GODFREY PHILLIPS
INDIA LIMITED

Information Security Policy

Godfrey Phillips India Limited

Effective From

19-July-2023

Document Approvers

S.No.	Approver Name	Designation	Date	Signature
1	Mohd Irfan	HEAD - IT	19-July-2023	

Document Control

S No	Type of Information	Document Data
1	Document Title	Information Security Policy
2	Version No.	2.1
3	Date of Release	19-July-2023
4	Document Owner	Head-Cyber Security
5	Document Author	Head-Cyber Security
6	Process Owner	Respective IT Leads + Head of Cyber Security
7	Document Approver	HEAD - IT

Document Change History

Version No.	Revision Date	Reviewed By	Description of Change	Date Approved
1.0	08-11-2018	Priya Dar (CIO), Sanjay Gupta (ERP Head), Manoj Varma (Manager Infra)	Revised/updated	08-11-2018
2.0	14-Oct-2022	Mohd Irfan (Head-Infra), Sanjay Gupta (Head Enterprise Apps), Pankaj Dhingra (Head Digital), Farman Khalid (Head BI & Data Projects), Umesh Kumar (Head Cyber Security)	Revised/updated	14-Oct-2022
2.1	19-July-2023	Mohd Irfan (Head-IT)	- Scope - Role Change - Frequency of ISC / MRM	19-July-2023

Table of Contents

1. Introduction

Security of information assets of Godfrey Phillips India (GPI) is of paramount importance. Confidentiality, Integrity, and Availability of these assets shall always be maintained through controls that are commensurate to the criticality of the asset, so as to protect the assets from all types of threats, whether internal or external, deliberate, or accidental. It shall also be ensured that all legal, regulatory, statutory, and contractual obligations are met.

2. Policy Statement and Objective – A.5.1.1

2.1 Policy Statement

Godfrey Philips India Ltd. shall protect its infrastructure and propriety information generated or processed within by building robust Information Security Management System. All employees, contractors, sub-contractors, and vendors shall be committed to comply with the Information Security Policy wherever applicable.

The objectives have been mentioned below:

i. Defining agreed information security principles within the organization.
ii. Providing a framework for implementing Information security management in GPI.
iii. Raising awareness of security risks relating to information of GPI and IT infrastructure used by GPI. Information security awareness training is imparted to all employees.
iv. Fulfilling the organization's audit and legal obligations.
v. All suspected breaches of information security are assessed, reported, investigated, and responded.
vi. Integrity of information is maintained through protection from unauthorized modification.
vii. Information is available to authorized users when needed.
viii. Ensuring Continual Improvement to the information security management system.

2.2 Scope

The Information Security Policy applies to all domains and functions of GPI and its subsidiaries including employees and all related stakeholders.

2.3 Document Review – A.5.1.2

The document owner is the Head-Cyber Security who is responsible of maintaining the accuracy of the Information Security policy. The document shall be reviewed annually or if there is a significant change in the existing IT environment affecting the policies, whichever is earlier. This includes reviewing the Risk Assessment and the Information Security Policy. The reviews shall be carried out for accessing the following:

i. The extent of conformity to the Information Security Policy
ii. Evaluating the capability of ISMS to ensure compliance with applicable laws and regulations
iii. Identifying the potential areas of improvements.

Post review, responsible parties shall be identified, and stipulated timelines shall be defined for corrective actions which shall be taken to eliminate the cause of non-conformity or other undesirable situation to prevent occurrence. Preventive action shall be taken to eliminate the cause of a potential non-compliance or other potential situation. Additional policies could be issued and/ or existing policies could be updated, as required.

2.1.1 Policy Exceptions

Any exception to the requirements stated in this policy must be properly documented and approved by the CIO/HEAD – IT, all policy exceptions must be reviewed annually.

3. Information Security Organization

The organization structure for Information Security shall be clearly defined, reviewed, and updated as necessary. While defining roles and responsibilities within the organization structure, segregation of duties and the principle of least privilege shall be employed, wherever applicable.

3.1.1 Organization Structure- Roles and Responsibility – A.6.1.1

3.1.2 IT Steering Committee (ITSC)

- The IT Steering Council consists of: CEO, CIO/HEAD - IT, CFO, CHRO, Head Strategy, Head Sales & Distribution, Business Head – Cigarettes, Head – Infra and Head- Cyber Security.
- ITSC will be updated every six months of Security related matters and provide broad Strategic guidance.

3.1.3 Information Security Council (ISC) / Management review meeting

ITSC consists of: CIO/HEAD - IT, CHRO, CFO, CLO, IT Leads and will meet at-least once in a year.

- Provide management direction and support for implementation and maintenance of the information security management system.
- Ensure that the information security management reviews are conducted periodically (as above)
- Reviewing major security incidents reports.
- Approving major security initiatives.
- Analyzing cost effectiveness of security implementation.
- Reviewing non-conformances raised during internal/external audits. And oversee appropriate actions.
- Decide the acceptable levels of information security risks.
- Provide management support to ensure that the IS Controls/ remedial measures suggested by Head Cyber Security / CISO are implemented in respective departments

3.1.4 Chief Information Officer / Head - IT

- Overseeing the security of information and information infrastructure at GPI.
- Identify information security objectives and align them to the corporate strategic plans.
- Provide broad strategic directions & ensure the Cybersecurity initiatives are in alignment with overall IT Strategy.

- Approve policies related to information security management. Approve periodic changes as needed.
- Reviewing periodic audit report specific to data Center/IT operations.
- Ensuring IT strategies and processes support company-wide goals

3.1.5 Head Cyber Security

- Overall accountability of Cybersecurity in organization. Defining information security processes.
- Review the compliance of information security and report information security compliance to ISC.
- Reviewing the effective implementation of security controls across all departments, by conducting suitable audits. Suggest remedial measures.
- Address Information Security concerns and issues arising from different functions (if any). Further, ensure that appropriate advice is provided.
- Ensure periodic effective information security awareness program to impart awareness to all the employees.
- Perform required Risk Assessment exercises in the organization. Recommend suitable risk mitigation measures.
- Advise the ISC regarding the acceptable levels of information security risks.
- Keeping the ISMS up to date with all the policies, properly documented and available to all the concerned people.
- Facilitating and coordinating various activities pertaining to implementation and monitoring of Information Security Policy.
- Ensuring that provisions are in place for the continued protection of information system resources in the organization.
- Reviewing, analyzing, and resolving the information security incidents reported in the organization. Reporting to the ISC/ Cert-In as suitable.
- Arranging for independent information security audits / reviews, vulnerabilities assessment, penetration testing and facilitate resolution of security related issues reported by the systems in the audit.
- Reporting the compliance or the lack of compliance in the Information Security Policy.
- Identification and deployment of security tools & technology to improve information security posture of GPI.
- Ensure that the information security management reviews are conducted periodically.

3.1.6 Manager -Cyber Security

- Responsible for Technical assessment like Vulnerability assessment, Penetration Testing, Red Teaming kind of initiatives
- Responsible for monitoring security posture from DC, Cloud environment and coordinating with appropriate team (Infra and/or Apps) for the resolution
- Monitoring security intrusions and activities and taking counter measures by coordinating with other departments.
- Initiating and implementing corrective & preventive action for security incidents.
- Directs and oversees the assessment, selection, implementation, and maintenance of information security tools and technologies

- Security tools/systems implementation and governance
- Coordinate or assist in the investigation of information security threats or other attacks on the information assets.

