Section 1. Introduction

1.1 Overview

- Information Technology is embedded in various mission-critical operations and remains a key business enabler for GUST to achieve its strategic objectives.
- The infrastructure, systems and applications used in supporting various business services are part of GUST information assets. The protection of GUST information assets from various risks and threats, is critical to the organization and requires a robust Information Security Management System to preserve the Confidentiality, Integrity and Availability "CIA" of GUST information assets.
- This policy demonstrates GUST management's intent for information security and their expectations towards implementing and maintaining an effective management system to protect its information assets and establish a secure work environment.
- The Information Security Policy has taken into consideration strategic business drivers and objectives and is aligned with ISO 27001 standard.

1.2 Purpose

- The objective of the Information Security Policy is to articulate management's intent and direction to ensure adequate protection of GUST information assets in a practical and effective manner.
- The Information Security Policy aligns with GUST strategic business objectives through addressing the key objectives of protecting the CIA (Confidentiality, Integrity & Availability) of the information assets affecting and supporting GUST business operations:
    - **Confidentiality** - property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
    - **Integrity** - property of accuracy and completeness.
    - **Availability** - property of being accessible and usable upon demand by an authorized entity.

1.3 Scope

- This policy applies to all computer and data communication systems owned by and/or administered by GUST. This document does not limit itself to information handled via computers and/or networks, and includes e-mail, Internet access and all forms of transmission.

1.4 Applicability and Compliance

- This policy shall apply to all students, employees, contractors, and visitors of GUST.
- Violations of this policy will result in corrective action being taken by the management.
- Violators shall be subject to disciplinary action taken by the Human Resources Department, consistent with the severity of the incident as determined by an investigation conducted by IT management.

1.5 Ownership

- The Information Security Officer of GUST owns this Information Security policy and is responsible for maintaining the relevance of the policy on a continuous basis.
- The policy shall be internally reviewed every year by the Information Security Officer.
- Any revision to the Information Security policy shall be approved by the IT Manager and the University Senior Management.

1.6 Exception

- Exceptions to any part of this policy are only permitted if the IT Manager authorizes exclusions approved by University Management due to unique circumstances.
- Requests for exceptions must be made in writing to the IT Manager stating the business need and unique circumstances requiring an exception. Exceptions shall be granted on a case-by-case basis.

1.7 Definitions

Definitions	Description
Audit	Audit is a planned and documented activity performed by qualified personnel to determine by investigation, examination, or evaluation of objective evidence, the adequacy and compliance with established procedures, or applicable documents, and the effectiveness of implementation.
Access Control	Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.
Antivirus	Software that is designed to detect, protect, and remove viruses, worms, trojans, and any malicious software.
Backup	Backup or the process of backing up refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.
Confidentiality	Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.
Encryption	Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data by encoding and transforming information into unreadable cipher text.

Definitions	Description
Email System	An email system, email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages.
Integrity	Integrity refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification.
Information Systems	IT Resources include Servers, Desktops, Workstations, Laptops, Mobile Devices, Network Devices, Security Devices, Wireless Devices, Databases, Operating Systems, and Application Software.
Media	Computer Media, often called storage or memory, is a technology consisting of computer components and recording media used to retain digital data.
Malicious Content	Malicious Content or Code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.
Non-repudiation	Nonrepudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption etc. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
Network Security	Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves authorizing data access in a network, controlled by the network administrator.
Policy	Policy is a set of rules issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the information's security.
Password	A password is a basic security mechanism that consists of a secret pass phrase created using alphabetic, numeric, alphanumeric, and symbolic characters, or a combination. A password is used to restrict access to a system, application, or service to only those users who have memorized or stored and/or are authorized to use it.
Patch	A patch is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.

Definitions	Description
Security Incident	An information security incident is made up of one or more unwanted or unexpected information security events that could compromise the security of information and weaken or impair business operations.
User ID	User identification (user ID) is a logical entity used to identify a user on software, system or within any generic IT environment. It is used within any IT enabled system to identify and distinguish between the users who access or use it.
Virus	A computer virus is a type of malware that, when executed, replicates by inserting copies of it (modified) into other computer programs, data files etc. Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing confidential information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.

Section 2. Information Security Policy

2.1 Information Security Risk Management

- The risk assessment methodology followed shall be in accordance with the international best practices (e.g., ISO 31000, ISO 27001, NIST 800-39).
- Risk tolerance levels shall be specified and determined based on GUST's priorities and objectives.
- The risk assessment shall be conducted annually, or whenever:
    - New products and technologies are introduced.
    - There is a notable change in technology, business, or operations-related processes.
    - New material risks are detected.
    - New third-party agreements are signed.
- A range of threats and associated vulnerabilities shall be identified and analysed with consideration of the environments in which the risks exist.
- The identified information security risks shall be documented in a risk register.
- A risk owner shall be assigned for each relevant risk. The likelihood and impact shall be evaluated for each identified risk to determine the priority and required resources for a risk response / treatment.
- The Information Security Officer shall ensure that risks documented in the risk register translate into risk response plans.
- Risk treatment responses shall be analyzed and prioritized based on effectiveness, cost, and required efforts.
- Risk treatment plan shall categorize the risk response strategy (e.g., risk acceptance, risk avoidance, risk mitigation, transfer, etc.).
- Risk response strategy shall be tracked and managed. Risk acceptance, avoidance, or transfer cases and the basis for categorization shall be documented and approved.
- The applied responses shall be monitored to track compliance, ensure effectiveness of risk mitigation controls, and ensure their operation has not led to the introduction of new risks.
- The Information Security Officer shall regularly report to the management on the status, exposure, resolution and status of the security gaps and risks open within the organization.

2.2 Information Security Compliance

2.2.1 Information Security Compliance

- All users must be familiar with the policies drawn up and should comply with the Information Security policy.
- All users are required to read, understand, and comply with the Acceptable Usage Policy and other related policies and procedures. If any user does not fully understand the underlying of these policies, he/she should consult with the Information Security Officer.
- To achieve compliance with GUST information security policy, the respective department must ensure all security procedures within their area of responsibility are carried out correctly.

- To monitor and enforce compliance with this policy, GUST shall conduct an ongoing program of security reviews, system monitoring and independent audits.
- Implemented security measures shall be periodically reviewed and when necessary adjusted, to ensure they remain effective and cost-efficient.
- GUST must identify and review regularly the requirements for confidentiality or non-disclosure agreements to reflect the organization's business and operational needs.
- GUST shall sign confidentiality or non-disclosure agreements as part of the hiring contract and code of conduct with employees before granting access to sensitive information or information processing facilities.
- GUST shall sign confidentiality agreements with third-party organizations/ users as part of the contractual agreement and NDAs before granting access to sensitive information or information processing facilities.

2.2.2 Copyright and Software Licensing Legislation

- Copying of copyrighted material is a breach of law. Infringement of copyright is a criminal matter. The following are guidelines in this regard:
    - Lack of familiarity with copyright laws may result in inadvertent breaches of it, which may lead to potential legal action.
    - A failure to adhere to the legal requirements relating to software licensing can result in legal action against the user as well as GUST.
    - This policy also adheres to the protection of information copyrights regarding any contractor's or consultant's copyrighted materials.
- Copying and distributing copyrighted software is illegal unless the owner of the software expressly grants permission. The following issues are to be considered when implementing the policy:
    - Unless GUST has a license from the owner of the software to copy and distribute computer software, copying and distribution is not permitted.
    - Software should not be copied and distributed across the computer network. This illegal activity threatens GUST integrity as it may result in legal action against GUST.
    - Use of unlicensed software by contractors and consultants on GUST premises could result in legal action against GUST.
    - Software licenses should be kept in safe custody. If required they should be produced for inspection, otherwise GUST may be subjected to the risk of fines and possible reputation loss.
    - Strong internal controls should be implemented. Otherwise, it may result in the maximum number of permitted users being exceeded. Even a single excess copy places GUST at risk of prosecution under copyright laws.
    - The Information Security Officer shall obtain legal advice on the requirements and legislation governing intellectual property rights and software licensing.
    - Resale of old or redundant computer equipment can result in infringement of the copyright law, as software license agreements may not be transferable, so all the software on the storage media should be expunged.
    - Shareware software should not be used beyond its evaluation period.
    - Cracking or breaking the licenses of software is also a violation of copyright law.

2.3 User Access Management

2.3.1 Access Management

Access to any Information/System shall NOT be provided to anyone unless:

- The access is essential to perform official responsibilities for GUST and shall be in line with the roles and responsibilities of the user and business requirements.
- A specific authorization request (wherever applicable) is duly filled in by the user and his access to the system is authorized by the system owner.
- The person is a current, regular, contractual or temporary employee of GUST, or the person is designated by GUST having a contractual binding with GUST for providing services that require access to the Information Systems.
- Audit trail and related documents for User Access Management (i.e., Creation, Modification, Revocation, Deletion, and Suspension of Users) shall be maintained and reviewed to ensure that no unapproved/unauthorized access has been granted.
- Information about the User e.g., Name, Department, Designation, Contact Number, Purpose and Time of Access etc. shall be stored in the system or in any easily accessible manner.
- The User and the Information Owner shall be provided with the detail of access rights associated with the 'User ID'.
- Every user shall be assigned a unique 'User ID' and no two users shall be allowed to share the same 'User ID'.
- Users provided with the unique 'User ID' account shall be responsible for the activities carried out using that account.
- The organization shall ensure that access to the information / Information Systems is granted through pre-defined User Profiles/Roles.

