الجامعة الخليجية

GULF UNIVERSITY

Title: Access Control Procedures

Code: GU-PR58ACC

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 IT Policy

1. Purpose

The purpose of this document is to describe Access Control procedures at Gulf University. It details principles to set guidelines of access control for users, systems, and accounts.

2. Scope

This document applies to all university users on campus. Also, it covers the responsibilities of users including staff members (full-time and part time academic and administrative), students and GU alumni members, vendors, and all visitors.

3. Acronyms

BQA	Education and Training Quality Authority
GU	Gulf University
HEC	Higher Education Council
HOD	Head of Department
IT	Information Technology
ITD	Information Technology Department
SM	Social media

4. Definitions

Account: Account means the username and password provided by the Information Technology Department.

System Account: System account means an account that has a special purpose related to application or system administration.

5. Procedure Details

5.1 Provisioning User Accounts

5.1.1. A new user account request initiated by the Human Resources Department to the ITD.

5.1.2. ITD personal will create the account and share first-login credentials with end user.

5.1.3. Users must set their passwords according to Password Policy.

5.1.4. Multi Factor Authentication (MFA) is configured on a conditional policy basis for all staff and accessible systems.

5.1.5. Users must accept the User Confidentiality Agreement.

5.1.6. Other accounts required by colleges, units and other departments should be requested to ITD according to User Accounts Procedure, with reason and validity justification.

5.2 Provisioning System Accounts

5.2.1. User Accounts for systems and applications is created as per job role and/or requested by management, Deans and Heads of Departments.

5.2.2. System Accounts users must maintain confidentiality as in line with User Accounts Procedure.

5.2.3. The IT Manager must approve any temporary accounts before creation.

5.2.4. ITD should reset/disable any default passwords.

5.2.5. User and System Accounts are logged and tracked using Azure Cloud Tools frequently and periodically to ensure security and integrity.

5.2.6. All system accounts have default group privileges; Dean/HOD can request further privileges to ITD as per role requirements.

5.2.7. Account Deactivation: Account Deactivation requests are initiated by the Human Resources Department by sending a request by email or service request to ITD.

5.3 Physical Access

5.3.1. All university students, staff, visitors must wear ID Card during their work/study on-campus.

5.3.2. Security personnel must not allow students and visitors to access the campus without wearing an ID Card.

5.3.2. Vendors and contractors must get permission from the Facilities Department to enter campus.

5.3.3. Employees and students must notify security personnel whenever they encounter suspicious visitors or any unidentified personnel.

6. Responsibilities

Staff Members and Students are responsible for:

- Following this document appropriately.

HODs, Deans and Managers of Administrative Departments are responsible for:

- Following this document appropriately.

IT Department is responsible for:

- Appropriate implementation of this document

Vice President for Academic Affairs is responsible for:

- Ensuring 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

- Asset Management Policy

8. Related Procedures

- No Related Procedures

9. Related References and Standards

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