3.1.7 Compliance Lead

- Responsible for performing all Security internal audits & IT risk assessment activities, tracking till closure
- Oversee formal risk assessment and self-assessments program for various Information Services systems and processes
- Planning for information security risk management, security incident management, Change Management, and overall information security requirements as per Information Security Policies of GPI
- Ensuring hardening of servers/controls across all deployment platforms like DC, Mult-cloud (e.g. CIS Controls for Linux, windows for servers)
- Keeping tab on implementation of various advisories/Patches/security update across all platforms and MIS/reporting
- Record keeping for the purpose of compliance covering all types of IT/Info security audits
- Weekly/Monthly advisory creation and dissemination across organization to educate users. The advisories will be based on GPI's policies & latest development in cyber security and potential impact to GPI
- Information security training calendar creation and delivery management across all GPI's function and locations
- KPI/dashboard management
- Responsible for update of the policies, procedures related to Information Security and privacy
- Responsible for Initiating and advocating safe practices and Industry standards
- Strong knowledge of the requirement of Computer Applications and Network security technologies and principles
- Ensuring BCP-Drill annual calendar creation across Applications landscape, its Tracking, reporting in-line with BCMS policies of GPI
- Ensuring Access review as per defined frequency in the policy

3.1.8 Head-Digital and Team

- Engaging with Cyber Security team at the time of initiation of new projects
- Supporting Cyber Security team in all security related projects/activities of GPI
- Ensuring compliance with GPI's Information security policies as applicable
- Ensuring actions in consultation with Cyber Security Team and respective partners on identified risks/vulnerabilities related to this function.
- Ensuring access controls are implemented as per the policy and review of the access is done periodically, dormant users are disabled/deactivated
- Planning and execution of Business Continuity planning as per defined policy

3.1.9 Head-Enterprise Applications and Team

- Engaging with Cyber Security team at the time of initiation of new projects
- Supporting Cyber Security team in all security related projects/activities of GPI

- Ensuring compliance with GPI's Information security policies as applicable
- Ensuring actions in consultation with Cyber Security Team and respective partners on identified risks/vulnerabilities related to this function.
- Ensuring access controls are implemented as per the policy and review of the access is done periodically, dormant users are disabled/deactivated
- Planning and execution of Business Continuity planning as per defined policy

3.1.10 Head- BI & Data Projects and Team

- Engaging with Cyber Security team at the time of initiation of new projects
- Supporting Cyber Security team in all security related projects/activities of GPI
- Ensuring compliance with GPI's Information security policies as applicable
- Ensuring actions in consultation with Cyber Security Team and respective partners on identified risks/vulnerabilities related to this function.
- Ensuring access controls are implemented as per the policy and review of the access is done periodically, dormant users are disabled/deactivated
- Planning and execution of Business Continuity planning as per defined policy

3.1.11 Head-Infra

- Engaging with Cyber Security team at the time of initiation of new projects
- Supporting Cyber Security team in all security related projects/activities of GPI
- Ensuring compliance with GPI's Information security policies as applicable
- Ensuring actions in consultation with Cyber Security Team and respective partners on identified risks/vulnerabilities related to this function.
- Ensuring access controls are implemented as per the policy and review of the access is done periodically, dormant users are disabled/deactivated
- Planning and execution of Business Continuity planning as per defined policy
- Reviewing Capacity Management related to IT Infrastructure

3.1.12 Data Center Coordinator

- Conducting periodic audits for idle accounts and user privileges.
- Obtaining prior approval before opening ports on firewall or router or any networking devices to provide access to internal servers.
- Maintain relevant access lists of devices.
- Taking backup and maintaining associated logs.
- Maintaining fault logs to record disruptions
- Participate in BCP activities.
- Periodic review of third parties
- Performing capacity planning
- Ensuring security of DC devices e.g., virus scanning on all servers, Patch management etc

3.1.13 Network Administrator

- Monitoring and administering Network devices.

- Ensuring security of LAN devices.
- Conducting periodic audits for idle accounts and privileges of existing users.
- Monitoring network traffic and protocols on the network. Ensuring only standard protocols are used on the network.
- Closure for open ports for vulnerabilities and threats.
- Maintain relevant access lists
- Taking configuration file backup of network devices
- Maintaining change control logs for ensuring any changes in the network or its components are authorized and controlled.
- Periodic review of third parties
- Maintaining fault logs to record disruptions to the network or its components.
- Participate in BCP activities.

3.1.14 System Administrator

- Monitoring and administering Servers and desktops.
- Ensuring that all applicable patches, service packs, and updates are installed.
- Conducting periodic audits for idle or unused accounts and privileges of existing users.
- Performing system reviews to identify unusual activity.
- Taking data backups and maintaining backup logs.
- Maintaining fault logs to record disruptions
- Participating in BCP activities.
- Checking optimization of utilization of servers.
- Performing Capacity planning
- Periodic review of third parties
- Maintenance of asset register

3.1.15 Database Administrator

- Designing, developing, organizing, managing, and controlling databases in accordance with applicable security policies,
- Backup and restoration
- Recovering databases in a secure manner when damaged or compromised.
- Conducting periodic audits for idle accounts and privileges of existing users.
- Reviewing logs.
- Participate in BCP activities.

3.1.16 Manufacturing Operations

- Supporting Cyber Security team in security related projects/activities of GPI
- Ensuring compliance with GPI’s Information security policies as applicable
- Executing actions in consultation with Cyber Security team and respective partners on identified risks/vulnerabilities related to this function
- Ensuring access controls are implemented as per the policy and review of the access is done periodically, dormant users are disabled/deactivated
- Planning and execution of Business Continuity planning as per defined policy

3.1.17 Contact with Authorities and Special Interest Groups – A.6.1.3 and A.6.1.4

Appropriate contacts with law enforcement agencies, fire department, emergency services and service providers shall be maintained by the administration department to escalate to the respective authorities as required.

Membership with special Interest forums shall be maintained by Cyber Security team for receiving and distributing the updates on new vulnerabilities, security threats, Industry best practices, early warning, and alerts.

3.1.18 Information Security in Project Management - A.6.1.5

To ensure that information security principles and objectives are imbibed in the organisation culture, Cyber Security team will be involved to ensure information security requirements are adhered to during the entire life cycle of the project since its on-boarding, during normal operations and transfer or off- boarding. This is applicable for IT projects only

The aspects that should be covered in the various stages are as follows:

On-boarding of a Project:

- The information security requirements related to the upcoming business/project shall be clearly identified and communicated to the relevant stakeholders.
- Evaluation of the information security requirements for the project basis the existing organisation environment identified so that the differential requirements or controls can be implemented.

During normal operations:

- Information security requirements are monitored as per project requirements. The examples of security requirements is vulnerability assessments, periodic access reviews etc

Project Transfer or off-boarding:

- Application/Infrastructure team shall intimate the Cyber Security team about systems/servers getting decommissioned

4. Third-Party Management A.15.1.1

All external parties who are contracted with GPI shall agree to follow the Information Security Requirements based on the engagement of GPI in mitigating the risks associated with the third parties. Information Security requirements shall be communicated to any such parties prior to any commencement of the engagement.

4.1.1 Third-Party Access A.13.2.2, A.15.1.2, A.15.1.3

i. All services to be provided by a third-party shall be clearly identified.
ii. Non-Disclosure Agreements shall be signed with all the third parties.

iii. GPI shall conduct a risk assessment to identify potential risks to GPI's Information Assets as a result of outsourcing to the third-party and appropriate controls shall be implemented. This shall be done once in two years.

iv. A formal contract and/or SOW/agreement shall be entered between GPI and each third-party providing services to GPI or using GPI's information systems to address the secure transfer of business information between GPI and third parties. Third-party service delivery agreement shall include security requirements of GPI, service definitions and service delivery levels / timelines.

v. GPI shall ensure that security controls and service levels specified in the service level agreement are implemented, operated, and maintained by the third-party

4.1.2 Third-party Service Delivery A.15.2.1 A.15.2.2

i. Security controls and service level associate reports and records of third-party service providers shall be independently assessed, reviewed, and monitored. Third-party reviews/audit shall be carried out, as required, to review the performance and adherence to the service levels by the third-party.

ii. Changes to the provision of services, including maintaining and improving existing information security policies. and controls, shall be managed, taking account of the criticality of business systems and processes Involved and re-assessment of risks.