2.3.2 Access and Information Classification

- The organization shall ensure that access granted to the information is in line with the Information Classification e.g., granting access to 'Confidential' Information shall require authorization from respective management and scrutiny of business need.
- The access to the information or Information systems shall be provided on a 'need to know' basis, i.e., the access shall not be more than required to perform official responsibilities.
- No user shall be allowed to gain unauthorized access through a 'User ID' not explicitly assigned to that user.

2.3.3 Segregation of Duties

- A Segregation of Duties (SoD) Matrix for every system (e.g. Application, Database, Operating System, Technical Solution, etc.) shall be developed to indicate the positions where conflict of interest may arise, if access of any distinct function is granted to same Person/Group/Department.
- The access shall be granted by ensuring Segregation of Duties to avoid 'Conflict of Interest'.

2.3.4 Privileged Users

- The default privileged 'User ID' such as "root", "Administrator", "System" and other similar user accounts shall not be provided to anyone (including System/Application/Database Administrators) on a permanent basis.
- The privileged users requiring Super-User/Administrative access shall be created with a separate User ID provided to individual system admin/Database administrator/network administrator. The individuals who are assigned with high privileged administrative access are accountable for activities carried out using the user account.
- Administrative User ID shall not be used for routine activities. Whenever a need arises, the default Super-User/Administrative ID shall be provided for specific tasks with the approval of the Information Security Officer. After use, the password shall be changed and stored securely.
- Default passwords of highest privileged accounts like 'Super User', 'Root' and 'Administrator' shall be changed as soon as the system becomes operative.
- Passwords of built-in administrator and other highest privileged system, application and database accounts are to be sealed and kept securely in an envelope or in Password Safe with the Information Security Officer. On change of these passwords, the new password shall be given to the Information Security Officer in a sealed and dated envelope or updated in Password Safe.
- In case of an emergency, the passwords that are stored in the envelope shall be accessed after getting permission from the Information Security Officer.
- A register shall be maintained to log details of use of sealed passwords.
- Once the sealed password is accessed by an IT staff, password shall be changed by the concerned person and sealed and kept with the Information Security Officer to be stored securely.
- Privileged access to IT infrastructure such as server operating systems, database and network administration are allowed only for GUST IT Department personnel upon authorization by the Information Security Officer. End-users are allowed privileged access to application-level only.

2.3.5 Temporary Accounts

- Temporary Accounts may be created for the purpose of providing predetermined file and / or application access on short notice for the use of a Temporary Employee.
- The rules applied for a Regular Employee shall be applicable for the temporary access but with assignment of start date and end date as appropriate.

2.3.6 Access Revocation

- The access to the Systems shall be revoked as soon as the user is not required to perform the official duties for GUST.
- The access to the System shall be revoked in a manner so that it is possible to track the history of activities performed by the user.
- Users shall be disabled from all Systems as soon as their services are terminated from GUST because of resignation, termination, retirement, contract termination, etc.

- In case of transfer of the Users to other departments/functions, their 'User ID' shall immediately be disabled from all Systems that are not required for discharging the new responsibilities.

2.3.7 User Account Reviews

- User access rights shall be reviewed by the System/Business Owners at least once annually and after any major change in the systems or in the User profiles which may include Creation, Modification, Suspension and Revocation of User Accounts and related profiles.
- Privileged User IDs shall be reviewed once in six (6) months.

2.4 Password Management

- All User-level passwords shall contain at least 8 alphanumeric characters.
- All privileged accounts shall contain at least 16 alphanumeric characters or use two-factor authentication.
- All service accounts shall contain at least 21 alphanumeric characters.
- The password shall be case sensitive and shall contain the combination of upper and lower case (e.g., a-z, A-Z).
- The password shall have at least one special character e.g., 0-9,!@#$%^&*()_+|~- .
- Systems shall be configured to ensure that the initial, temporary passwords for newly allocated accounts are changed at the first logon.
- Default vendor passwords shall be changed immediately, following the installation of software or hardware.
- Passwords shall not be displayed on the screen when being entered, and the password verification file is to be stored separately from the main application system data. Passwords stored in this file shall be stored in encrypted form.
- A "User ID" shall not be used as a password (either as it is, reversed or in upper case).
- First, middle, or last names of user shall not be used in passwords, as they are easily guessed.
- The password shall not be a word found in dictionary or a country name or organization's name.
- The passwords shall not be personal information such as family name, birth date, initials, names of family members, etc.
- All User-level accounts passwords (e.g., email, web, desktop computer, etc.) shall be changed every ninety (90) days.
- Users who are assigned accounts with privileged permissions (e.g., domain administrators, database administrators, application super users, etc.) shall change the passwords of those accounts every 90 days or shall use two-factor authentication.
- Password history shall be enforced for a minimum of five iterations i.e., during password change users shall not be allowed to reuse the last five passwords.
- User accounts shall be locked after no more than 5 failed attempts to access the system.
- All local administrator accounts shall be managed by Microsoft Local Administrator Password Solution (LAPS).

2.5 Remote Access

- The IT department shall ensure that VPN is used while remotely accessing GUST network via public telecommunications network or Internet. Furthermore, GUST shall ensure that necessary security measures are adhered to during access to GUST network using VPN.
- It is the responsibility of employees and contractors with remote access/VPN privileges to ensure that unauthorized users including Family Members are not allowed access to GUST internal networks. At no time should any employee provide his or her login or email password to anyone, not even family members.
- Employees and contractors with remote access/VPN privileges to GUST internal network must not use non-organization email accounts or other resources to conduct business, thereby ensuring that official business is never confused with personal business.
- VPN use is to be strictly controlled using domain password authentication as mentioned in Section 2.4 Password Management.
- When actively connected to the internal network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- VPN gateways will be set up and managed by the IT department.
- All computers connected to GUST internal networks via VPN, or any other technology must use the most up-to-date anti-virus software that is the corporate standard.
- VPN users will be automatically disconnected from GUST network after thirty minutes of inactivity. The user then logs on again to reconnect to network. Pings or other artificial network processes are not to be used to keep the connection open.
- While using VPN technology with personal equipment, users must understand that their machines are a de-facto extension of GUST network and as such are subject to the same rules and regulations that apply to organization-owned equipment, i.e., their machines must be configured to comply with GUST Security Policies.
- Access to VPN will be removed, if 90 days have elapsed from the last successful login. Once access is removed, a user will be required to go through the approval process to regain access.
- All VPN access shall be logged as per Log Management Policy.
- Only GUST-owned equipment is permitted to connect to GUST network for remote access via VPN.
- Non GUST-owned devices can be granted remote access via secure methods, with prior approval from the Information Security Officer.

2.6 Mobile Device Security

- End Users are expected to use the computing devices (e.g., desktops, laptops, mobiles) that are assigned to them to carry out their business activities. Users are generally not allowed to use computing devices that are assigned to others. If there are business needs to temporarily use another user's assigned device, permission to do so must be granted by the original device user or by their department manager.
- The portable device shall be tagged to a unique employee or third-party vendor staff.
- Users shall ensure that their portable computing devices are configured with auto-lock and protected with a password or pin to prevent unauthorized access.

- Users shall not attempt to modify their computer hardware or install additional parts to their computers. Any such modifications must be made only by authorized IT staff after proper request and approval from the IT department.
- Users shall not install or execute any software on GUST computing devices without prior review and approval by the IT department.
- Installation or use of illegal or pirated software on GUST computing devices is prohibited.
- Portable devices shall be permitted to connect to the enterprise network after necessary authorization.
- GUST employees and third-party suppliers shall not connect personal equipment to GUST corporate network without prior authorization.
- All portable devices that are connected to the enterprise network shall be monitored.
- Only computing devices owned and managed by GUST must be used by employees working remotely from GUST premises for GUST business purposes.
- All teleworkers must use appropriate measures to maintain the information security of information assets and must always follow the agreed information security policy.
- User access to GUST data on portable devices should be based on least privilege principle with appropriate approvals.
- Users shall ensure that their laptops and other mobile devices are carried in their possession as hand luggage when travelling to prevent damage or loss of such items.
- If a GUST provided computing or communication device is lost or stolen, the user assigned the device shall promptly report the incident to IT Help Desk for proper action and precautionary measures.
- Users are required to store business-based documentation on the server/cloud and are enforced to refrain from storing it on the local drive.
- Confidential data must not be stored on mobile data storage devices.
- When allowing third-party mobile computing devices or personally owned devices to the network, the following checks shall be performed and authorized as per GUST approval process:
    - Concerned users should be informed about the GUST Information Security Policy and corresponding policies.
    - Scanning the devices for malicious code, software, and applications
    - Scanning the devices for antivirus updates
    - Scanning the devices for critical software updates and patches
    - Scanning for unauthorized software
    - Disabling unnecessary hardware (e.g., wireless, modem connections, USB ports etc.).

