31. Third-party Management Policy

- The information security requirements and controls shall be formally documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract.
- Confidentiality and non-disclosure of GILAC data shall be addressed in vendor contracts using legally enforceable terms.
- Appropriate legal advice shall be obtained to ensure that contractual documentation is valid within the country in which it is to be applied.
- If required then separate Non- Disclosure agreement shall be made on Government stamp paper and it shall be used where a more specific level of control over confidentiality is required.

- Contracts with third-party vendors shall include terms for complete deletion of data/ information at the end of the Agreement.
- Contracts shall also outline clauses for notification and reporting of unauthorized disclosure or confidential information leakage to GILAC within the agreed timeframe.
- Appropriate due diligence shall be exercised in the selection and approval of new vendor/supplier before contracts are agreed.
- The information security provisions in place at existing suppliers (where due diligence was not undertaken as part of initial selection) shall be clearly understood and improved where necessary.
- The supplier shall be expected to exercise adequate control over the information security policies and procedures used within sub-contractors who play apart in the supply chain of delivery of goods or services to Godrej.
- Godrej shall have all rights to audit the information security practices of the vendor/supplier and, where appropriate sub-contractors.
- The selection of required controls shall be based upon a comprehensive risk assessment taking into account Information Security requirements, the product or services to be supplied, its criticality to the organization and compatibility of the suppliers.
- For those vendors/suppliers that were not subject to information security due diligence assessment being made, an evaluation process shall be undertaken in order to identify any required improvements.
- SLA and performance of vendors/suppliers shall be monitored and reviewed as per contractual agreements on **bi-annual** basis.

32. Cloud Security Policy

- GILAC shall perform an assessment of the cloud service provider (CSP) prior to onboarding.
- The Procurement and Legal teams shall include the necessary legal, non-disclosure, business continuity and disaster recovery clauses in the CSP contract.
- The Data Owner/Custodian shall classify the data being hosted/stored at the CSP as per the 'GILAC Information Classification Scheme'.
- The organization shall ensure that the CSP's data privacy policy complies with the applicable laws.
- The IT team should implement the necessary cryptography controls for the data as per the data classification and on the network channel.
- Contracts with CSP shall include clauses for complete deletion of data/ information at the end of the Agreement.
- Contract shall also include clauses for the return of data to the organization and that there is no vendor-lock in period defined by the CSP.
- Wherever applicable, GILAC shall align its Cloud Security controls with industry good practices such as CIS benchmark.
- Roles and responsibilities for protecting the cloud environment should be agreed with the CSP, including shared responsibilities and the need for collaboration.

- GILAC shall ensure monitoring of security-related events and logs for cloud systems.
- The IT team shall implement the appropriate access permissions for the cloud environment as per the 'GILAC Access Management Policy'.
- Access to cloud-based services shall be provided using multi-factor authentication mechanism.
- Secure methods of connecting to cloud services shall be provided, which may include applying HTTPS (TLS) to all network traffic, configuring a virtual private network (VPN) for sensitive traffic and/or implementing a wide area network (WAN) solution for critical and/or highly sensitive information, segmenting networks by implementing virtual local area networks (VLANs), etc.
- The IT team should perform periodic backups of data hosted/stored on cloud environment as per 'GILAC Data backup & restoration policy'.
- GILAC shall conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services and that the acquisition or outsourcing of dedicated information security services is approved by Cyber Security Team within the organization.
- The organization performs scans to identify vulnerabilities in the cloud environment as well as applications hosted in the cloud as per GILAC's Vulnerability Management Policy.
- Information security awareness, education and training programs about cloud services shall be provided to employees and the supervising managers, including those of business units.
- The organization shall perform penetration testing at a defined frequency on cloud information systems and application hosted.
- Information security events shall be reported through appropriate management channels as quickly as possible. The mechanisms for incident reporting shall be agreed with the CSP as part of the agreement.
- Organizations shall regularly monitor, review and audit supplier/ CSP service delivery & SLA to ensure CSP complies to GILAC's Information Security Policies.

