الجـــامعـــة الخـــليجـــية

GULF UNIVERSITY

| | |
|---|---|
| **Title:** | **IT Policy** |
| **Code:** | GU-PLIT01 |
| **Version:** | 1.1 |
| **Date of Issue:** | 2023 |
| **Effective Date:** | July 2023 |
| **Approval Authority:** | University Council |
| **Document Owner:** | Chief Operating Officer |

**Review:** The policy is subject to a periodic review every 4 years or in a shorter cycle as per amendments of regulations and policies

الجامعة الخليجية
P.O.Box : 26489, Adliya
Kingdom of Bahrain
GULF UNIVERSITY

## 1. Acronyms

| | |
|---|---|
| **GU** | Gulf University |
| **ITD** | Information Technology Department |
| **HOD** | Head of the Department |
| **UPDRC** | University Policy Development & Review Committee |

## 2. Definitions

**Information:** It includes all resources that has a value to the university.

**Information System Environment:** It defines the total environment and includes, but is not limited to, all documentation, physical and logical controls, personnel, hardware, software, and information.

**Authentication:** It relates to the identification requirements associated with an individual using a computer system with authorized access only.

**Availability:** It means that authorized users have access to information and associated assets as and when needed.

**Confidentiality:** This ensures that information is accessible only to those authorized to have access to use.

## 3. Policy Statement

The purpose of a consolidated IT policy is to set out principles for maintaining a secure and efficient IT environment. The policy ensures proper use of resources, protection of data, prompt incident handling, and secure password practices. The users are required to follow the compliance is essential, and failure to comply might result in disciplinary actions and legal consequences.

## 4. Policy Principle

4.1 Gulf University is committed to protect the confidentiality, integrity, and availability of information assets through robust security measures, awareness training, and proactive threat assessment.

4.2 Gulf University ensures alignment with legal, regulatory, and industry standards, including data protection, privacy, intellectual property rights, and IT governance frameworks to maintain trust and safeguard the university's reputation.

4.3 Gulf University encourages technology-enabled collaboration, seamless communication, and enhanced productivity through reliable and user-friendly IT tools and platforms for students, faculty, staff, and external stakeholders.

4.4 Gulf University commits to provide training, resources, and support to enhance IT skills and knowledge, empowering users to leverage IT resources effectively and responsibly.

4.5 Gulf University is committed to proactively identifying, assessing, and mitigating risks associated with technology use, implementing controls, disaster recovery plans, and data backup mechanisms for business continuity.

4.6 Gulf University promotes energy-efficient practices, responsible electronic waste disposal, and eco-friendly technologies to minimize the environmental impact of IT operations.

4.7 GU is committed to support staff and students in providing IT services and facilities in terms of internet and network facilities, email, IT helpdesk in completing their responsibilities.

4.8 GU commits to authorize all the users to access IT services and facilities in professional, ethical manner from multiple devices namely, desktop, laptop, smart phone, iPad, tablet etc.

4.9 GU commits to create and manage documents and records in professional manner within the university wide policies and procedures with courteous communication.

4.10 GU is committed to implemented tracking mechanism to measure the utilization of computer labs and software.

4.11 GU is committed to identify and handle incidents of information security effectively, minimize their business impact and reduce the risk of future occurrence of such incidents.

4.12 GU ensures that information security incidents are timely reported and investigated in appropriate manner. These are managed and resolved by designated persons in ITD who have relevant skills and expertise to deal with incidents.

# 5. Policy Details

## 5.1 Access level & Privileges

5.1.1 All account, service and platform access is managed through secure authentication controls.

5.1.2 All GU systems can be accessed through single sign-on only to prevent unauthorized/overprivileged access.

5.1.3 Staff receive access based on their line manager requirement and IT manager approval.

5.1.4 All emails are created once the user is officially on board. Administrative staff receive unique role-based email addresses, academic staff receive name-based email addresses. Students are provided with unique ID-based email addresses.

5.1.5 Protection of user accounts is ensured through selection of strong passwords and securing them consistently without giving opportunity for unauthorized use.

5.1.6 IT department holds the responsibility to secure password as confidential information such that it is not disclosed to any person either in oral or written form.

5.1.7 All system level and user level passwords are subjected to change at stipulated intervals. The locked account is reinstated automatically after 30 minutes or with the necessary intervention or support of system administrator.

5.1.8 Configuration of information systems is done such that user id is locked and access is denied to the user after entering the incorrect password for maximum 3 times.

5.1.9 All system level and user level passwords conform to the guidelines of password character and password is different than the username.

5.1.10 GU is committed to provide Office 365 Educational License by Microsoft to all staff and students (end users) for the most effective use of this software in collaborating across boundaries and cultures.

5.1.11 GU commits to create and manage documents and records in professional manner within the university wide policies and procedures with courteous communication.

5.1.12 GU ensures that end users must not be using Office 365 to store, maintain, or transmit any kind of restricted/confidential data.

5.1.13 GU ensures that end users must store university/work related documents/files/folders in OneDrive as per standard space given by the university.