2.7 Security Awareness and Training

- The Information Security Officer shall arrange for and conduct information security awareness programs for all interested parties who have access to GUST information systems and information assets. These awareness programs are to enable GUST to improve the security posture by imparting knowledge and common understanding among all interested parties to safeguard information assets through a security-conscious environment.
- Skills and Competency requirements including Qualification, Experience and other special Skills required for each role shall be identified and documented by the Information Security Officer.
- The Information Security Officer shall also assess the existing skills among the staff identified against various information security roles and identify the skills gap assessment report.
- A comprehensive training and awareness program addressing the requirements, based on the skills gap report, for all information security roles shall be formulated.
- Security training requirements shall be prepared based on the training and awareness program and submitted to GUST IT Management for consideration in the annual training plan.
- Periodic information Security awareness and education shall be conducted for all GUST employees.
- The awareness sections shall cover information security basics, associated policies and procedures and employee responsibilities.
- Information security awareness and education material shall be made available for all Employees who have access to GUST Information Systems and Information Assets.
- Training and Awareness evaluation methods and criteria for measuring the effectiveness of information security training shall be formulated.
- Managers and Team Leaders shall evaluate the training requirements of their staff members and recommend appropriate training to improve the efficiency and effectiveness of the staff members.
- Training records shall be maintained by respective Managers and HR Department.

2.8 Malware Protection

- The IT Department shall evaluate, install and maintain anti-virus software and/or tools for use on all desktop computers, laptops, servers and other computing devices.
- The anti-virus software cannot be un-configured for ease of user's motivation. Users may not bypass scanning processes that could arrest transmission of computer viruses and malware.
- Updates to the antivirus and anti-malware programs from a central server shall be automatic.
- The antivirus product shall be operated in real time on all servers and client computers.
- New Antivirus definitions/signature shall be applied when released by the vendor.
- Routine Antivirus scanning of all files and executable shall be enforced daily on all GUST key Information Systems.

- All users are responsible for taking reasonable measures to protect against malicious infection.
- Any willful activities with the introduction of computer viruses or disruptive/destructive programs into GUST network environment are strictly prohibited, and violators may be subject to disciplinary action.
- The IT department shall ensure that appropriate detection and prevention measures are implemented at key network locations to protect the organization against risks introduced by malicious code/malware programs.
- All Windows-based computers (clients and servers) connected to the organization's IT infrastructure or networked resources shall have organization-supported antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network.
- All critical systems (server, desktops, and laptops) shall be installed with the latest anti-virus software and EDR (Endpoint Detection and Response) solution.
- The IT department shall maintain virus detection programs on personal computers used to store confidential or sensitive information or to run critical applications.
- The IT department reserves the right to disconnect any machine from the network if an infection is found or suspected. The machine will be disconnected until the infection is removed.
- Any activity intended to create and/or distribute malicious programs onto GUST network (e.g., viruses, worms, Trojan horses, etc.) is strictly prohibited.
- If an employee receives what is believed to be a virus, or suspects that a computer is infected, the incident shall be reported to the IT Help Desk immediately.
- No employee shall attempt to destroy or remove a virus, or any evidence of that virus, without direction from the Information Security Officer.
- Any critical changes concerning Antivirus Software and configuration settings shall follow the change management process.
- All drives to the computer shall be disabled. Exceptions shall be approved by the Information Security Officer. All these drives shall be included for virus scanning.
- All removable media (e.g., CD, USB and others) shall be scanned for viruses before being used.
- Virus scanning results shall be logged, automatically collected, and audited by Antivirus Software Administrator and quarterly verified by the Information Security Officer.
- Logical access to the Antivirus Software for servers shall be restricted to the authorized personnel only.
- Logging shall be enabled on the Antivirus Software servers.
- The e-mail server shall have the antivirus program installed and shall check all e-mail attachments before sending them to individual mailboxes.
- Antivirus software shall be configured such that all content downloaded from the Internet is automatically checked for viruses.
- Managed Service/Third Party personnel shall not be allowed to connect Information Systems to GUST network without updated Antivirus Software with appropriate settings.

2.9 Security Incident Management

2.9.1 Security Incident Detection

- Whenever a security incident, such as a virus, worm, spam / hoax email, discovery of hacking tools, altered data and similar incidents is suspected or confirmed, the appropriate Security Incident Procedures shall be followed.
- The Information Security Officer shall determine if GUST IT or GUST corporate-wide communication is required, what constitutes the content of the communication, and how best to distribute the communication.
- In the case where law enforcement is involved, GUST Legal Department will act as the liaison between law enforcement and GUST IT.

2.9.2 Roles and Responsibilities

- The Information Security Officer is responsible for:
    - Communicating the security incident to the IT Manager and initiating the appropriate Incident Management action including service restoration if required.
    - Determining the physical and electronic evidence to be gathered as part of the Incident Investigation. and
    - Initiating, completing, and documenting the security incident investigation.
- The Information Security Officer, along with the technical teams, is responsible for:
    - Monitoring and ensuring that any damage from a security incident is resolved or mitigated and that the vulnerability is eliminated or minimized where possible.
    - Communicating new issues or vulnerabilities to the system Vendor and working/ coordinating with the Vendor to eliminate or mitigate the vulnerability.
- The Information Security Officer is responsible for communicating with GUST Legal Department for coordinating with any Third-Party Organizations and Law Enforcement Agencies.
- In the case where law enforcement is not involved, the Information Security Officer along with GUST IT Management / HR Department or any other relevant Department shall recommend disciplinary actions, if found appropriate.

2.9.3 End-User Responsibility

- Any person using GUST information resources has the responsibility to report suspected hardware or software security incidents to their supervisor and/or IT Help Desk.
- All GUST Employees, GUST contractors and third-party users shall be made aware of their responsibilities to report any Information Security Incident as quickly as possible.
- IT Help Desk can be notified by email, phone or raising a ticket on the tool and shall take the appropriate action to help the person stop/prevent an attack and return the system/ machine to operating condition. Information Security Officer shall investigate the security incident to determine what further action needs to be initiated, if any.

2.9.4 Security Incident Categorization

- A security incident shall be categorized. While determining the level of incidents, the following factors need to be considered:
    - Financial impact.
    - Credibility impact.
    - Impact to GUST's image.
- All the security incidents shall be classified in the following categories:
    - System downtime or unavailablility.
    - Logical security breaches.
    - Physical security breaches.
    - Security policy violations.
    - Virus incidents.

2.9.5 Security Incident Prioritising

- GUST IT shall respond effectively whenever a security incident occurs. In order to minimize the effect of critical security incidents, and to have a coordinated response, all security incidents shall be reported to IT Helpdesk. Emergency and critical security incidents may also be reported to Tier 2 support teams directly for immediate remedial action in coordination with the Information Security Officer. In all cases, concerned IT support personnel shall report such security incidents to the Information Security Officer at the earliest possible time.
- Security incidents shall be prioritized and following are the priorities that the management should consider for responding to the security incident:
    - Priority one (P1) – protection of human life and people's safety, and incidents affecting GUST public image / reputation.
    - Priority two (P2)– protection of classified and/or sensitive data of systems, networks or sites.
    - Priority three (P3) – prevention of damage to systems (e.g., loss or alteration of system files, damage to disk drives).

2.9.6 Security Incident Handling

- GUST IT shall ensure that all Security Incidents reported shall be addressed with appropriate steps to contain the impact of the incident.
- Information Security Officer shall analyze the cause and the impact of the incidents and recommend appropriate measures to contain the damage and remove the cause of incidents.
- An escalation process shall be developed for the incidents that are not resolved.
- All high-risk Security Incidents shall be communicated to IT Manager.
- The Business Continuity Plan of GUST shall be invoked in case significant damage has already been caused by an incident.
- The information regarding the security incidents shall not be shared with any external parties without approval of the IT Manager.
- The incident shall be closed only after ensuring that the services has been resumed to normal and all causes of the incident in future.

- The cause of the incident shall be analyzed and system vulnerabilities shall be removed to avoid the incident in future.
- Every step taken, from the time the incident was detected to its final resolution and closure, shall be documented and time-stamped along with the collected evidence.

2.9.7 Collection of Evidence

- Information Security Officer shall identify the cause for a security incident, collect evidence and appraise its impact on GUST's Information systems and data. The Information Security Officer shall consider following points / items while collecting the evidence:
    - Evidence for security breaches are collected if security incident causes a breach with statutory, regulatory or contractual obligations, criminal or civil law. and
    - Evidence collected have to be evaluated according to their particular circumstances, and this may, or may not, require various departments to be involved.