33. Cryptography Policy

- Confidentiality, integrity, authenticity and non-repudiation of business-critical information during its transmission over un-trusted networks shall be maintained.
- Encryption algorithms shall be implemented based on risk assessment.
- Legal and regulatory requirements of cryptographic controls shall be complied with by only using standard publicly released and tested algorithms.
- All encryption products and processes deployed on information assets shall be approved by Head of Information Security before deployment.

34. Business Continuity & Disaster Recovery

- Business Functional Heads shall identify critical business applications & processes under their purview that are required for continued operations of GILAC, in the event of a disaster. The criticality of applications & processes shall be evaluated based on the impact to business and implications on BU's services.

- Business process and technology redundancies shall be identified and deployed to avoid or reduce impact of disaster events. DR site shall be set up for critical business applications and processes to ensure continuity of business.
- Business Functional Heads shall identify and document the Recovery Time Objective [RTO] and Recovery Point Objective [RPO] for critical business applications and processes.
- Business Functional Heads along with IT department Heads shall evaluate and define DR plan.
- Business Functional Heads along with IT Team shall conduct DR drills/tests on **biannual** basis to verify the appropriateness of the DR plan.
- Application owner shall be responsible for reviewing and updating the DR plan based on the test results.
- DR plan documents shall be accessible and available to respective stake owners and teams in case the same needs to be referred in an event of an incident/disaster.
- Business Heads shall maintain all records with respect to DR drills for a minimum period of 2 years.
- Training & Awareness program shall be established for all GILAC functions and facilities. Relevant records shall be kept for a minimum period of 2 years for reporting purpose and to identify areas of improvement.
- Business Heads shall document & maintain all records in case of incidents/disasters where DR needs to be invoked. Same shall be retained for a minimum period of 2 years.
- Business Functional Heads shall work together with the IT Team to improve Recovery Time taken on the DR Setup for critical business applications.

35. Operational Technology (OT) Policy

- In case of a need to connect OT network with internal corporate network, necessary security controls shall be implemented, before establishing the connection. Approved connections shall be restricted and limited to identified secure services / protocols.
- GILAC shall ensure strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network)
- OT systems should be patched periodically basis OEM recommendations.
- GILAC shall perform periodic vulnerability assessments for OT systems.
- GILAC shall restrict access to OT locations and devices to authorized personnel only, the access shall be provided in compliance with physical security policy.
- Up-to-date anti-virus and malware protection solutions for OT shall be implemented. GILAC shall ensure that monitoring for malware detection is performed continuously.
- OT systems shall be securely configured and hardened, as per OEM recommendations, prior to production deployment. OT systems shall be periodically reviewed to ensure compliance.
- GILAC shall restrict unauthorized traffic to OT networks by configuring proper security controls (e.g. proxy servers, firewalls, etc.)
- GILAC shall implement necessary controls for continuous monitoring of cybersecurity event logs on OT network.

- External storage media, mobile devices or any other external devices shall not be connected to OT technology components and OT networks.
- OT Systems shall not have direct unsecured internet connectivity.

36. Compliance

36.1. Compliance Management

- All relevant legislative, statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date.
- Organization shall ensure compliance to Information Security and IT requirements defined in the 'IT Act' (latest) and mandatory cyber security guidelines issued by 'CERT-In' and same shall be reviewed periodically
- All employees shall adhere to the policies and procedures to maintain and keep up to date all relevant statutory, regulatory, and contractual requirements.
- Compliance violations shall be documented, reported and investigated by authorized personnel or team.
- Corporate Audit Team shall supervise and take necessary action in case of any deviation observed.
- Compliance with Information Security Policies and Procedures shall be reported to the GILAC Information Security Council on a periodic basis.
- All relevant statutory, regulatory and contractual documents and records shall be retained by resp departments of the Business Units for a period as per the required documentation/contracts.
- A review of compliance with legal and regulatory requirements that affect information security shall be performed regularly and when new legislation or regulatory requirements come into effect.

