Information Security and Privacy Policy

Version 1.0

Date – 12/03/2020

Document Ownership – Chief Information Security Officer

genpact

Transformation Happens Here

NOTICE

Version Control

Version No.	Version Date	Type of Changes	Author	Approver	Date of next Review
1.0	12/03/2020	New Release	Sriram Lakshmanan	Ramachandra Hegde	11/03/2021

Contents

1 Introduction

Information Security and Privacy Policy aims to protect confidentiality, maintain integrity, and ensure availability of all information collection, storage, processing, transfer, and disposal, disclosure and retention/archival through its information systems along with protecting personal information and adherence to privacy requirements applicable to Genpact.

2 Applicability and Scope

All the employees, vendors/ third parties, contractors and consultants shall be committed to comply with the Information Security and Privacy Policy.

Please refer ISMS Scope document for detailed scope.

3 Policy Approach

Objectives	• Ensure adequate organizational and governance processes are in place to align information security objective with business and organization objectives; • Protect the confidentiality, integrity and availability of Genpact and its client's information; • Comply with applicable legal, statutory, regulatory or contractual obligations; • Identify and manage the risks pertaining to information assets through risk management; • Implement mechanisms to ensure that systems are in place to capture and investigate security incidents and to take adequate actions; • Ensure that all the personal information collected, processed and used at Genpact is adequately protected against threats and used for the identified business purpose in compliance with global data protection laws; and • Raise awareness of information security risks, information security and related policies and consequences of their non-conformance within Genpact
Policy Owner	Chief Information Security Officer
Access Restrictions	• View Access - All employees • Modify Access - Policy Author
Communication Plan	CISO/CISO designate shall communicate in case of any change
Storage & Retention Period	• Storage: Genpact Intranet Portal/Document Management repository • Retention period: Current year +2 years to 11 years (as applicable)
Exclusions	• Aspects relating to national sovereignty, national security and public policy. • Disciplinary actions resulting from wilful disobedience / non-compliance will be covered under specific policies, as applicable
Implementation	Information Security and Privacy Policy shall be implemented through domain specific and associated functional policies, procedures, standards and guidelines.

4 Organization of Information Security and Privacy

4.1 Internal Organization

- The organization of Information Security and Privacy system will be enforced by assigning the security roles and governing the implementation of security and privacy across the organization.

4.2 Roles and Responsibilities

- Information security and privacy roles shall be based on Information Security and Privacy Governance Structure defined in Information Security and Privacy framework;
- Information security and privacy processes and their responsibilities shall be identified and defined; and
- Information owners as per the framework shall be responsible for adhering security & privacy requirements of the information asset and for identifying & implementing the controls that are necessary to protect the asset.

4.3 Segregation of Duties

- Businesses and functions shall ensure that the same personnel in their team do not have responsibilities for multiple duties such that it could lead to the circumventing of existing security controls, and unauthorized or unintentional modification or misuse of the organization's assets;
- Segregation of duties is required so that no single user can subvert any security controls of the IT infrastructure / application that would adversely impact the business operations; and
- Segregation of duties review shall be performed by functional and business teams on a periodic basis.

4.4 Information Security and Privacy in Project Management

- Information Security and Privacy aspects shall be taken into consideration for all the projects including Mergers and Acquisitions;
- Global Information Security Team (GIST) shall ensure that information security risks are identified, addressed and reviewed regularly;
- Data Protection and Privacy office (DPPO) shall ensure that privacy risks are identified, addressed and reviewed regularly; and
- Information security and Privacy based risk assessment shall be conducted at an early stage of the project to identify Information Security and Privacy requirements at all phases including planning phase to the implementation and continuous operation phases.

5 Information Security and Privacy Policy

Information Security and Privacy Policy, which is based on the Information Security and Privacy framework demonstrates Genpact's commitment to information security and protection of information. It defines the leading practices across identified domains for ensuring security and privacy of information throughout the information life cycle at Genpact. This policy also sets out the minimum standard and shall guide all Genpact employees even if local law is less restrictive. Supplemental policies and practices shall be developed as needed to meet the local/industry specific data protection laws which may provide for stricter or specific privacy and protection standards than are set forth in this policy.

5.1 Policy Statements

Function specific policies shall be documented as per the policy statements identified in line with the requirements of all the Information Security and Privacy domains at Genpact.