2.9.8 Security Incident Recovery Action Plan

- The respective manager(s) shall prepare the corrective action plan for the security incident. The action plan, though specific to each case, shall typically cover the following:
    - Particulars about the operating unit, location, date and time.
    - Facts and explanation / reasons for the incident.
    - Other business units affected.
    - Corrective action to be taken.
    - Estimated cost of implementing the corrective action.
    - Estimated time frame, start date and end date. and
    - Personnel responsible for taking the action.

2.9.9 Monitoring

- Security incidents related to critical information assets, IT equipment and facilities shall be reviewed and monitored by the concerned manager(s), responsible personnel and the Information Security Officer.
- The findings shall be discussed in the management meetings. The magnitude and criticality of the security incidents may prompt the concerned manager(s) and Information Security Officer to discuss and take actions on the security incidents immediately instead of at fixed intervals with the management.

2.9.10 Documentation and Reporting

- The Information Security Officer shall maintain a central database of all such security incidents. After analyzing the extent of analysis and facts about the security incident, the Information Security Officer shall appraise the top management.
- The same shall be formally documented along with relevant evidence collected or observations.

2.9.11 Learning from Security Incidents

- Based on the documentation and reporting, the Information Security Officer shall identify recurring or high impact security incidents or malfunctions and shall perform root cause analysis and implement additional controls to limit the frequency, damage and cost of future occurrences. The information shall be used to spread awareness across the organization in order to avoid the recurrence of such security incidents.

2.9.12 Examples of Security Incidents

- Loss of service, equipment or facilities
- System malfunctions or overloads
- Human errors
- Breaches of physical security arrangements
- Uncontrolled system changes
- Access violations
- Successful hacking attempts
- Virus incidents involving e-mail, Internet, USB and other media
- Malfunctioning of systems, software or hardware
- Misuse of IT resources
- Power problems
- Natural calamity or disaster
- Suspicious activities
- Non-compliances with policies and guidelines

2.10 Log Management

- Logging features shall be enabled for all the critical devices including Application Servers, Network Devices, Security Devices and other such system software components.
- The information access like User login, logout, login failure, password change, etc. shall be logged and reviewed.
- The activities performed through privileged 'User ID' shall be logged and monitored.
- At a minimum, the following types of events/incidents shall be logged:
    - Start-up and shutdown.
    - User / Object Authentication.
    - Authorisation/permission granted.
    - Access failure.
    - Unsuccessful attempt.
    - Deletion of system files, User-IDs and other critical system utilities and routines.
    - Failure or overriding of validation and verification points.
    - Establishment of remote network connection.
    - Transfer of Classified Data / Information.
    - Changes to system configuration.
    - Output to removable media.
    - Output to a printer.
    - Administrator's activities.
    - Errors/exceptions.

    - All denied attempts to any port, protocol or service shall be logged.
- The appropriateness of log configuration shall be reviewed at regular intervals in light of actual type of incidents/events that happen from time to time.
- Where appropriate, logging systems and log files shall be monitored on an ongoing basis considering the system criticality to safeguard against unauthorized changes and operational problems such as:
    - The security logging facility is being deactivated.
    - Alterations to log file contents (accidental or intentional modification) or to dates and times of log files or individual entries.
    - Deletion or renaming of log files.
    - Exhaustion of log file space, thereby causing records to be discarded or overwritten.
- Dedicated team shall be assigned to monitor the generated log files, this is including privileged operation and activities logs.
- Periodic review and verification should be carried out by the Information Security Officer on the monitoring and reviewing status of critical logs events.
- A separation of roles should be considered between the person(s) undertaking the review and those monitoring the logs.
- Relevant message types shall be transferred automatically to a centralized secure logging system where information from multiple sources may be correlated and analyzed in order to help identify significant events for security monitoring purposes
- All system clocks shall be synchronized to ensure the accuracy of the logged events.
- Centralized log server shall be deployed for collecting, storing and analyzing the logs generated by the servers, network and security devices.
- The Information Security Officer shall make necessary arrangement to analyze the critical logs for activities that affect the security of the system.
- Unauthorized activities identified during the log reviews shall be reported to the Information Security Officer.
- All security logs shall be maintained online for at least 1 year and no one shall be allowed to disable, modify, or delete the logs without formal permission from the Information Security Officer. The logs should be backed up and maintained as per the retaining period and kept off-site or in a fireproof cabinet.
- Administrator activities shall be logged across all the servers and devices and Administrator logs shall be reviewed periodically by the Information Security Officer.
- Administrator logs shall never be deleted and due to need of system space, shall be archived and kept in the possession of the Information Security Officer.
- The log of issuance of the privileged user passwords shall be maintained and reviewed along with the purpose of issuance.
- The audit log shall bind the individual ID of the user causing (or associated with) the audited event to the audit record for that event.
- The audit facility used by the application shall ensure that the application's audit records are protected from deletion or unauthorized modification.
- It shall be ensured that the Domain/Authentication server is configured to log hostnames or MAC addresses for all clients and logs are stored online for 30 days and offline for one year.

- Logs for security devices such as Firewall, IPS, IDS, and Web filters shall be reviewed on a daily basis.
- The audit trail events shall be stamped with accurate date and time, and shall include source IP, destination IP, protocol used, and action taken.
- Operational logs and fault logs stored in soft copy shall be backed up daily. Periodically these logs shall be archived. The frequency of archiving depends on business needs.
- Periodic review and verification shall be carried out by the Information Security Officer and on the monitoring and reviewing of critical logs.

2.11 Network Security

2.11.1 Security of Network Devices

- Users must only be provided with access to the network services based on the business requirements.
- Policies on the use of network services must be consistent with the Access Management Policy.
- All methods of remote access to the Information System shall be documented, monitored, and controlled, including remote access for privileged functions.
- Users are prohibited from attaching USB modems directly to their computers.
- Access to all external networks shall pass through an access control point (i.e., firewall) before reaching any intended hosts, and subjected to authentication.
- Only authorized and approved network devices shall be connected to the network.
- Operational responsibility for networks shall be separated from computer operations where appropriate.
- Systems containing highly sensitive information may be segregated—virtually or physically.
- Use of clear (i.e., unencrypted) passwords to access network devices internally or externally shall be prohibited.
- GUST owned Information Systems that intermittently or continuously connect to an internal or external network shall employ encrypted, password-based access controls.
- Access to network devices shall be authenticated using centralized access control mechanisms.
- All network devices and network related servers shall have adequate security patches and service packs applied.
- All physical network access points/ports shall be disabled unless a device is attached.
- Session time-out of five minutes shall be configured on all network equipment that disconnects network terminal devices from associated terminal emulation sessions.
- Use of network probing and exploring utilities is not allowed unless explicitly authorized.
- In the case of outsourced network services, service levels, and management requirements of all network services shall be identified and included in network Services Level Agreement (SLA).
- All connections and accounts related to external network connections shall be reviewed and deleted as soon as they are no longer required.

2.11.2 Network Management

- All network and security device clocks shall be synchronized to ensure the accuracy of audit logs.
- Centralized log server shall be deployed for collecting, storing and analyzing the logs generated by the servers, network and security devices.
- Access to the network devices and related systems shall be restricted to authorized users with individual user IDs and passwords.
- Network Administrator shall ensure that all sessions to the network management are secured using an encryption such as 3DES, SSH, or SSL. Wherever the encryption is not possible necessary approval shall be obtained.
- Network Administrator shall ensure that the current and previous version of network device configurations shall be backed up as per Backup Policy to ensure recovery.
- Network administrator shall ensure that a 'Logon Banner' is provided to summarize the requirements for access to a system.
- Network monitoring mechanisms shall be active to detect, record, and prevent network hacking attempts and denial of service attacks.
- All network device faults shall be logged and monitored. Sensitive/critical network devices logs shall be reviewed on daily basis as per Log Management Policy.
- MAC addresses shall be statically configured on access ports to implement port security wherever possible.
- No Wireless Access Point shall be attached to GUST IT Network without formal approval from The Information Security Officer. Network Administrator shall deploy and enable IPS to identify and prevent rogue access points and other wireless threats.
- All network management passwords shall be changed periodically as per GUST Password Policy.
- It shall be ensured that all default manufacturer passwords are changed.
- Employees, consultants and suppliers who access GUST IT Network via Internet should use Virtual Private Network (VPN) and shall follow the Remote Access Policy.
- Any change in the internal network architecture, configuration or network connectivity shall follow the Change Management process.
- Modifications to access control lists (ACLs) shall follow the Change Management process.
- Documents including logical and physical diagrams, showing cable routings and the network devices shall be prepared.

2.11.3 Segregation of Network

- GUST shall implement controls to segregate various user groups within the network by dividing them into separate logical network domains and control traffic among these domains.
- Network perimeter shall be implemented by installing a Secure Gateway/Firewall between any two networks to be interconnected to control access and information flow between the two domains.
- Segregation of networks shall be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

2.11.4 Demilitarized Zone (DMZ) Security

- Traffic from internal and external network to DMZ shall be routed through network access control devices such as firewalls.
- All servers within the DMZ shall be configured to log operating system and application activities and other events as per the Log Management Policy.
- Redundant, default and unneeded user accounts on all servers within the DMZ shall be removed.
- The operating systems of all servers residing within the DMZ shall be configured to enable services that are specifically required.
- All operating systems shall be updated to the latest service packs and patches available in order to address the security concerns arising due to known vulnerabilities.
- Non-compliance with updating of security patches and service packs shall be documented with appropriate rationale.
- Physical access to the DMZ shall be controlled and physical access to the DMZ area shall be logged.
- Audit trails shall be reviewed, and incidents of security breach would be escalated based on severity level definitions based on the Incident Management Procedure.
- Audit logs shall be archived and shall be maintained as per the Log Management Policy.

