الجـــامعـــة الخـــليجـــية
GULF UNIVERSITY

**Title: Information Security Procedures**

**Code:** GU-PR53INFOS

**Version:** 3.1

**Date of Issue:** 2023

**Effective Date:** November 2023

**Approval Authority:** University Council

**Document Owner:** IT Department

**Review:** The procedures are subject to periodic reviews as per amendments of Information Security Policy and University Policies/Regulations

## 1. Purpose

The purpose of this document is to describe information security procedures at Gulf University. It details principles to manage information security and maintain appropriate security controls in the information processing resources and facilities.

## 2. Scope

The document applies to all users of information at Gulf University.

## 3. Acronyms

| | |
|---|---|
| **BQA** | Education and Training Quality Authority |
| **GU** | Gulf University |
| **HEC** | Higher Education Council |
| **IS** | Information Security |
| **ITD** | Information Technology Department |

## 4. Definitions

**Availability:** Availability means ensuring that authorized users have access to information and associated assets when required.

**Confidential:** Confidential means information that is accessible only to authorized personnel.

**Critical:** Critical means information that is essential to carry normal operational processes of the institutions.

**Information Asset:** Includes all resources that has a value to the university.

**Sensitive:** High classified information for the university associated with authorized access.

## 5. Procedures Details

**5.1 Accessing & Protecting Data:** Gulf University implement the following configuration procedure to protect data, privacy and confidentiality:

5.1.1 ITD implements a Single Sign On (SSO) for all systems under the campus management platform to enable backend data protection.

5.1.2 ITD enforces Multi Factor Authentication (MFA) for all staff and enables the same for all students to ensure secure access to information, data, and preventing unauthorized access.

5.1.3 ITD accepts third party systems that can only integrated seamlessly with main systems in campus to ensure a smooth data synchronization.

5.1.4 ITD limits the disclosure of faculty information to what is necessary for official purposes only, for instance faculty directories may include basic contact information (name, office location, email).

5.1.5 ITD adds confidentiality articles as in agreements, memorandums, contracts and where applicable.

**5.2 Incidents Respond:**

5.2.1 Colleges, units and departments across the university shall cooperate with ITD in case of any incident relevant to Information Security.

5.2.2 End users shall report any information security incidents, breaches, suspected incidents, breaches or potential control weaknesses to the ITD.

- Identification: Detect any incident by observing any service disruptions or behavior that impact end user, colleagues or students, and inform ITD immediately.
- Categorization: Once an incident is identified and sent, ITD will determine if it is hardware, software, security, or something else.
- Prioritization: ITD will prioritize the incidents based on the impact and urgency. Some incidents may require immediate response, while others can wait.
- Response: ITD will deal with every incident depending on the impact, this could involve quick fixes, workarounds, or temporary solutions. IT Manager must escalate high impact incidents to the management promptly.
- Closure: ITD must have a record/logs for all incidents, including date, type, impact, actions taken and closure date.

### 5.3 Information Security Responsibilities:

5.3.1 Colleges, units, departments and all end users across the university shall cooperate with ITD in implementing and maintaining the desired level of information security by:

- identifying, agreeing and implementing specific methodologies and processes related to information security including assessment of risk and assigning security classification to information systems assets.
- agreeing and assessing the adequacy of organization wide security initiatives.
- coordination of information security initiatives for new systems, including information security in the information systems.
- promoting organization wide support for information security.

5.3.2 GU shall formulate an Information Security Steering Committee comprising a cross functional mix of top management personnel.

5.3.3 IT Manager shall call for a meeting with the Steering Committee whenever any discussion amongst information security, major security incidents and recovery capabilities.

5.3.4 ITD shall have the overall responsibility for the development and implementation of information security and related control processes.

5.3.5 ITD shall implement security and protection controls for all information asset. Assets shall be handled by assets owners. The level of protection to be provided to the asset shall depend on its classification in accordance with Asset Management Policy and the following activities:

- the assets and security processes associated with each individual system must be identified and defined.
- asset ownership shall be agreed upon and the level of responsibility shall be documented.
- authorization levels shall be defined and documented.

5.3.6 ITD shall hire individuals with relevant expertise in the various aspects of information security to provide GU with specialist information security advice on a continuous basis.

5.3.7 ITD shall also 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, due to the wide area of expertise and skill sets required to maintain an appropriate level of information security.

5.3.8 ITD shall be the specialist service department and shall be segregated from other departments. Due to the requirement for separation of duties, an individual assigned to the ITD must not also be assigned to any other role.

## 6. Responsibilities

**Academic and Administration Staff Members are responsible for:**

- following this document appropriately

**IT Department is responsible for:**

- appropriate implementation of this document

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

- systematic review of the effectiveness of this document.

## 7. Related Policies

- IT Policy

## 8. Related Procedures

- Access Control Procedures
- Assets Management Procedures

## 9. Related References and Standards

| | |
|---|---|
| **BQA** | Institutional Review Handbook |
| **BQA** | National Qualifications Framework Handbook |
| **BQA** | Programs-within-College Reviews Handbook |