5.1.14 ITD at GU does not  back up data stored on Office 365 nor OneDrive, and cannot restore, or recover, any data or documents that are deleted from these applications.

5.1.15 GU ensures that information shared and managed within this technological environment including chat, meeting, email is restricted to relevant academic and administrative operations of the university as per the compliance.

## 5.2 Back up

5.2.1 Gulf University ensures that all business critical information, system or hardware configuration are backed up and retained according to the requirement of the university.

5.2.2 Frequency and retention of back up are determined by the criticality of information. At a minimum, backup copies are retained for 90 days.

5.2.3 Gulf University commits to store in a secure off-site location a minimum one fully recoverable back-up version of business critical information. Confidential data is backed up and stored in encrypted form.

5.2.4 Automated comprehensive data backups are done every single day on cloud while manual backups are done every week on Thursday on a physical location as a second disaster recovery plan.

5.2.5 IT system administrator holds the responsibility for back up testing via restoring a sample of the backups in a formal schedule in the test environment.

5.2.6 Penetration test is done once a year.

## 5.3 Security

5.3.1 All information security related suspected incidents or breaches or potential control weaknesses shall be reported by end users to the ITD.

5.3.2 Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

5.3.3 All information security responsibilities shall be clearly defined. ITD shall be responsible for directing and coordinating information security for:

- Review/approve IS policies and responsibilities
- Review/update departments/units end users and group privileges
- Frequent review/update status of end users in Active Directory
- Monitor the changes of IS Assets to major threats
- Review/monitoring IS incidents as per related policy/procedure
- Apply/approve major initiatives to enhance IS and related risks

5.3.4 ITD, at its option and as appropriate, shall hire the services of external information security consultants either continuously or on a case-by-case basis to provide advice on specific aspects of information systems security.

5.3.5 Moodle instance is registered with Moodle site so that the list of all security issues is received which are fixed on the day they are released.

5.3.6 ITD is responsible to upgrade the Moodle core regularly to ensure all latest security issues are fixed on time.

5.3.7 ITD is responsible to take regular backup of Moodle as it is a crucial part of securing any system and back-ups are fully restorable.

5.3.8 ITD is equipped with incident prevention activities arising from cyber security attack, possibility of breach of security, loss of information, hacked server, stolen password etc. Whenever a security incident, such as virus, worm, hoax mail, discovery of hacking tools, altered data etc., is suspected or confirmed, the appropriate actions are taken to prevent further damage.

5.3.9 ITD keeps records of incidents with required documentation to classify whether reporting of incidents are actual, suspected, threatened or potential.

5.3.10 GU in collaboration with ITD commits to monitor the incidents related to information security over time to identify the threats of repeated incidents and the extent of risk therein.

## 5.4 IT Services

5.4.1 ITD provides secure and innovative services to students, faculty and staff keeping all IT-related services available and accessible along with IT team.

5.4.2 ITD is committed to installation and maintenance of all computer hardware, workstations and servers along with telecommunication and web services. ITD is responsible to provide licensed software applications for staff and students with emphasis of program related software.

5.4.3 ITD holds the responsibility to design and manage university website and provide up to date information.

5.4.4 ITD provides e services to staff and students in accessing email, Turnitin, Learning Management System, Digital Library, SharePoint, academic calendar, class schedule, exam update. GU also supports staff and students by providing remote access to computer labs.

5.4.5 ITD maintains assets that are under warranty. Devices that are out of warranty are evaluated and maintained only in case of valid business need after proper approval from IT manager.

5.4.6 IT helpdesk provides 24x7 online/offline instant support during working days.

### 5.5 Updates

5.5.1 GU commits to upgrade computer labs with required updating of software, subscription of new software, replacing hardware, developing new lab to comply with the academic and administrative operations of the university.

5.5.2 System updates are tested and implemented 1-2 weeks before the beginning of every semester.

5.5.3 Upgrade in IT Facilities/resources: For hardware upgrade is done in every 3 years, for software upgrade is done in annually.

5.5.4 Replacement of IT devices: up to maximum 7 years depending on the status of the device

5.5.5 Replacement of server: Maximum 7 years

5.5.6 ITD records, maintains and updates database of the software and service subscriptions.

## 6. Responsibilities

**ITD is responsible for:**

- following and appropriate implementation of this policy.

**Academic and administrative staff are responsible for:**

- appropriate implementation of this policy.

**Heads of Departments are responsible for:**

- ensuring that all faculty members are fully informed of this policy.
- appropriate implementation of this policy.

**Head of all University constituents are responsible for:**

- appropriate implementation of this policy.

**University Policy Development and Review Committee is responsible for:**

- systematic review of the effectiveness of this policy.

## 7. Related References and Standards

| | |
|---|---|
| **BQA** | Institutional Reviews Handbook |
| **BQA** | National Qualifications Framework Handbook |
| **BQA** | Programs-within-College Reviews Handbook |
| **HEC** | Institutional Accreditation Standards Handbook |