2.11.5 Network Availability

- Adequate redundancy shall be built into the Network at the Link level and device level as per the business continuity requirements.
- Network devices and links shall be continuously monitored for availability.
- Redundant links should have the same level of security as the primary links.

2.11.6 Wireless Network Security

- While designing and implementing wireless network security, the following shall be performed:
    - The Service Set Identifiers (SSIDs) of the access points shall not reveal information about GUST to external network users.
    - Creation of ad hoc wireless networks is prohibited.
    - Inbound connection requests to mobile devices must be disabled.
    - Strong encryption shall be configured on the wireless network.
    - Unidentified Access Points (APs) must be restricted.
    - While accessing core network through wireless AP, similar authentication and access controls shall be applied as that of wired network.
    - Data traffic from the guest network shall not pass through the core network.
    - Near-field wireless connectivity options shall be disabled, e.g., Bluetooth, Infrared.
    - Connection to the wireless guest network shall only be allowed during a particular defined timeframe.
    - If information of classification ‘Confidential’ or above needs to be sent through the public wireless network, VPN shall be used.

2.12 Human Resources Security

2.12.1 Defining Security Responsibilities

- Terms and conditions of employment shall state the employee's responsibilities for Information Security. Where appropriate, these responsibilities shall continue for a defined period following termination of employment. Action to be taken if the employee disregards security requirements shall be covered in these terms and conditions.
- The Employee's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation) shall be clarified and included in the terms and conditions of employment.
- The End-user Acceptable Use Policy, that describes user responsibilities and expected behaviors about Information System usage, shall be communicated to all users of GUST Information Systems.
- While signing contracts with suppliers, contractors and service providers whose personnel will be on the premises of GUST, a document containing the security responsibilities shall be annexed (Non-Disclosure Agreements – NDA).
- The Information Security Officer shall be responsible for providing the relevant Information Security Policies and related documents to read and understand to the suppliers, contractors and service providers personnel who will be on GUST premises.
- Formal acceptance of understating the relevant Information Security documents shall be taken from suppliers, contractors and service providers personnel on the GUST premises.

2.12.2 Security Prior to Employment

- HR Department, in coordination with the concerned department, shall carry out verification checks (screening) on permanent staff at the time of job applications.
- Background screenings shall be performed in line with relevant laws, regulations and organizational requirements prior to onboarding/hiring employees.
- HR Department shall ensure that all personnel with access to sensitive information are trustworthy and understand their responsibilities. This shall at least include the following:
    - Availability of satisfactory character references (one)
    - A check (for completeness and accuracy) of the applicant's curriculum vitae (CV)
    - Confirmation of claimed academic and professional qualifications
    - Independent identity checks (passport or similar document)
    - Checks of criminal records.
- Where applicable, a screening process shall be carried out by concerned manager department for contractors and temporary staff. Where these employees are provided through a 3rd party agency, the contract with the agency shall clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. Agreement with all third parties shall clearly specify all responsibilities and notification procedures for screening.

2.12.3 Security During Employment

- All staff shall sign a confidentiality or non-disclosure agreements and acknowledge understanding the Acceptable Usage Policy as part of their employment before they are granted access to Information Systems.
- GUST Employees and Contractors' staff that are not already covered by an existing confidentiality agreement and code of conduct shall be required to sign them.
- The non-disclosure agreement shall require employees not to disclose any information derived as a result of their access to GUST information systems to any unauthorized parties. The agreement shall also include specific obligations regarding the recovery and non-disclosure of all information assets and proprietary information in possession of employees upon their termination prior to settlement of dues and their departure from GUST.
- Awareness of legal aspects of using computer-based information systems is important so that users do not breach legal requirements inadvertently.
- The following aspects need specific attention:
    - Ignorance of staff to observe compliance with the legal aspects of using the information systems may lead to prosecution against the user as well as GUST.
    - Not following the changes in the law may result in GUST unknowingly breaching laws and regulations.
    - The terms and conditions of employment should stipulate GUST code of conduct. Otherwise, it may result in inability to proceed with disciplinary action against an employee found to be breaking the legal compliance requirements.
- According to awareness and training policy, GUST Employees and Contractors' staffs shall be given the periodic awareness and/or trainings on information security policies, requirements, business controls, and the correct use of facilities owned by GUST.
- Employees and Contract Staff shall be trained to report the suspected security breaches, security weaknesses or security threats on Information Systems.
- All GUST roles, duties and processes shall adopt the principle of segregation of duties to reduce opportunities for unauthorized or unintentional modification or misuse of GUST information assets.

2.12.4 Employment/Contract Termination or Change

- HR Department shall send the Revocation Request to the IT Department to take the proper action and send it back to HR Department to complete the employee clearance process.
- All Information Systems access shall be revoked by IT Department upon receiving the revocation request from HR Department effectively from the date of issuance of termination/resignation.
- All Information assets issued to the concerned person shall be recovered with immediate effect and prior to settlement of dues and departure from GUST.
- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced during the relieving process.

2.13 Technical Vulnerability Management

- Vulnerability assessments (e.g., missing security updates, missing baseline configuration, application security testing, penetration testing and code reviews) of network, systems and applications shall be conducted on periodic basis or whenever significant changes occur to the environment, to identify the existence of vulnerabilities and classify them based on their impact.
- GUST shall receive notifications from trusted information sources about latest vulnerabilities and follow risk-based approach for prioritizing and treating the vulnerabilities identified and notifications received from information sources.
- An automated vulnerability and compliance scanning tool shall be implemented for the immediate detection and remediation.
- Mitigation plan shall be developed to remediate vulnerabilities in a timely manner. The findings of vulnerability assessments shall be reported, logged for initiating remediation activities and tracked till closure.
- A patch shall only be applied to remediate a technical vulnerability after it has been assessed for the associated risks of installing it. If installing patch introduces new risks, other compensating controls shall be applied.
- The patches shall only be obtained from trusted sources and, if the requirement is not urgent, patches should be applied in batches.
- GUST shall conduct validation after remediating the vulnerabilities to assess whether gaps addressed are in line with risk decisions.

2.14 Secure Configuration

- Security configuration standards (Minimum Security Baselines – MSB) shall be defined and implemented to cover technology assets used within the organization.
- Security configuration standards shall be based on global best practices (such as NIST, Center for Internet Security (CIS) benchmarks etc.), guidelines issued by Original Equipment Manufacturers (OEMs), and internal policies and best practices of GUST.
- Security configuration standards shall, at a minimum, include the following:
    - Installing only approved and supported version of software.
    - Installing minimum components or services necessary to meet the requirements.
    - Applying up-to-date security updates.
    - Protecting data in line with asset management and information classification requirements.
    - Disabling or restricting access to weak or unnecessary services and ports.
    - Changing default passwords, removing or disabling unneeded accounts.
    - Configuring access control based on need-to-know and need-to-have principles.
    - Removing local administrator privileges from end-users' devices.
    - Disabling weak or insecure protocols and algorithms and ensuring that only latest and industry supported algorithms are used.
    - Setting security measures to lock or terminate (logout or logoff or close the application page) sessions after meeting a predefined period of inactivity and conditions.
    - Measures to protect against malicious software, malware, ransomware, data loss, denial of services, advanced threats etc.

    - Synchronizing system clocks against an agreed reference such as Universal Coordinated Time (UTC) and monitor their accuracy. This applies to routers, switches, servers and other relevant networking equipment.
    - Enabling logging and monitoring.
- Compliance with security configuration standards shall be monitored periodically.
- New technology deployments shall be configured as per configuration standards and testing shall be performed prior to going live to confirm the compliance.
- The software and information processing facilities shall be protected against malicious software (malware).
- GUST shall implement controls to detect sources of malicious code and prevent introduction of malicious code into the operating environment.

2.15 Security Patch Management

- All systems owned by GUST must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, servers and network systems owned and managed by either GUST or their third-party.
- Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration policy for all workstations at the organization.
- All operating systems, information processing devices and applications shall be properly configured to install the recommended software updates.
- Information related to patches shall be obtained from authorized and genuine sources such as vendor mailing lists/ websites, security alert announcement, etc.
- As soon as patches are available, they shall be downloaded from trusted sources.
- Patches that correct a known critical security vulnerability need to be deployed as soon as possible, and no later than two weeks following release.
- The Information Security Officer with input from related support functions shall carry out an assessment to understand the impact of applying the patch.
- Patches shall be tested in the test environment before actual implementation in the service environment.
- Wherever testing is not feasible, exceptions to this requirement shall be recorded, justified, and communicated to the Information Security Officer.
- Suitable tools shall be utilized for carrying out patch management in the server and network environment.
- Appropriate and authorized scanning mechanisms shall be deployed to understand the status of the patches implementation in the systems and applications periodically.
- Patches deployment for all system components in GUST shall follow the Change Management Process.
- Any changes being applied to the infrastructure must be logged and the date on which they are applied is made known.
- Changes and relevant downtime during patch deployment shall be communicated to affected parties.