5. Asset Management

The Asset Management specifies the importance of information assets including identification of the asset owner, asset classification and determining confidentiality (C), integrity (I) and availability (A) ratings of the assets. All information assets must be classified to indicate the need, priorities and degree of protection needed. All information has varying degrees of sensitivity and criticality. Inventories of assets help ensure that effective asset protection takes place. Inventories of assets help ensure that effective asset protection takes place.

5.1.1 Information Asset Inventory – A.8.1.1, A.8.1.2

i. GPI's information assets shall be listed in an Information Asset Register. Information Asset Register shall be maintained on an ongoing basis.

ii. Each Information Asset shall be clearly identified individually and (if appropriate) collectively in combination with other Information Assets to form an identifiable Information asset.

iii. The Information Asset Inventory shall contain the following information as a minimum:

   a. The type and location of asset.
   b. Name of the function that uses this asset
   c. The Asset Owner and Custodian.
   d. The classification of the asset.
   e. The confidentiality, integrity, availability (CIA) ratings of the information asset; and
   f. The overall criticality rating for each information asset.

5.1.2 Information Classification – A.8.2.1

The first step in establishing the safeguards that are required for a particular type of information is to determine the level of sensitivity applicable to such information. Information classification is a method of assigning such levels and thereby determining the extent to which the information need to be controlled and secured.

i. Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

ii. Respective information owners are responsible for assigning appropriate classification to information assets in line with the guidelines as defined in the Table below

iii. Results of classification should be updated in accordance with changes of their value, sensitivity, and criticality through their life cycle.

iv. Information classification will determine the baseline security controls for the protection of information/asset.

v. Information security measures to be implemented will be commensurate with the value, sensitivity, and risk involved.

vi. All employees are responsible for ensuring that company information assets receive an appropriate level of protection by observing information classification guidelines.

vii. All Information Assets shall be classified according to this policy. All information shall be handled according to the classification levels to ensure security of the Information Assets.

5.1.3 Information Classification Category

Classification	Description
Public	This classification applies to the information which has been explicitly approved by the management for release to the public. Examples include: Product brochures widely distributed. Information widely available in the public domain, including publicly available Company web site areas.
Internal	This classification applies to the information of GPI which is meant for use by employees of GPI (e.g., policy and procedure documents.) While its unauthorized disclosure is against the policy, it is not expected that this disclosure affects the business, shareholders, business partners, employees and customers. Most corporate information intended for use by and disclosure to employees fall into this category. Examples include: Training materials, policies, work instructions, departmental memos, internal staff announcements, news and notifications, phone and email directories, internal vacancy notices, intranet Web pages"

Confidential	This classification applies to the information of GPI which if (disclosed outside GPI) to unauthorized individuals, altered, misused, or destroyed will cause damage to its business, shareholders, business partners, employees, and customers. Access to this information require approval from the owner of the information and shall be given on a need-to-know basis. Examples include: Operating procedures and guidelines, marketing, or promotional information (prior to authorized release), investment options, financial transaction receipt, productivity reports, disciplinary reports, contracts, service level agreements, contract negotiations, including bank account numbers of employees. For staff matters relating to GPI or its employees or officers. Examples of such information include: - Compensation and benefits - Recruitment and staffing - Discipline and conduct - Appraisals and reviews
Restricted	This classification applies to the assets containing the information of GPI, which if disclosed (either within GPI or outside GPI) to unauthorized individuals, altered, misused, or destroyed will cause damage to its business, shareholders, business partners, employees and customers. This information, if not adequately protected, may result in non-compliance with applicable laws and regulations. Access to this information require approval from the owner of the information and shall be given on a need-to-know basis Examples include: Strategy documents/plans, Initiatives documents

5.1.4 Acceptable Use of Information Assets – A.8.13

i. GPI shall ensure that there are rules defined and implemented for the acceptable usage of all the Information Assets of GPI.

Refer GPI Acceptable use policy.

ii. Employees, contractors and third parties of GPI shall follow the guidelines for the acceptable level of use of all the Information Assets of GPI. Information Assets shall be used for business and operational purposes and shall be protected from damage on account of nonofficial usage.

6. Human Resource Security

Information security controls shall be designed and integrated in the Human Resources (HR) processes to ensure that appropriate security measures are taken during the employee lifecycle – prior to employment, during employment and after termination or change of employment within the organization.

6.1.1 Background Checks / Screening – A.7.1.1

To reduce the risk of human error, theft, fraud or misuse of facilities, background checks shall be carried out for all potential recruits' preferably prior appointment. This includes checks on:

i. Claimed academic and professional qualifications.
ii. Identity checks (e.g.: passport, Aadhaar etc).
iii. Criminal records
iv. Address/demographic information verification

6.1.2 Terms and Conditions of employment - A.7.1.2, A.13.2.4

All employees, contractors and third-party users of GPI Information Assets shall sign and agree terms and conditions of their contract, these terms, and conditions shall state GPI's as well as the employee's responsibilities towards Information Security.
All employees, contractors and third-party users of GPI shall sign the Non-Disclosure Agreements as an indication of their acceptance to protect the' confidential and sensitive information of GPI.

6.1.3 Management Responsibility - A.7.2.1

All supervisory roles are responsible for the performance and conduct of the staff personnel reporting to them. Supervisors are required to monitor performance of each of their staff, . and ensure employees and contractors apply information security in accordance with the established policies and procedures of GPI.

6.1.4 User Awareness and Training - A.7.2.2

Information Security awareness and training shall be conducted for all the employees, contractors, and third-party users at least once in six months and record of all such trainings shall be maintained by IT department.

6.1.5 Disciplinary Process - A.7.2.3

There shall be a formal disciplinary process for employees, contractors or third-party users who have violated GPI's Information Security Policy.
In the cases of serious misconduct, the process shall allow for the instant removal of duties, access rights, and the various allocated privileges up to and including termination.

Refer GPI Disciplinary Process Policy for more details

6.1.6 Termination Process - A.7.3.1

To reduce the risk of theft, fraud or misuse of facilities, all terminations shall be appropriately handled and responsibilities for performing employment termination shall be defined and assigned.

Refer GPI Disciplinary Process Policy for more details

6.1.7 Return of Assets – A.8.1.4

All employees, contractors and third-party users shall return all GPI's assets in their possession upon cessation/termination of their employment, contract, or agreement.

6.1.8 Removal of Access Rights – A.9.2.1, A.9.2.6

Access rights of all employees, contractors and, third-party users to Information and information processing facilities shall be removed upon termination, of their employment, contract, or agreement, or adjusted upon change.

7. Cryptography

7.1.1 Policy on the use of cryptographic controls A.10.1.1

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

i. Cryptographic mechanisms shall be employed to prevent unauthorized access.
ii. Cryptographic mechanism shall be reviewed annually by Head-Cyber Security and cascaded to Head-Applications for relevant changes, if any.
iii. The access to the servers for maintenance/operational /development work shall be done using encrypted channel

7.1.2 Key Management A.10.1.2

The cryptographic techniques are only effective in supporting security objectives if keys are securely managed over their lifecycle.

i. The key management policy for ownership, distribution, archival, storage and revocation of keys shall be established to protect the keys throughout their lifecycle.
ii. The cryptographic keys shall be protected against unauthorized modification, substitution, unintended destruction, and loss.