36.2. Intellectual Property Rights (IPR)

- Information Owners shall be responsible for identifying Intellectual Property (IP) that may be used in business processes and corresponding obligations.
- Information Owners shall be responsible for maintaining and retaining proof of entitlement and usage of licenses of identified IP.
- IP shall be acquired only through Original Equipment Manufacturers (OEMs) or authorized resellers and only licensed IP shall be used.
- IP material protected by copyright shall not be copied, duplicated or converted to another format, in full or in part other than permitted by copyright law.
- Media containing IP shall be removed from or securely overwritten prior to disposing.
- Information Owners shall disclose the IP owner credentials on the IP utilized for official purposes.

36.3. Use of Cryptographic Controls

- GILAC shall ensure that the use of cryptographic controls is compatible to the laws of India and as well as the laws of its clients' country if any.

37. Data Privacy

37.1. Privacy Governance

- Responsibility for privacy and protection of sensitive personal information of all internal / external stakeholders shall be established.
- All Business Units shall designate a Grievance Officer to address privacy related grievances from stakeholder, if applicable.
- Processes and procedures shall be established to protect Sensitive Personal Information (SPI) in accordance with the applicable compliance requirements.
- Organization should consider hiding sensitive data (e.g. PII, SPI, etc.) by using techniques such as data masking, pseudonymization or anonymization taking applicable legislation into consideration.
- Personal data of stakeholders shall be securely stored, in manual or electronic form in accordance with the applicable compliance requirements.
- Privacy Impact Assessments (PIA) shall be conducted by respective Business Units periodically and when changes are anticipated on how sensitive personal information of stakeholders is acquired, stored, used or disclosed.
- Privacy training shall be administered to all staff and authorized third-party personnel who handle sensitive personal information.
- Changes to Legal and regulatory landscape related to privacy shall be periodically monitored and any impact from such changes shall be identified and addressed.

37.2. Notice

- An online privacy notice shall be made available for stakeholders during collection of sensitive personal information.
- Privacy notice shall clearly and conspicuously describe how GILAC collects, uses, stores and discloses sensitive personal information.

37.3. Consent

- GILAC shall obtain the stakeholder consent prior to collection, processing and transfer of sensitive personal information.
- Upon customer's request, GILAC shall provide mechanisms to correct or amend stakeholder's sensitive personal information.

- If the stakeholder withdraws his/her consent to use his/her personal information by GILAC, GILAC shall consider not providing services for which the information was sought, but data will be retained as per legal and regulatory requirements.

37.4. Collection and Use

- GILAC shall limit the collection of sensitive personal information that is necessary and relevant for the purposes for which information is being collected.
- Sensitive personal information shall only be collected by reasonable, lawful and fair means.
- GILAC shall limit the use of sensitive personal information for the purposes identified in the privacy notice.

37.5. Disclosure

- Sensitive personal information of stakeholders shall only be disclosed for the purposes outlined in the privacy notice.

37.6. Retention and Destruction

- Sensitive personal information of stakeholders shall be retained for only as long as necessary to fulfill the stated purpose or based on legal or regulatory requirements.

37.7. Privacy Incidents and Grievances

- Incidents that involve misuse, unauthorized access or disclosure of sensitive personal information shall be categorized and handled as privacy incidents.
- Grievance Officer shall address stakeholder privacy related complaints in accordance with legal or regulatory requirements.

38. Responsible Parties

There should be documented standards and procedures for managing the asset lifecycle. The owner of this policy is the Group CISO, who shall be responsible for the maintenance and updating of the policy document.
While Group CISO is the owner of this policy, he/she can utilize various departments within the organization to implement, enforce and support this policy.