2.16 Clear Desk & Clear Screen

2.16.1 Clear Desk

- To avoid loss, damage or leakage, business related hardcopy documents, materials or digital storage media shall not be left on unattended desks after working hours.
- During working hours, any sensitive and/or confidential business information in hardcopy or digital storage media shall not be left unattended on desks or other office areas.
- When not in use, hard copies and digital storage media shall be stored in drawers, cabinets or other forms of suitable storage.
- Restricted and Confidential information shall not be pinned on boards or office walls.
- Restricted and Confidential information, when printed, shall be cleared from printers immediately.
- In the meeting rooms, at the end of each meeting, care shall be taken to collect any business documents/materials and to clear any business information written on boards.

2.16.2 Clear Screen

- All the workstations must be protected by key locks, passwords, screen savers or equivalent controls when not in use. The use of screen savers or screen shields should be considered for computer monitors in open areas or where public may have sight of the screen.
- Users need to manually lock their Desktops and Laptops (press “Windows” key and “L” keys at the same time OR press CTRL, ALT and DEL keys at the same time followed by clicking the ‘LOCK COMPUTER’ button on Windows O/S) when they leave their workplace for a short period of time.
- All user workstations must have password-locked screen savers enabled to activate after a period of inactivity. This is an additional safeguard that does not preclude the requirement for users to manually log off or lock their login sessions when leaving their computers unattended (see previous point).

2.17 Physical and Environmental Security

2.17.1 Secure Areas

- Security perimeters shall be defined and used to protect areas that contain confidential information and information processing facilities.
- IT facilities that host critical IT applications shall be secured and controlled to ensure that access to servers, network and applications is restricted to authorized personnel only.
- IT facilities shall be physically protected from threats and environmental hazards. Protective equipment such as fire extinguisher and smoke detectors shall be installed and properly maintained.
- All critical areas shall be under continuous monitoring via CCTV / surveillance cameras. The critical areas identified for camera surveillance shall be identified by IT department.

- Physical access to office premise shall be controlled by an Access Card Control System. Access inside the office shall be restricted only to authorized personnel and audit trail of all access shall be securely maintained.

2.17.2 Data Centre

- All servers shall be placed in the Data Centre.
- Only authorized personnel will have access to the sensitive and critical Information Systems & Services area, Data Center and associated facilities to the extent necessary for the execution of their official duties. Only those individuals who have a legitimate business need can be in the Data Center.
- All visitors including IT personnel are required to register upon visiting the Data Centre and be escorted and monitored at all times.
- All computing and telecommunications equipment and data media must be located safe and protected from potential sources of hazards.
- The Data Center operating environment must always be clean. Eating, drinking and smoking are strictly prohibited.
- Adequate detection controls (e.g., fire alarm, smoke detector, CCTV etc.,) and safety devices (e.g., fire extinguishers, water hydrants etc.) shall be placed within reach in all restricted zones, switch rooms and data centres.
- Equipment should be protected from power failures and other electrical disturbances. A suitable electrical supply should be provided that conforms to the equipment manufacturer's specifications. Various options should be considered to achieve continuity of power supply:
    - Multiple feeds to avoid a single point of failure.
    - Un-interruptible power supplies with redundant configuration.
    - Back-up generator.
- UPS equipment should be regularly checked and maintained to ensure its adequate capacity and should be tested with the manufacturer's recommendations. UPS should support orderly close-down or continuous running is recommended for equipment supporting critical business operations.
- A back-up generator should be considered if processing is to continue for prolonged power failures. There should be an SLA that ensures the maximum uptime with the supplier/contractor for maintaining of UPS and Power Generator. If installed, generators should be regularly tested in accordance with the manufacturer's specifications. Adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period.
- Emergency power off switches should be located near emergency exits in critical equipment rooms to facilitate rapid power down in case of emergency.

2.17.3 Equipment Protection

- Equipment to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards.
- Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten as per media handling and destruction policy.

- Damaged devices containing sensitive data require assessment along with Information Security Officer to determine whether the item should be physically destroyed rather than repaired or discarded.
- All equipment containing storage media (e.g., fixed hard drives) must be checked to ensure that any critical business information assets and licensed software are removed, securely overwritten or destroyed prior to disposal.
- Users shall ensure that unattended equipment is given appropriate protection to avoid uncompromised information preservation and equipment safety.
- Equipment shall be securely disposed to avoid leakage of information or data.
- Equipment, information or software shall not be taken out from GUST premises without prior authorization.
- Spot checks shall be carried out to detect unauthorized removal of property. All the individuals of GUST should be made aware about spot checks.
- Employees, contractors and third party users who have authority to permit removal of assets shall be clearly identified and defined.

2.18 Internet Security

- The sites accessed by users including the contents stored in or transmitted by organization-owned equipment, is the property of GUST.
- The Internet access in GUST is provided to users only to conduct the business of GUST in an efficient and convenient manner. Incidental personal use is permissible as described in the Acceptable Usage Policy.
- GUST reserves the right to examine such sites and contents to ensure compliance with this policy.
- Usage of 'Peer to Peer Software' for file sharing from external network (Internet) is prohibited.
- GUST does not permit the usage of internet services involving but not limited to the following situations:
    - Access, upload, download, or distribute materials related to adult entertainment, alcohol and drugs, games, hacking, violence, militancy, racism, sex, weapons, gambling.
    - Violate the state, local, or federal law.
    - Vandalize or damage the property of any other individual or organization.
    - Invade or abuse the privacy of others.
    - Violate copyright or use intellectual material without permission.
    - Non-work-related matters.
- GUST has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- When users provide information on public forums such as Newsgroups, Blog Sites, Bulletin Boards, Social Media site, etc., they shall clearly indicate that the opinions expressed are their own and not necessarily those of GUST's.
- Inappropriate electronic postings, which include non-work-related postings, to public forums are prohibited. These include postings which harass, annoy, alarm, or otherwise attack others in a forum as well as postings which might be considered as a threat against a user, group, or an organization or contain profanity, religious or political statements.

- No files or documents shall be sent that may cause legal liability or harm the reputation of GUST.
- GUST may install software and/or hardware to monitor and record all IT resources usage, including email and website visits. GUST retains the right to record or inspect all files stored on GUST systems.
- Users are reminded that Web browsers leave 'footprints' (or cookies) providing a trail of all sites visited by the users.
- GUST shall activate logs and reserves the right to examine:
    - Files on personal computers
    - Web browser cache files
    - Web browser bookmarks and cookies
    - Temp folders
    - Download folders
    - Logs of web sites visited
    - Other information stored on or passing through GUST computers and networks.
- These logs shall be used by GUST to assess compliance with internal policies, security analysis and assist GUST with internal investigations, if required later.

2.19 E-mail Security

- All messages composed, sent or received through the corporate email remains as the property of GUST.
- GUST does not permit the usage of email services involving but not limited to the following situations:
    - Sensitive and Illegal Matters: Creation and distribution of any offensive or disruptive messages such as those containing sexual implications, gender specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability is prohibited. Employees who receive any emails with the relevant content from any employee should report the matter to the management immediately
    - Use of E-Mail for Personal Purpose: Sending of chain letters, junk mail, jokes and executables is prohibited. Users are also not allowed to use the organization's email to register with any non-related business matters (e.g. Facebook, Internet Banking, Social Network organization, Personal Event, BlogSpot, e-Trading, etc). The organization's email may be used to register with trusted academic social media platforms only.
    - Originator message or attachment: Copying a message or attachment belonging to another person without prior permission of the originator is forbidden. In such scenarios, the permission of the originator or relevant Manager must be obtained. In case the attachment is provided for further use, the originator should specify this in the email.
    - Disclosure of confidential information: Unauthorized transmission of trade secrets, confidential information, or privileged communications is strictly prohibited. Any disclosure of confidential information through email shall be encrypted or password protected.
- Controls to protect and secure email and messaging systems from security risks (such as spam, malicious links / attachments, email phishing) shall be implemented.