8. Physical & Environmental Security

The aim is to protect the business premises and information assets from unauthorized access, damage, and interference.

8.1.1 Physical Security Controls

8.1.2 Physical Security Perimeter – A11.1.1

All GPI offices must be divided into different zones. Each zone must have appropriate level of access restrictions and access authorization requirements.

8.1.3 Physical Entry Controls A11.1.2

i. Only those employees, whose job description demands access to critical areas (e.g., server room, network room etc.), shall be allowed to enter.

ii. Identification cards shall be issued to all employees of GPI and shall be visibly displayed as a means of physical identification while inside GPI premises.

iii. All entry and exit points shall be identified and controlled. Reception area shall be manned during office hours.

iv. All movement of Information assets going in and out of premises shall be duly authorized and tracked.

v. Visitor's entry into the premises shall be restricted by appropriate security validations.

vi. All visitors shall 'be required to sign to the visitor's register. Visitors shall be restricted to the reception area / visitor room unless they are escorted.

vii. Visitors shall be issued 'visitor' identification badges which they shall visibly display within GPI premises.

viii. The identification badges shall not be carrying any access card on them.

ix. These identification badges shall be collected back from the visitors prior to their departure from GPI.

8.1.4 Securing Offices, Rooms, and Facilities A11.1.3

i. Depending on the sensitivity of information handled within, the physical security for offices, rooms and facilities shall be designed and applied.

ii. Access to server room must be restricted Only authorized IT Department personnel and other authorized personnel shall be allowed to access the server room.

8.1.5 Working in Secure Areas A11.1.5

The restricted areas shall be identified, and the security controls should be implemented to prevent intrusion and damage to these areas. It shall be ensured that:

a. Appropriate physical access controls, are implemented in these areas.

b. Employees are provided access to the restricted areas on ‘need to have’ basis only;

c. Entry and Exit, as well as movement of any assets in restricted areas is monitored and recorded;

8.1.6 Public Access, Delivery and Loading Areas A11.1.6

i. Areas where loading and unloading of items are done shall be separated from information processing facilities.

ii. These areas shall be monitored and equipped with the appropriate physical security controls during loading and unloading of items.

iii. Access to these areas shall be confined to authorized personnel only during loading and unloading activities.

iv. The movement of all incoming and outgoing items shall be documented and all incoming items shall be inspected for potential threats.

8.1.7 Environmental Security

8.1.8 Protecting against External and Environmental threats A11.1.4

i. GPI's offices shall be fitted with appropriate firefighting (fire extinguisher, smoke detectors, sprinklers, fire hydrants, fire alarms, etc.) devices at critical locations including all critical areas in order to arrest the fire and to avoid damage to the various resources of GPI.
ii. Evacuation drills shall be conducted on a quarterly basis.
iii. Appropriate safety measure shall be taken to avoid loss and damage due to water flooding,
iv. HVAC failure, and inappropriate drainage system etc. within the premises of GPI should be checked and monitored regularly to resolve any failures.
v. Physical protection against damage from natural or man-made disaster shall be designed and applied.
vi. All critical areas shall be equipped with adequate environmental security measures.

8.1.9 Supporting Utilities A11.2.2

Appropriate measure shall be taken to protect equipment from power failures or other disruptions caused by failures in supporting utilities.

All servers and network equipment shall be fitted with uninterruptible power supply systems, electrical power filters, or surge.

8.1.10 Equipment Siting and Protection A11.2.1

Appropriate measures shall be taken to ensure that unauthorized persons don't have access to critical equipment and critical areas.

i. Critical information assets shall be placed in secure area.
ii. The secure areas shall be used only for accessing the information assets.

8.1.11 Cabling Security A11.2.3

Adequate protection (e.g., conduiting, tagging etc.) shall be applied to protect power and telecommunications cabling carrying data or supporting information services from interception or damage.

8.1.12 Equipment Maintenance A11.2.4

i. All equipment shall be properly maintained to ensure their continued availability for uninterrupted business activities. Provisions for Annual Maintenance Contracts (AMC) using approved vendors shall be used as applicable.
ii. All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning, are in appropriate condition for the information systems and/ or facilities that they are supporting.

8.1.13 Security of IT Equipment

GPI's office electronic equipment shall be physically secured and shall be adequately protected to ensure unauthorized person doesn’t have easy access to the equipment.

8.1.14 Security of Equipment Off-Premises A11.2.6

Security shall be applied to off-site equipment (e.g., Laptops, cellphones) taking into account the different risks of working outside GPI's premises. For example, each user carrying / managing the portable devices / equipment such as Laptops, Cellphones, etc. that is owned or hired by GPI shall be responsible for the security of equipment.

8.1.15 Disposal of Media A11.2.7

IT equipment and devices containing sensitive information shall be disposed-off only after approval. Further, appropriate data and media destruction shall be performed prior to disposal. Disposal of retired hardware and media shall comply with prevalent environmental regulations.

8.1.16 Removal of Information Assets A11.2.5

Equipment or software shall not be taken off-site without prior authorization

9. Communications and Operations Management

Operations management aims at increasing system availability and ensuring secure functioning of the information processing facility. This covers all hardware, software, and network systems.

9.1.1 Operational Procedures and Responsibility

9.1.2 Documented Operating Procedures A.12.1.1

i. An operational procedure shall be developed as and when a new information system or service is introduced. The operational manual shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure.

ii. The procedure shall encompass necessary checklists (as required) to implement the various activities mentioned above.

iii. All system and application administrators shall ensure that operational manuals are updated at specified intervals or at the time of any system change(s).

9.1.3 Change Control A.12.1.2

i. Changes to IT assets (including applications, servers, systems software, security architecture and network devices) shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. This involves obtaining prior approval, performing impact analysis, testing, and maintaining up-to-date documentation for the entire process. Change should be tested in a non-production environment before deployment and ineffective changes should be rolled-back,

ii. All changes shall be controlled and documented to ensure that any changes do not compromise confidentiality, integrity or availability of information processed by or stored in the IT systems.

iii. All the change requests shall be initiated through IT Service Management Tool (ITSM). The change request shall be reviewed and approved by authorized personnel before starting the development of change.

iv. Appropriate processes must be put in place for all changes requiring emergency actions and response process, which bypass the Policies outlined.

v. The change management process should include provision for contingency or fallback process where necessary to ensure continuity of operations. This should include procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

9.1.4 Segregation of Duties – A.6.1.2

i. Segregation of duties shall ensure that the same person does not perform conflicting roles at the same time as any two of the following functions:
   - System administration
   - Network Administration
   - Database administration
   - Security audit

ii. In the event when it is not feasible to segregate the duties, other controls such as, monitoring of activities, audit logs etc. shall be used to monitor the activities.

9.1.5 Separation of development, test, and operational facilities A.12.1.4

The Development/test and production facilities / environments shall be separated to reduce the risks of unauthorized changes to the production system.

9.1.6 System Planning and Acceptance

i. GPI shall continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of GPI.

ii. Acceptance tests for new information systems, upgrades shall be established, and suitable tests of the system shall be carried out prior to acceptance.

9.1.7 Antivirus Management A.12.2.1

i. All servers, desktops, workstations, gateways, and any other access points to GPI's network shall be protected against malicious executables/malware.

ii. Anti-virus application shall ensure early detection, efficient containment, and eradication of malicious code.