- **Identity and Access Management -** Organization shall ensure authorized user access using secure and risk-based authentication methods to information and information processing systems, services and govern the life-cycle process of all types of identities.
- **Communication Security -** Organization shall ensure secured use of all communication channels for all employees, contractors, consultants, vendors and third parties operating behalf of Genpact.
- **Capacity Management -** Organization shall ensure that usage of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
- **Change Management -** Organization shall ensure that changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.
- **Human Resource Security** - Organization shall ensure that security is addressed during recruitment, employment and after termination or change of employment, of employees and external parties.
- **Information Security and Privacy Incident Management -** Organization shall establish adequate controls to ensure a consistent and effective approach to the management of information security and privacy incidents, including communication on Information Security events and Privacy breaches.
- **Log Management -** Organization shall establish adequate controls so that product functionality and audit logs recording user activities, exceptions, faults and information security events are produced and monitored.
- **Remote Working and Mobile Computing -** Organization shall establish adequate controls to reduce information security risks while working remotely using mobile devices.
- **Network Security -** Organization shall establish adequate control for the protection of information in networks and its supporting information processing facilities.
- **Password Management -** Organization shall establish adequate set of rules to create, manage and retrieve the password needed to access the information systems.
- **Threat and Vulnerability Management -** Organization shall ensure that information about technical vulnerabilities of information systems is timely obtained, exposure to such vulnerabilities is evaluated and appropriate measures are taken to address the associated risk.
- **Physical Security -** Organization shall establish adequate controls to prevent unauthorized physical access, damage, interference to the Genpact's information and information processing facilities.
- **Vendor Governance -** Organization shall ensure protection of information assets which are accessible by third parties / vendors.
- **Compliance Management -** Organization shall establish controls for adherence of legal, statutory, regulatory or contractual obligations (as applicable) related to information security, privacy and other requirements.
- **Media Disposal -** Organization shall outline adequate rule for the proper disposal of media (physical or electronic) to protect sensitive and classified information.
- **Clear Screen & Clear Desk -** Organization shall ensure that all business information used in work areas is secured from the risk of unauthorized access, loss or damage during /outside business hours or when areas are unattended.
- **Acceptable Usage -** Organization shall establish adequate controls to define the acceptable usage of internet, e-mails, systems, storage media, operating systems, application, software and business information.

- **Anti-Malware -** Organization shall implement an anti-malware solution to ensure prevention, detection and removal of potential viruses and malware and thereby protect the confidentiality, integrity and availability of information systems.
- **Asset Management -** Organization shall ensure protection of its information and information assets by establishing adequate controls to addresses security issues with regards to asset management, classification, handling and labelling of information assets.
- **System Acquisition and Development -** Organization shall ensure that the security requirements are considered and implemented for the acquisition, development and enhancement of information systems and applications throughout the complete lifecycle.
- **Cryptography -** Organization shall ensure the confidentiality and integrity of sensitive information at rest and/or in motion in information systems by using suitable encryption technology.
- **Backup & Recovery -** Organization shall ensure the availability of critical business information by conducting periodic backups such that information is available for restoration of business operations when needed in the event of disasters or system failures.
- **Business Continuity Management -** Organization shall define, implement, test and maintain practical continuity plans to recover and restore interrupted critical services (s) or function(s) to an acceptable level within a predetermined time after a disaster or extended disruption or security failure.
- **Cloud Security -** Organization shall ensure that the provisioning of cloud service(s) is in accordance with the business, information security, legal and regulatory requirements to preserve the CIA values of information processed or transmitted by cloud computing provider.
- **Social media -** Organization shall define a set of rules for employees, contractors, consultants, vendors and third parties who post content on the Internet either as part of their job or as a private person while in association with Genpact.
- **Work from Home -** Organization shall define set of rules to control remote access and safeguard information systems from unauthorized access while working remotely from home.
- **BYOD -** Organization shall ensure the use of personal smartphones, laptops and tablets in a controlled restricted environment to minimize risk of unauthorized access or disruption.
- **Data Privacy -** Organization shall define set of controls to collect, processes, transfer and retain personal data in compliance with global data protection laws and regulations.
- **Document management** – Organization shall ensure that all the documents are created, managed, refreshed and made available to stakeholders throughout the organization in accordance with predefined set of rules.

6 Risk Assessment

Risk Assessment is to be carried out on a periodic basis to ensure risks are identified and treated. The potential impact on Information Security and Privacy shall be assessed whenever new processes are implemented or when significant changes are made to such processes. Measures to address the Information and Privacy risk is to be aligned with the Genpact risk assessment methodology.

7 Awareness and Training

Genpact shall develop and implement awareness and training program to educate Employees, Vendors/Third Parties, Contractors and Consultants around securing the information system thereby ensuring the security & privacy of information.

8 Monitoring and Measurement

Genpact shall monitor and measure the Information Security and Privacy performance and effectiveness of Information Security and Privacy Policy as per defined KPIs and metrices.

9 Internal Assessments

Genpact shall ensure that the Information Security and Privacy internal assessments are conducted regularly to determine whether the Information Security and Privacy policy:

- Has been properly implemented and is maintained;
- Is effective in meeting the Genpact information security and privacy requirements; and
- Provides information on the results of the internal assessment to the management.

10 Policy Compliance

All business and support functions shall be responsible for adhering and maintaining requirements defined in Information Security and Privacy policy and all other domain specific and associated functional policies. Any individual or businesses affiliated with Genpact having access to the Genpact's information assets and system shall adhere to this policy. All information systems shall be designed to comply with this policy.

11 Review and Change

The Information Security and Privacy Policy will be reviewed annually, at a minimum. However, the policy can be subject to updates depending on the various triggers and their impact on Genpact's Information Security & Privacy posture.

12 Policy Deviations

Any deviation to this policy shall be treated as per the Genpact Infosec Exception Management Process.

13 Policy Violations

Violations of this policy may include, but are not limited to any act that:

- Does not comply with the requirements of Information Security and Privacy Policy or related policies;
- Exposes Genpact to actual or potential loss through the compromise of Information Security and Privacy;
- Involves the disclosure of confidential information or the unauthorized use of Genpact' s information;
- Loss of confidentiality or disclosure of Genpact and client sensitive information assets; and
- Violates any applicable laws or contractual commitments of Genpact.

Failure to comply with the Information Security and Privacy Policy shall result in appropriate disciplinary actions as per CAP policy.

14 Annexure

14.1 Document Reference List

Please refer to the ISMS Master List of Documents.

14.2 Abbreviations

Please refer this Link.