- GUST reserves the right to monitor emails through security solutions without prior notice to ensure compliance. This is only to detect any security risks, however without disclosing confidential information in the email content to unauthorized personnel.
- Information transferred through email shall be protected from interception, copying, modification, misrouting and destruction.
- Appropriate security measures (such as digital signatures and encryption) shall be implemented to protect the confidentiality of information being communicated through emails.
- Information involved in electronic messaging such as instant messaging, email and fax shall be protected from misuse, unauthorized access, modification or denial of service.
- Access to the email Service application by unauthorized persons shall be restricted.
- It shall be ensured that the email service is not running as root or system/administrator.
- Content Filtering shall be configured to block suspicious messages and to notify the recipients about the blocked message.
- The size of attachments of incoming shall be restricted to 30 MB and that of outgoing attachment shall be restricted to 30 MB unless there is an exception.
- The audit logs of the Email Service shall be enabled.
- It shall be ensured that Firewall blocks all inbound traffic to the Email Service Application Server except from the required ports.
- IDS/IPS shall be configured to monitor the Email traffic and critical files, system resources available on the Email Service.
- Network Switches shall be used to segment the Email Service to protect against network eavesdropping.
- On Email Client, the following shall be disabled:
    - Automatic opening of next message.
    - Processing of active content.
    - Ability of Email client to store username and passwords.
- Secure authentication and access shall be enabled on Email Clients.
- Only necessary plug-ins from trusted sources shall be enabled and installed on Email Clients

2.20 Physical Media Handling and Destruction

- IT supplied Media shall only be used to store, process, transfer, dispose data or information for business purpose.
- Where possible, media that is supplied by GUST IT shall be used. However, when the use of media that is supplied by third parties is required, then it shall be examined by IT to ensure compliance.
- All the media shall be classified as per the Information Classification Policy.
- Data that is classified as Restricted" and Confidential shall be stored into media by encrypting the data /information stored.
- When the media is connected to a system (desktop/laptop), anti-malicious software shall be used to scan and remove computer virus, if any found.
- Only data that are authorized and necessary to be transferred shall be saved on to the media.

- Special care shall be taken to physically protect the Media and Stored Data from loss, theft or damage. Anyone using Media to transfer data shall consider the most appropriate way to transport the device and be able to demonstrate that reasonable care is taken to avoid damage, theft or loss.
- The media used shall have a life span in accordance with retention requirements of data.
- The media shall have a low susceptibility to physical damage and be tolerant of a wide range of environmental conditions without data loss.
- Arrangements shall be made to ensure that Media is protected against physical threats e.g. misplacement, theft, fire, humidity, dust and other similar threats.
- Access to the Media shall be restricted to ensure authorized access, the media data is quickly identifiable and accessible when required.
- The IT Department shall be responsible for maintaining inventory logs of all media and conduct media inventories at least annually.
- In case of movement of the media, the designated staff for the media transfer shall be responsible for management/oversight of the transfers that they own, including:
    - Logging and updating media transfer records, including media location.
    - Sent by secured courier or other delivery method that can be tracked.
    - Ensuring management approval is in place.
    - Reporting security incidents and informing the Information Security Officer.
- The media for data backup shall be stored off-site to ensure its availability in case of a disaster.
- The physical security controls of the off-site location/facility of the data backup shall be reviewed and inspected annually.
- The Media shall be disposed of after the approval of the Data Owner and the Information Security Officer, as per the following:
    - Hard-copy materials shall be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
    - Storage containers used for materials that are to be destroyed shall be secured.
    - Staff/Student personal data on electronic media shall be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).
- It shall be ensured that the data on the media is not accessible by any means after the disposal.
- It shall be ensured that the media is disposed of in secure manner.

2.21 Information Classification and Labelling

2.21.1 Classification of Information

GUST shall use four classification categories:

- Public (General Use, Low Sensitivity)
    - This information has been specifically approved for public release by GUST Management. Unauthorized disclosure of this information should not cause problems for GUST, its customers or its business partners. Examples are marketing brochures and material posted on the website. Disclosure of the university information to the public shall require the existence of this label, the

specific permission of the information owner or long-standing practice of publicly distributing this information.

- Internal (Internal Use, Private, Medium Sensitivity)
    - This information is intended for use within the university and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against law and regulations or may cause problems to GUST, its customers or business partners. This type of information is available within the university such as address book, internal mail communications, policies and procedures, etc.
- Confidential (High Sensitivity)
    - This information is private or otherwise sensitive and shall be restricted to those authorized and with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against law and regulations, or may cause significant problems to GUST, its customers or its business partners. Decisions about the provision of access to this information shall be cleared through the information owner. Examples are customer personally identifiable information (PII).
    - If information is not marked with one of these categories, it shall default into the Sensitive 'Internal Use Only' category.
- Restricted (Highest Sensitivity)
    - This information is extremely sensitive in nature and shall be restricted to only authorized specific individuals defined. Unauthorized disclosure of this information may cause significant harm, legal cases to be raised against GUST, customer loss, market competition loss or other events with a high value impact on the business or to the customer base. Examples of this information are as follows: GUST business strategy, business secrets, marketing plan, high net worth customer account details, senior management reports, trade secrets and pre-release financial reports.

2.21.2 Information Labelling

- Owners of information assets shall be accountable for their classification.
- The owner or creator of the information shall designate an appropriate label and the user or recipient of this information shall consistently maintain an assigned label.
- Sensitive information labels shall be used in electronic mail or paper memos.
- Labels for sensitive information shall appear on the outside of media, backup tapes reels, optical media, external storage disks, audio cassettes and other storage media.
- If a storage volume such as USB drive contains information with multiple classifications, the most sensitive category shall appear on the outside label.
- When creating a collection of information source with various classifications, the collection shall be classified at the highest sensitivity level of the source information.

2.22 Information Handling

2.22.1 Data Protection

- Storage, retention and disposal of important records shall be performed in accordance with:

    - Statutory, regulatory and contractual requirements.
    - Local and cross-border business requirements.
    - Information Classification policy.
- Security controls shall be implemented to protect confidentiality, integrity and availability of sensitive data and important records while at rest and in transit.
- Encryption techniques used to protect important records shall be in accordance with the Cryptography Policy.
- Information transferred within GUST or to external networks shall be protected from interception, copying, modification, misrouting and destruction as detailed in the Information Transfer policy section.
- Wherever possible, data transmission between processes within an application should have no manual intervention.
- All the transactional data residing in the databases should be protected from unauthorized access. Database administrations should not be allowed to view/edit/delete the data.
- Access should be allowed on need-to-know basis and sufficient audit trails should be available for any changes to the production data.
- Applications should be configured to ensure the integrity of data is maintained during input, internal processing and output.
- Content copied from and to all removable devices such as USB Flash drives, CD-DVD, Plug and Play devices, apple devices, mobile phones, Bluetooth, modems, etc. shall be blocked by Endpoint Data Loss Prevention (DLP) solution.
- Full disk encryption shall be enforced on GUST-owned Laptops.
- Data stored in the file servers shall be protected by folder level access control.
- Data stored on mobile devices shall be protected by Mobile Devices Management (MDM) system.
- Data stored in the backup media shall be encrypted using encryption technology.
- GUST shall use DLP technologies to monitor data in motion. The incident calls shall be reported and analyzed by the Information Security Officer.
- Violations shall be communicated to Department Heads and HR department to take appropriate disciplinary actions where applicable.
- Media such as tape, CD and USB drive used to record or store classified information, shall be treated with the same level of criticality, as the highest classification of data residing on such media.
- The data shall hold the classification levels from the time it is created until the time it is destroyed or re-labeled.
- User-level controls shall be implemented for all department folders and user access shall be reviewed once a year at a minimum by the Department Heads, and the Information Security Officer shall be responsible for the department folder access review.

2.22.2 Data Privacy

- The privacy and protection of Personally Identifiable Information (PII) at GUST shall be followed in accordance with this policy, the related contractual clauses and relevant global and local legislations.
- Guidelines to safeguard the privacy of the user identifiable information from unauthorized access or improper use shall be implemented.

- All kinds of data such as personally identifiable information shared by users shall be:
    - processed fairly, lawfully and securely.
    - processed in relation to the purpose for which it is collected.
    - maintained up to date and accurate as necessary.
    - retained for no longer than is necessary for the purpose for which it is collected.
- Users shall be provided with at least the following information before collecting personally identifiable information (PII):
    - Purposes of processing the information
    - Any further information regarding the specific circumstances in which personal information is collected, such as:
        - The recipients of the information.
        - Whether submission of information is obligatory or voluntary, as well as the impact of failure to submit such information.
        - The existence of the right to access, update or remove personal information.
        - Whether personal information will be used for marketing purpose.
- Access to data identified as per this policy should be monitored and reviewed.
- Test data shall be selected carefully, protected and controlled to avoid the use of PII and confidential production data in test environment. If needed for testing, the business purpose should be captured and approved along with authorization controls, logging, audit trails and monitoring.

2.22.3 Data Retention and Disposal

- The Data owners shall set their own data retention requirements to sufficiently maintain their business operations and to meet the legal and regulatory requirements, business dependency, data residency requirements and data privacy requirements etc.
- The data shall be categorized and the retention requirement for each category shall be specified.
- All data depending on its category, need and relevance shall have a well-defined retention period.
- No information of any category other than PUBLIC shall be stored beyond its defined retention period.
- The Data retention requirements shall also specify the period for which the data shall be retained as live before archiving it for a specified time period.
- The Information Security Officer shall ensure that data is properly retained according to the defined requirements.
- Arrangements shall be made to ensure that data is protected against physical threats e.g., misplacement, theft, fire, humidity, dust and other similar physical and environmental threats.
- Access to the retained data shall be restricted to ensure authorized access.
- All information shall be securely purged after the defined retention period.
- All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
- All classified data shall be disposed of in a secure manner to ensure complete removal of the data, including both paper-based and electronic forms.