9.1.8 Backup Management A.12.3.1

i. Backup procedures shall be maintained to ensure that backup is carried out on a regular basis. Backup procedure shall include the following:
   - Backup schedule.
   - Restoration of data.

ii. Regular backups in the form of daily and/or weekly (incremental) backups shall be taken in line with business requirements.

iii. The IT Team along with DC support vendor shall schedule backup as per the inputs received from the requestor/ Information owner.

iv. The Domain/Application owner shall determine the criticality/ classification of the data for the backup.

v. The Domain/Application owner will provide details of what must be backed up per system to the IT team.

vi. A complete list of the various servers in scope and the associated details such as the retention period, the schedule of backup, the type of backup, Business/Data Owner, etc., shall be maintained by the IT team in the form of the Daily Backup Report, and backup success rate is reviewed monthly basis in Monthly Operations Report reviews.

vii. A full back-up shall be taken before and after any critical changes to hardware, OS, application or configuration including the following:
  - Upgrade of operating system
  - Installing a new application component

viii. The backup procedure chosen for backup shall meet the following objectives:
  - Recovery Time Objectives – time required to recover data.

i. Recovery point objective – helps in determining how often to take backups, so you can minimize data lost between your last backup and a failure event.

9.1.9 Backup Restoration

i. The restoration of backup shall be carried out as per the business requirements of GPI .

ii. The restoration tests shall be performed to assess the effectiveness of the backed-up information. On a successful restoration, the details of the restoration must be recorded, and the process must be terminated

iii. In case of a failed restoration, an Incident shall be raised.

iv. For, an unplanned restoration request, the user/information owner shall make a request to the Application owner (stating the reasons for restoration) for obtaining approval of restoration of data. The Application owner shall ensure that the user is authorized to access the data required for restoration prior and shall forward the request to the IT Infra Head. Thereafter, the DC support vendor shall perform the restoration and update the user.

v. A log/record of all restoration will be maintained. The log/record should contain the following information, at a minimum:
  - Source and destination of the information restored
  - Data and time of restoration
  - Results and Sign-off/verification details

vi. Frequency of recovery testing for each application shall be performed annually and can be determined by the IT team based on:
  - Criticality of the application
  - Redundancy currently in place

vii. In-case of repeated failure in restoration, the root cause analysis (RCA) of the event shall be performed.

9.1.10 Network Security

GPI network shall be used for valid business purposes only. The protection of information contained in the organization networks is therefore the responsibility of the management and the activity and content of user information on the organization computer networks is within the scope of review by management.

9.1.11 Network Controls A.13.1.1

i. All network equipment and communication lines shall be identified, documented, and updated regularly.

ii. Network diagrams at all levels (WAN & LAN segments) shall be maintained and updated regularly.

iii. All connections initiated from outside of GPI networks to GPI-DC/Cloud networks and vice versa shall be routed and controlled through firewall positioned at the network boundaries

iv. Firewall ports shall be opened based on business need and approval only. All unsecure ports shall be closed by default

v. Firewall configurations/rule shall be reviewed on a bi-annually basis by GPI Security team to ensure business need for the open ports

vi. Third-party independent network assessment shall be carried once in two years (biennial) to provide assurance to the management, customers, and stakeholders.

9.1.12 Firewall

i. Firewalls shall be deployed to limit the inbound and outbound traffic in GPI network. The following controls shall be implemented:

ii. Firewall segmentation based on risk levels. Systems with similar risk level shall be put into one segment. (E.g., De-Militarized Zone where publicly accessible systems are hosted, an internal local area network zone, a secure zone where critical servers/ databases/ network devices are located, etc.).

iii. An updated, reviewed, and approved network diagram with all connections to and from the firewalls.

iv. Any changes in the firewall configurations shall follow the change management process.

v. Enabling the audit logging on the firewall to ensure that all critical accesses and changes to firewall configuration and policy are tracked. These logs/alerts shall be regularly monitored by the firewall administrator/Security team of GPI.

vi. Intrusion prevention systems deployed along with the firewalls shall also be monitored to detect / prevent the Intrusion and other unauthorized/ malicious activities.

9.1.13 Security of Network Services A.13.1.2

i. Head Cyber Security and Head Infra are required to identify the security features, service levels and management requirements of all network services included in any network services agreement, whether these services are provided in-house or outsourced.

ii. Non-essential and default services shall be disabled on all information systems and the default and vulnerable services required for business operations shall be fixed by implementing alternative mitigation controls.

iii. Changes to the security of network services shall follow a formal Change Management Process with an approval from the Head Cyber Security prior to the implementation of change in the production environment.

9.1.14 Media Handling

9.1.15 Management of Removable Media – A.8.3.1

Only approved users shall be allowed to use removable media for transfer of information from GPI’s assets.

9.1.16 Disposal of Media A.8.3.2

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

ii. Disposal shall be done only by authorized users and a formal report of the secure disposal of media containing GPI information shall be generated and recorded.

iii. All employees and third- party staff are required to securely dispose media containing GPI's information.

9.1.17 Information Labelling & Handling - A.8.2.2 and 8.2.3

Information labelling and handling of classified information is a key requirement for information sharing and storage arrangements. All information used for or by the organization, shall be filed and/or stored appropriately, according to its classification

9.1.18 Security of System Documentation

i. The appropriate security measures shall be implemented to maintain the security of the system documentation for critical information systems.
ii. Access to these documents shall be granted only to authorized users.

9.1.19 Information Exchange / Information Transfer

To prevent loss, modification, destruction, or misuse of information, GPI shall protect and control exchange of critical business information assets and software with third parties and outside organization.

9.1.20 Information and Software Exchange Agreements A.13.2.4

i. Formal agreements/NDA shall be established for the exchange of critical business information assets or software outside the organizations.
ii. These agreements shall specify management responsibilities, notification requirements, packaging and transmission standards, responsibilities and liabilities, data and software ownership, protection responsibilities and measures, and all encryption requirements as applicable.

9.1.21 Physical Media In Transit – A.8.3.3

Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation beyond GPI's physical boundaries.

i. Documents, Assets, and removable media carrying GPI’s information shall be transported after authorization. An NDA (Non-disclosure agreement) may be signed with the third parties responsible for the movement of GPI’s information asset as required
ii. Record/Gate-Pass shall be maintained for asset being transported which identifies the content, protection applied and the time of dispatch and receival.
iii. All employees, strategic partner and sub-contractor staff carrying GPI’s asset are required to ensure its appropriate protection during transit.

9.1.22 Publicly Available Information

i. Any information stored or generated in GPI that are made publicly available for public consumption must be and approved by appropriate authorities before making it public.
ii. Adequate controls must be put in place to ensure that integrity of such information is protected.
iii. All changes to the organization's website shall be controlled and logged.
iv. ‘Corporate Affairs of GPI’ shall be responsible for authorizing all changes to the organization/corporate's website.

9.1.23 Patch Management

i. Patch management solution shall be used as patching process.

ii. Patches shall be applied on test machine before patching it on the production or critical servers.
iii. Patches for critical systems shall follow the Change Management Process.
iv. Security patches shall be deployed, security Patches related to Zero-day vulnerabilities with high severity will be given highest priorities.
v. It is recommended roaming workstation should be configured Windows Automatic Updates to automatically download and install patches.

9.1.24 Email Security A.13.2.3

i. The following activities are strictly prohibited, with no exceptions: Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). If a user receives an e-mail of this nature, they must promptly notify to Email Security Team at GPI (emailsecurity-gpi@modi-ent.com).
ii. Any form of harassment via email, telephone etc., whether through language, frequency, or size of messages.
iii. Unauthorized use, or forging, of email header information.
iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
v. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
vi. Use of unsolicited email originating from within GPI's networks of other Internet/ Intranet/ Extranet service providers on behalf of, or to advertise, any service hosted by GPI or connected via GPI's network.
vii. User shall not carry personal mass storage devices in office premises.
ix. User shall not officially communicate through personal email account, and it shall be done through company's official e-mail system.
x. User shall not access their personal emails using company provided computing device.
xi. In case user is suspicious/doubtful that his/her e-mail account has been possibly compromised. User shall:
    a) Immediately inform to Email Security Team at GPI (emailsecurity-gpi@modi-ent.com) for assistance.
    b) Disconnect the computer from network/Shutdown the computer immediately and do not attempt to delete any content or files on the computer.
xii. The following activities are strictly prohibited, but not limited to:

i. Opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
ii. Downloading inappropriate material such as picture files, music files, or video files for personal use is strictly prohibited as this may bring viruses, trojans etc. to GPI systems.
iii. Introduction, storage, processing, or transmittal of pornographic material into GPI's information systems.

Note: Employees shall adhere to Media Policy of GPI.

9.1.25 Logging and Monitoring

GPI shall develop, communicate, and implement formal methods for logging and auditing relating to operations in day-to-day administration of IT and information security related areas. It should be ensured that the auditing and logging is reported in time to the appropriate authorities.

9.1.26 Audit logging A.12.4.1

i. Activities or use accounts should be audited to prevent misuse of functions that might result in compromise of information systems accounts. Logs shall be monitored and analyzed for any possible unauthorized use of information systems.
ii. All the critical logs shall be retained for a minimum period of 180 days and/or as per the directive from CERT-In/regulatory body
iii. Security controls shall be built to ensure the integrity of logs.
iv. Implement real-time monitoring for all accounts and access activities when required.
v. It shall be ensured that the system administrators do not have permissions to erase or deactivate logs of their own activities.
vi. Access to audit trails and logs shall be provided to authorized users only
vii. All unsuccessful and successful login attempts should be captured and logged
viii. Logs from security devices/system e.g., Firewalls, Anti-virus, End-Point Detection & Response, servers shall be collected, analyzed for any potential malicious activity

9.1.27 Monitoring System Use

i. Systems shall be monitored to detect deviation from access control policy and record monitor able events to provide evidence in case of security incidents.
ii. Audit logs recording exceptions and security relevant events on critical information processing facilities, must be recorded, and stored.
iii. Audit logs must include User ID, Date and time of event, Terminal identity/location and description of the vents.
iv. Audit logs must be reviewed on a regular basis to ensure that any unauthorized activity is identified in timely manner.
v. System logs must be securely transmitted and collected, protected, and appropriately archived.
vi. Audit logs shall be monitored to ensure that the users perform only authorized activities. The areas to be regularly monitored include Privileged access, Unauthorized access attempts, Failed logon attempts, System Alerts, etc.

9.1.28 Protection of Log Information A.12.4.2

i. Log information shall be protected against unauthorized access, alterations and operational problems. Access to logs shall be provided on 'need-to-know' and 'need-to-have' basis.
ii. Appropriate controls shall be implemented to prevent:
   - Alterations of the message types that are recorded.
   - Editing or deletions of the log files.
   - Exceeding the storage capacity of the logging media.

9.1.29 Administrator and Operator Logs A.12.4.3

i. Information system shall be configured in such a way that the system administrator and system operator activities are logged.
ii. System and Operator logs shall be maintained and provided the same level of protection.
iii. System administrator and Operator logs shall be reviewed on a regular basis.

9.1.30 Fault Logging

All types of faults shall be logged and analyzed along with taking appropriate action.

9.1.31 Clock Synchronization A.12.4.4

i. The clocks of GPI's systems shall be synchronized correctly to the NTP server as per the CERT-IN or government directives issued time to time to ensure the accuracy of audit logs that may be used for investigations.

ii. The correct interpretation of the date/ time format shall be ensured. The format shall be identical across all servers and network devices.

9.1.32 Capacity Management A.12.1.3

The objective of the Capacity Management is to:

- Understand the future business requirements from the perspective of GPI by tracking the current utilization of information systems and their capacity.
- Ensure that all the current and future Capacity and performance requirement are provided cost-effectively.

Information processing resources shall be regularly monitored to ensure continued availability of capacity to meet future requirements, for example in terms of processing power, bandwidth, storage, etc. This shall include monitoring the performance of all servers and network devices that have a greater cost and lead-time for procurement of new capacity once the need arises.

Based on the monitoring activities, projections of future capacity requirements shall be made by the respective teams to ensure that adequate processing power, bandwidth, and storage are available.

Capacity Planning Criteria

The following will be considered during the evaluation of the capacity of information processing resources:

- New business requirements.
- Expansion plans of organizational units and organization as a whole.
- Contingency plans for information systems.
- Storage capacity for systems.

These aspects would be monitored on a periodic frequency and in case certain thresholds are crossed then deliberation would be performed in case capacity needs to be increased and how would it be carried out basis interactions within the information systems and respective stakeholders.

10. Access Control – A.9.1.1

Access to information systems shall be controlled based on business and security requirements. Privileges shall be allocated to individuals on a need-to-know basis and event-to-event basis.

10.1.1 User Access Management

The access to GPI's information and information systems (Operating Systems, Applications, Databases, network equipment and others) shall be according to the principles of "least privilege" and "need to know" basis.

10.1.2 User Registration – A.9.2.1, A.9.2.2

Any access provisioning/modification must be aligned with the following requirements for the designated domain:

i. The requester must initiate the access request by intimation/information via email or via deployed system as applicable with business requirements approval, if any.
ii. The request generated must be classified into the respective domain that is Infrastructure, Enterprise applications, Business Intelligence and Location-specific applications.

10.1.3 Privilege Management A.9.2.3

i. Privilege or System user accounts are assigned to individuals who can perform certain security-relevant functions that ordinary users are not authorized to perform.
ii. Privileges must be allocated to individuals on a need-to-use and least privilege principles basis.
iii. Privileges and access rights granted to users shall be restricted, controlled, and recorded through a formal authorization and approval process. Changes to access rights and privileges shall also follow the same formal authorization and approval process.
iv. Privileges and access rights shall be individually defined for various information systems (for example operating systems, databases, application systems, etc.) along with the personnel or personnel level to whom the privileges can be allocated to.
v. User privileges shall be updated in a timely manner upon change in employment status, including promotion, departmental transfer, and employment termination.
vi. All privileged user accounts shall be reviewed by respective managers/asset-owners or the same shall be reviewed by the partners on a quarterly basis.
vii. A record of all privilege accounts along with changes, if any shall be maintained.

10.1.4 Review of User Access Rights - A.9.2.5

.

i. All user accounts and their associated privileges on applications, servers and network equipment shall be reviewed and approved by the Head Infrastructure/ Application Owners on a quarterly basis. A formal record of the review shall be maintained.
ii. Any identified redundant or inactive user accounts shall be disabled / deleted (within 90 days) where no longer required.
iii. A process for effective and timely removal of accounts associated with terminated users shall be followed to protect systems against former employees, contractors/third-party users. Human Resources shall disseminate notification to the IT team/Application Owner for terminations to ensure timely removal of user accounts.

10.1.5 User Password Management - A.9.2.4, A.9.3.1, A.9.4.3

i. All user passwords (individual as well as Administrator) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner.

ii. An initial password shall be provided to the users securely during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first logon as per the Password policy.

iii. Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems.

iv. The password and account policy shall be enforced for all user and administrative accounts on Operating systems, applications, databases, and all other information protected by password controls as per Password Policy

10.1.6 Unattended User Equipment - A11.2.8

i. Employees will be responsible for safeguarding the information assets installed in their areas.

ii. Active sessions must be secured by locking the workstation, password protected screen saver etc.

10.1.7 Clear Desk and Clear Screen A11.2.9

i. User must lock the session and Systems shall be enabled with a password protected screensaver whenever computing devices are left unattended.

ii. Where appropriate, paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially during off-office hours.

iii. Information assets like documents, correspondence, computer media etc. shall be secured when not in use, especially after working hours.

iv. Personal computers shall be protected with adequate controls (workstation locks, passwords, screen savers etc.) when not in use and after working hours.