- All classified data shall be completely cleared from the server, computer, laptop, mobile devices, and USB flash drive before disposal or re-use.

2.23 Information Transmission

- Cryptographic controls shall be used to protect critical data/ information assets transferred internally or to external networks.
- GUST IT shall ensure secure encryption is applied for services published to outside access.
- GUST information classified as RESTRICTED and CONFIDENTIAL shall be exchanged only over a trusted path or medium with controls to provide authenticity of content, proof of submission, and proof of receipt and non-repudiation of origin.
- Secure communication protocols such as TLS, IPSEC, SSH, SFTP shall be used when RESTRICTED and CONFIDENTIAL information is transmitted over internal and external networks.
- Data Loss Prevention (DLP) solution at the network shall be implemented to monitor outgoing email and web traffic, as well as detect data using keywords, document fingerprinting, etc.
- Endpoint Data Loss Prevention (DLP) solution shall be enforced to all GUST-owned laptop and desktops to prevent data leakage.
- RESTRICTED and CONFIDENTIAL business information and classified documents shall be excluded from systems which do not provide an appropriate level of protection.
- Information Systems containing secret information shall provide non-repudiation capability to determine whether a given individual took a particular action within specific systems by providing specific logical access.
- Information Systems and Media shall be controlled while in transit (paper or digital), with the pickup, receipt, transfer, and delivery of such media restricted to authorized personnel.
- End Users shall be subject to monitoring for data leakage, and all data leaving the university via different channels shall be protected using approved standard methods.
- Data leakage or transmission outside of normal approved business application channels, when detected shall be sent to the appropriate manager for confirmation that the data was approved to be sent outside GUST.
- Email, virus protection and encryption policies shall be aligned towards information exchange and to prevent any leakages.
- Information Systems shall terminate an online transaction at the end of a session or after a pre-defined time period of inactivity.
- Employees and Third parties shall be required to sign non-disclosure agreements (NDA) when performing information exchange.
- Formal agreements shall be established for the exchange and transfer of critical business information with external organizations such as suppliers and interested parties. These agreements shall be developed for both manual and electronic exchanges. These agreements shall reflect the sensitivity of the critical business information being exchanged or transferred and shall describe any protection requirements.
- Exchange and transfer agreements shall specify management responsibilities, notification requirements, packaging and transmission standards, courier identification,

responsibilities and liabilities, data and software ownership, protection responsibilities and measures, and all encryption requirements as appropriate.

- Information Security awareness sessions shall be carried out regularly for GUST community as needed. The Information Security awareness sessions shall include precautions which should be considered regarding information exchange.

2.24 Cryptography and Key Management

2.24.1 Use of Encryption

- Cryptography must be used to protect information (either hosted in-house or at third-party) with high confidentiality and / or integrity requirements.
- Use of cryptography shall be based on business need and purpose.
- GUST shall use appropriate encryption techniques to secure sensitive data within system logs, databases, networks, applications, and other information assets as applicable. These techniques shall be applied consistently across on-premises and cloud installations.
- The level of protection that business information needs and the required use of cryptographic controls to protect information according to its criticality and classification shall be assessed on a risk-based process.
- Data sent over all networks should be sent using secure channels and encrypted based on information classification.
- When applying cryptographic controls, applicable laws and regulations should be considered.
- The Information Security Officer shall define the list of approved encryption and security protocols as per the following:
    - Authentication Protocols, this can include Kerberos, RADIUS, TACACS+, etc.
    - Key Management Protocols, this can include Diffie-Hellman, QV (Menezes-QuVanstone), etc.
    - Network Security Protocols, this can include IEEE 802.1x, TLS, etc.
    - Secure Email Protocols, this can include Secure Multi-purpose Internet Mail Extension (S/MIME), IBE (Identity-Based Encryption), etc.
- The following Asymmetric Encryption Algorithms should be used in GUST environment:
    - For public key encryption purposes: RSA (minimum 2048 bit), DH (minimum 2048 bit) or ECDH (minimum 256 bit) algorithms.
    - For digital signature purposes: RSA (minimum 2048 bit), DSA (minimum 2048 bit) or ECDSA (minimum 256 bit) algorithms.
    - For key exchange purposes: DH (3072-bit or larger), ECDH (NIST P-256 or NIST P-384) or RSA (3072-bit or larger) algorithms.
- Keys used for all kind of encryption shall be protected against disclosure and misuse, this can include the following:
    - Access to keys is restricted to the fewest number of custodians necessary.
    - Key-encrypting keys are at least as strong as the data-encrypting keys they protect.
    - Key-encrypting keys are stored separately from data-encrypting keys.
    - Keys are stored securely in the fewest possible locations and forms.

- To increase the security of encrypted file systems, the system should use a hardware token for storage of the key or the Trusted Platform Module (TPM) for storage of the keys.
- The following requirements must be considered when implementing an encryption tool at GUST:
    - The handling requirements for sensitive information when transported by mobile or removable media, devices or across communication lines.
    - The impact of using encrypted information on other security controls (e.g. virus detection, malware detection or content inspection tools like DLP).
- The cryptographic key length shall be selected as per the information classification.
- Mobile devices must be encrypted where the information accessible on the device is classified as 'Confidential' and above.
- Cryptographic controls must ensure confidentiality, integrity and non-repudiation of messages containing confidential business data.
- Student data being transmitted across open, public networks shall be encrypted.

2.24.2 Key Management

- The key length used for encryption shall be as per the latest globally acceptable industry best practices.
- The keys may not be stored in application code. If deemed necessary, such keys should be encrypted within the application.
- Roles and responsibilities should be established for applying cryptographic controls and managing cryptographic keys.
- The cryptographic keys shall be managed and protected through their lifecycle including generating, storing, archiving, retrieving, distributing or transmitting, retiring and destroying keys.
- All cryptographic keys should be protected against modification and loss.
- Strength of the cryptographic algorithm and key length shall be based on the business requirement and criticality of the information handled.
- Key activation and de-activation dates shall be pre-defined.
- The key length for symmetric encryption must be no shorter than 128 Bit at the time of writing.
- As with encryption algorithms, up-to-date algorithms must be used, while algorithms with known flaws must be avoided. Therefore, hash functions like SHA-1 or MD5 shall be avoided, while more recent algorithms like SHA-3, RIPEMD-160 or Whirlpool shall be preferred.
- Custody of the keys and appropriate key management should be established.
- Key backups shall be protected through access restriction and secure storage mechanisms at least as stringent as enforced for operational keys.
- Encrypted data shall not be stored on the same medium as its corresponding encryption key.
- Keys used within a test/development environment shall not be used in a live/production environment and vice versa.

2.25 Cloud Security

- GUST shall maintain a list of approved cloud services.
- Use of cloud computing services involving GUST data must be formally authorized on a case-by-case basis by the Information Security Officer.
- GUST shall ensure that data is encrypted at rest as well as in transit. The cryptographic algorithms used to encrypt data shall be in line with GUST cryptographic policy.
- GUST shall ensure that the Cloud Service Provider (CSP) is using a unique set of encryption keys that is stored at GUST. The unique encryptions keys help protect data from being accessible if it is inadvertently leaked from one CSP customer to another.
- The Information Security Officer shall support the IT Manager in evaluating the necessity to encrypt data in the cloud or not.
- The use of cloud computing services must comply with all GUST IT and Security policies and procedures, including the Information Classification Procedure.
- For public data, cloud solutions are acceptable.
- GUST shall ensure separation of its environments (specifically virtual servers) from other environments hosted at the cloud service provider.
- Wherever applicable, multi-factor authentication (MFA) must be enforced to access all and any cloud services as a policy.
- Sufficient audit logging must be available to allow the IT personnel to understand the ways in which the proprietary data is being accessed and to identify whether any unauthorized access has occurred.
- All data pertaining to GUST must be removed from cloud services in the event of a contract coming to an end. Data must not be stored in the cloud for longer than is required based on the purview of the business.
- For storage that cannot be wiped, GUST shall ensure that the CSP uses a destruction process that destroys and renders the recovery of information impossible.
- GUST shall ensure that a written agreement exist with cloud service providers that include the following requirements:
    - Scope of services, operational level agreements and clearly defined roles and responsibilities.
    - Cybersecurity regulatory and legal compliance requirements.
    - Locations of data storage, data privacy, confidentiality and information sharing, access to data, encryption, data portability, and data retention.
    - Right to audit.
    - Code of conduct and dispute management.
    - Incident management, business continuity and disaster recovery requirements
    - Breach notification strategies, CSP shall notify GUST of confirmed security incidents that affect GUST data within 24 hours or as early as practical upon their discovery;
    - Secure termination of agreement.
    - Legal clauses/terms and conditions to ensure that GUST's intellectual properties (IPs) should remain intact while operating on cloud.