10.1.8 Network Access Control – A.9.1.2

i. All network and network services in GPI shall be identified and documented.

ii. Access to GPI network and network resources shall be on need-to-know basis and authorizations shall be obtained from appropriate authorities before providing access.

iii. Access to third parties shall be given after carefully analyzing need and after assessing risks involved in providing such access.

iv. Network and network services access shall be periodically reviewed to ensure that unauthorized network services are not used, or authorized network services are not accessed by unauthorized personnel.

v. Internet shall be accessed only for business purposes.

10.1.9 User Authentication for external connections

i. Remote access connections to the GPI network shall be provided to authorized users only and appropriate controls implemented to maintain the confidentiality, integrity, and availability of information.

ii. An updated list of all users with remote access to GPI network is maintained.

iii. Remote access to the network of GPI is allowed through secure channels only.

iv. Remote access Is allowed through pre-approved accounts only and monitoring is enabled for all such accounts.

v. Appropriate controls meeting the regulatory requirements are Implemented if remote access is provided to manufacturers or suppliers for diagnosis or maintenance activities.

vi. Dial-up modems shall not be used within GPI network.

10.1.10 Equipment identification in networks

As an additional authentication control for remote access, equipment identifier is recommended to be used to authenticate the equipment connecting to the critical information systems of GPI.

10.1.11 Remote diagnostic and configuration port protection

Any access to system diagnostic ports shall be authenticated. Common ports that are used for remote diagnostics shall be ensured that they are not used as an open door by popular attacks. Hence the ports shall be secured in order to eliminate the possibility of popular TCPIP attacks through a remote scan.

10.1.12 Segregation in networks A.13.1.3

i. GPI data center is accessed by third parties if something goes bad and by the IT operations team if need arises. This network needs to be logically segregated from the corporate LAN.
ii. All data center systems must be put in logically different network segment.

10.1.13 Network routing control A.13.2.1

Routing controls shall be enforced on shared networks and trusted networks for transfer of data/information in a protected manner. Network routing shall be controlled in such a way that at any point of time, there shall be no misrouting of information or messages and shall relate to the business requirements of data protection.

10.1.14 Operating System Access Controls – A.9.4.2

i. Hardening standards for all Operating Systems and critical applications must be developed and maintained. All installations of the operating systems and applications must pe configured as per the hardening standards
ii. Access to operating systems must be controlled by a secure log-on procedure.
iii. The logs for all the log-on and log-off activities shall be maintained.
iv. Sign-on to GPI information systems shall be accomplished only with the use of the personally assigned User ID.

10.1.15 Use of System Utilities – A.9.4.4

i. Any use of utility programs that could override the system and application controls shall be restricted and strongly controlled.
ii. It shall be ensured that vendor default utilities are disabled during new server, network device or workstation commissioning.
iii. If for troubleshooting purpose there is a need to use these utilities, administrators of the servers and network devices shall ensure that such utilities are enabled for an authorized activity and are disabled immediately after the use. They shall ensure that activities carried out by using such utilities are logged.

10.1.16 Application and Information Access control – A.9.4.1

Logical access to the applications shall be restricted to authorized users only. The appropriate security controls shall be used to restrict access to the applications of GPI. IT Team shall administer authorization/access to applications.

10.1.17 Mobile Computing and Teleworking – A.6.2.1

10.1.18 Mobile Computing and communication

GPI shall safeguard and prevent leakage of information through mobile devices such as laptops and mobile devices. It shall include, but not limited to the following:

i. Latest virus definitions shall be regularly updated on the mobile devices and laptops to prevent the corruption of information stored on these devices.
ii. If the user of the mobile device has access to confidential information, access shall be protected via the user authentication (e.g., user ID and password) and inactive session timeout controls, if applicable.
iii. Users of the mobile computing devices containing GPI's information (if any) shall be made responsible for taking reasonable precaution to minimize the risk of loss or theft or misuse of the device and the data relating to the business operations. Such devices shall not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.
iv. Devices must be kept up to date with manufacturer or network provided patches using a Patch Management system.

10.1.19 Teleworking - A.6.2.2

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

i. Establishing a secure communication channel between the teleworkers and the networks of GPI.
ii. Use of appropriate authentication mechanism for authenticating those using the teleworking solutions.
iii. Adequate physical security controls shall be implemented at teleworking site.
iv. Revocation of authority, access rights and return of equipment when the teleworking activity ceases or when the employee exists from GPI.
Refer GPI Acceptable Use Policy for more details.

11. Information System Acquisition, Development and Maintenance

The Information Systems Acquisition, Development and Maintenance section of this Policy define the security requirements that need to be identified and integrated during the development and maintenance of information systems and services. This section is applicable to both in-house development and development done by third parties for GPI.

11.1.1 Security Requirements of Information systems

11.1.2 Information security requirements analysis and specification A.14.1.1

Process Owners (Respective IT Leads) will engage Security team and shall jointly define, analyze, and document information security requirements prior to the commencement of:

- New information systems development projects
- Enhancements to existing information systems
- Procurement of new information systems.

ii. Information Security requirements shall be identified using various methods such as deriving compliance requirements from policies and regulations and incident reviews.

iii. Information Security requirements shall consider:

- User authentication requirements, password policy etc.
- Access provisioning and authorization process
- Vulnerability assessments

10.1.2 Securing Application Services on Public Networks A.14.1.2

Adequate measures shall be implemented within applications to prevent errors, loss, unauthorized modification, or misuse of information in applications. The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification

10.1.3 Protecting Application Services Transactions A.14.1.3

Adequate checks shall be implemented within the applications to detect any corruption of information in application service transactions. These checks shall be based on the nature of the application to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure and unauthorized message duplication or replay

This will be achieved via use of secure channels of transactions (e.g., https, MPLS etc.) with controlled access to authorized users only. Wherever possible/feasible integrity checks will be implemented by use of Hashes, checksum etc.

10.1.4 Secure System Engineering Principles A.14.2.5

Principles for engineering secure systems around Security Foundation, risk-based principles, reduction in vulnerabilities etc. has been covered under various sections of this policy. The principles shall be regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats.

10.1.5 Secure Development Policy A.14.2.1

Secure development is a requirement to build up a secure service, architecture, software, and system. Following aspects shall be considered:

- Engaging Cyber Security team in every Project
- Establishing of Security Requirements in the Project
- Establishing secure access to code repositories
- Establishing security guidelines and compliance of the same
- Vulnerability assessment of the application and its remediation
- Periodic Review of remediation progress of the identified vulnerabilities

.

11.1.3 Security in Development and Support Processes

11.1.4 System change control procedures A.14.2.2

i. Changes to systems within the development lifecycles shall be controlled to ensure the integrity of system, applications, and products. Introduction of new systems and major changes to existing systems shall follow formal change management process.

ii. All changes to applications and software packages shall be as per defined Change Management Process

11.1.5 Technical review of applications after operating platform changes A.14.2.3

i. New releases pertaining to the operating platform shall be tested/reviewed before being implemented in the operational environment to ensure that there is no adverse impact on operation, application controls or security.

ii. The application controls shall be reviewed to ensure that they have not been compromised by the operating system/platform changes.

iii. It shall be ensured that notification of operating system/platform changes is provided in time so that appropriate tests and reviews are done before implementation.

11.1.6 Restrictions on changes to software packages A.12.5.1, A.12.6.2, A.14.2.4

i. Modifications to software packages shall be controlled, limited to necessary changes.

ii. Any required software change shall be done considering the risk with built-in controls and integrity process and compatibility with other software in use.

iii. Any requirement for change to such software shall be controlled and shall undergo the Change Management Process

iv. Access to production set-up/servers will be given to apps team for deployment in controlled way i.e., approval from Head Cyber Security

11.1.7 Secure development environment A.9.4.5, A.14.2.6

i. GPI shall establish and appropriately protect secure development environments for system development and integration efforts. Adequate measures shall be taken to limit the risk of information leakage.

ii. GPI shall assess risk associated with individual system development efforts and establish secure development environments for specific system development efforts considering:

- Sensitivity of data to be processed, stored, and transmitted by the system
- Applicable internal and external requirements from regulations and policies
- Degree of outsourcing associated with system development
- Need to segregation between different development environments and access control requirement
- Monitoring the change to the environment
- Backup are stored
- Control over movement of data; and

iii. Access to software program libraries, source code shall be restricted to authorized IT staff on a need-to-know basis. The updating, maintenance and copying of software program libraries shall be subjected to strict change control procedures.

11.1.8 System security and Acceptance testing A.14.2.8 and A.14.2.9

i. Cyber security team is engaged in software development life cycle.

i. It should be ensured that security vulnerability identified during development are addressed for any new system/functionality added in the environment.

ii. System acceptance testing shall include testing of information security requirements and adherence to secure system development practices for both in-house and outsourced developments. System acceptance testing shall be performed according to business requirements as well.

iii. New/upgrade/enhanced information systems shall undergo information systems acceptance test to ensure that they satisfy pre-defined documented acceptance criteria before being implemented in production environment.

11.1.9 Test Data A.14.3.1

10.3.1 Protection of test data

The software development team (whether in-house or outsourced) shall ensure that test data is secured and during testing.

11.1.10 Technical Vulnerability Management A.12.6.1

i. Cyber Security Team shall identify and document all technical vulnerabilities of information systems and evaluate the exposure to such vulnerabilities. Appropriate measures shall be taken to mitigate the associated risk.

ii. The IT Department shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability assessment and vulnerability closure.

iii. Timelines shall be defined to react to notifications of potentially relevant technical vulnerabilities. It is recommended to conduct technical vulnerability assessment of IT components on a yearly basis.

12. Incident Management A.16

An Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information and Information Systems of GPI. It is related to exceptional situations or a situation that warrants intervention of senior management.

An incident can be reported by anyone in the GPI's environment; however, it is typically reported by one of the following teams:

1. SOC Team / GPI Security Team through correlation of alerts from devices such as firewalls, IPS, Anti- Virus, DLP and SIEM etc.

2. GPI Security Team through detecting anomaly in network/ system behavior
3. Business users by observing suspicious transactions
4. Customers through suspicious transactions related to their accounts

Additionally, any employee or third-party employee of GPI can report any observed security incident by sending an email to Cyber Security Team / IT helpdesk/emailsecurity-gpi@modi-ent.com. While sharing the mail, person reporting the incident should mention time/date of observation, details/narratives available and contact information (optional).

Refer GPI Cyber Crisis Management Plan for more details

13. Business Continuity Management

The purpose of Business Continuity Management process is to reduce the impact of security failures to an acceptable level through a combination of preventive and recovery controls.

13.1.1 Information Security Aspects of Business Continuity Management A.17.1.1, A.17.1.2

i. A managed process must be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
ii. It is recommended to create a comprehensive Business Continuity Plan (BCP) to maintain/ restore business operations in the required time scales following interruption to, or failure of, critical business processes.
iii. Business Continuity Plan must be developed for critical business processes to deal with the likely disruptive events along with their probability, impact and consequences for information security identified through Business Impact Analysis.

13.1.2 Testing of Business Continuity Plans A.17.1.3

i. BCP must be tested annually to identify incorrect assumptions, oversights, or changes in equipment or personnel.
ii. Test results must be reported to IT Steering Council and takeaways must be incorporated in the next cycle of revision.
iii. BCP must be reviewed annually after each test and updated to ensure that the BCP considers the effectiveness of the current nature of business processes. Infrastructure personnel, etc.

13.1.3 Business Continuity Planning Framework

A framework of BCP must be maintained to ensure all plans, across businesses and processes are consistent, to consistently address Information security requirements, and to identify priorities for testing and maintenance.

13.1.4 Availability of Information Processing Facilities. A.17.2.1

i. The organization shall verify the established and implemented information security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.

ii. Redundant components or architectures shall be considered in case existing architecture is unable to ensure the availability of information processing system

iii. Redundant information systems shall be tested to ensure the failover from one component to another component works as intended

14. Compliance

14.1.1 Compliance with Legal requirements

14.1.2 Identification of applicable legislation A.18.1.1

All relevant statutory, regulatory, and contractual requirements, pertaining to the business, must be defined explicitly, and documented for each of GPI's information systems. GPI must ensure compliance to each of the Laws and Acts relevant to its operations. These must include but not be limited to the Information Technology Act (Amendment) 2008, Companies Act, or any other laws or acts applicable to the organization. The list of applicable legislations shall be reviewed and approved at least once a year or whenever there is a change in any statutory, regulatory, contractual obligations.

14.1.3 Intellectual Property Rights A.18.1.2

.

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

a. Compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be IPR.

b. IPR including software or document copyright, design rights, trademarks, patents, and source code licenses are not infringed.

c. Only licensed software shall be installed within GPI network environment. Record of all software licenses shall be kept and updated regularly.

14.1.4 Protection of Organizational Records A.18.1.3

i. The organizational records shall be maintained and stored in a secure manner to prevent any loss, destruction, or falsification.

ii. Data that is no longer required, or has satisfied their required period of retention, shall be destroyed.

iii. Respective functional heads shall ensure the retention of organizational records such as backup, log storage, books of account, etc. in accordance with legislative, regulatory, and contractual requirements.

14.1.5 Data protection and privacy of personal information A.18.1.4

Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses for each business.

14.1.6 Regulation of Cryptographic Controls A.18.1.5

i. Wherever applicable, legal advice must be sought to ensure compliance with national laws and regulations

ii. Cryptographic controls shall be used in compliance with all relevant agreements, laws and regulations.

14.1.7 Independent reviews of security policy and technical compliance

14.1.8 Compliance with Security policy and standard A.18.1.2

Managers/respective leads shall ensure that all security procedures within their area of responsibility are, carried out correctly to achieve compliance with GPI Information Security Policy

14.1.9 Technical Compliance Checking A.18.1.3

i. Information processing resources shall be reviewed immediately after installation and thereafter on a requirement basis.

ii. GPI information processing resources shall be reviewed by an independent third-party at least on an annual basis.

iii. All systems shall undergo information security compliance check on the completion of an upgrade or major system change

14.1.10 Information Security Audit Consideration A.12.7.1

14.1.11 Information systems audit controls A.12.7.1

i. GPI shall conduct audits through competent independent party to ensure compliance with the Information Security Policies. Formal procedures shall be developed for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.

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

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

iv. All information audit systems/ tools shall be protected to prevent their misuse.

v. Audit tests shall be limited to read-only access to software and data.

14.1.12 Protection of System Audit Tools

Access to system audit tools, i.e., software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

15. Compliance

All permanent employees, contractual employees and users of GPI owned resources must comply with this policy. Any employee found to have violated this policy may subject to suitable actions like training/mentoring/warning etc. as per the degree of violation mentioned in the ‘Disciplinary Process Policy’

The following processes are utilized to enforce compliance with this policy and supporting standards:

i. Monitoring: GPI shall employ appropriate technology/process solutions to monitor policy compliance.
ii. Security Audits: Internal Audit may assess the implementation and compliance with this policy as part of its internal audit program.