Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Vice President of Administration and Finance
Implementing Authority: Information Technology Department
Effective Date: February 2024
Review: January 2025

IT Access Standards Policy & Procedures

1.0 Purpose

1.1 This policy provides guidelines and rules that govern the access and use of Information Technology (IT) resources in a secure manner.

1.2 Establish standards and requirements for access to information technology resources within the company. These standards ensure that access to computer systems, networks, applications, and data is provided and managed in a secure, consistent, and efficient manner.

1.3 The main objective is to protect the organization's IT infrastructure, protect sensitive data, and support the organization's operations effectively.

2.0 Scope

2.1 This policy applies to all university staff, faculty, students, and any other individuals granted access to the university IT resources.

2.2 The IT access standard applies to all personnel, be it employees, contractors, partners, or authorized persons who need to access the organization's IT resources.

2.3 This standard pertains to the access of various systems, networks, applications, databases, and digital assets owned or managed by the organization.

3.0 Definitions

3.1 Access Control List (ACL) - a list specifying the access rights granted to specific users or groups for individual IT resources.

3.2 Access review - a periodic assessment of user access rights to determine the continued need for access and to revoke unnecessary or inappropriate access.

3.3 Access roles - are sets of permissions that determine the actions an authorized user can perform on IT resources. They establish guidelines, policies, and procedures that regulate the granting, management, and withdrawal of access rights for computing resources within an organization. These standards define the protocols, safeguards, and accountabilities related to user identification, authorization, and access control.

3.4 Authentication mechanism - this is a procedure utilized to confirm the identity of a user who is asking for access to IT resources.

3.5 Authorization - the process of granting specific access rights and privileges to users based on their job roles and responsibilities.

3.6 Multi-Factor Authentication (MFA) - a security measure that requires users to provide two or more forms of identification before gaining access to IT resources.

3.7 User account - an individual's unique identity and credentials used to access the University's IT resources.

4.0 Policy

4.1. Access standards have been established to ensure proper user permissions and audits. These standards outline the criteria for user identification, password complexity, and multi-factor authentication to authenticate user identity and guarantee accessibility of computing resources.

4.2 The access policy strictly enforces the least privilege principle, ensuring that users are granted only the level of access necessary to complete their tasks. Access privileges are determined based on roles, functions, and business requirements, leaving no room for unauthorized access or misuse.

4.3 To maintain proper control and restriction of IT access, specific standards must be adhered to. These standards include considerations of user roles, economic impact, and security settings, managed through technologies like access control lists and permissions. Non-compliance with these standards will lead to severe repercussions.

4.4 The principle of segregation of duties is applied in IT access principles to avoid conflicts of interest, fraud, or unauthorized access.

4.5 Access standards primarily focus on monitoring and auditing processes to maintain strict surveillance of access activities, detect security vulnerabilities, and guarantee strict compliance with access policies. These standards establish a structured framework for entering access programs, conducting regular access audits, and enforcing audit controls to ensure accountability and promptly address any security concerns.

4.6 IT accessibility standards prioritize employee training and awareness programs to educate individuals about their responsibilities, proper use of approved IT resources, and security best practices.

5.0 Procedures

5.1. The IT department is responsible for maintaining the university's computer infrastructure inventory, encompassing hardware, software, networks, and data.

5.2 Meticulous documentation of each asset's location, specifications, and ownership information is imperative. Regular audits must be conducted to guarantee the inventory's accuracy and completeness.

5.3 The IT department has a critical responsibility to establish, organize, maintain, and supervise the IT infrastructure. Proper categorization of resources based on sensitivity level enables the determination of appropriate security measures and access restrictions.

5.4 Regular maintenance programs such as software updates, patches, and hardware maintenance must be implemented without fail to ensure optimal performance and resource protection.

5.5 The university's IT department is meticulous in granting access to IT resources, solely based on the roles and functions of staff members. Only essential resources are provided access, strictly adhering to the principle of least privilege.

5.6 IT regularly reviews access services and audits to ensure they meet changing requirements. User activity, access rights, and audit procedures are evaluated periodically, and updates are made as needed based on the results.

5.7 Employees must utilize computing resources properly, strictly adhering to university policies and procedures. Training programs and awareness campaigns effectively educate employees on these policies.

5.8 Users are responsible for protecting their personal information, such as usernames and passwords, and avoiding sharing them with unauthorized individuals. Any attempt to bypass security protocols or engage in cybersecurity attacks is strictly prohibited.

5.9 Consistent and thorough monitoring and assessment of the IT infrastructure are imperative to ensure strict adherence to policies, swiftly detect and address any security concerns, and proactively identify potential risks or vulnerabilities.

5.10 Deployment of highly effective monitoring systems and tools, meticulous scrutiny of system operations and records, and rigorous periodic audits are necessary to maintain a continuous and up-to-date security status of the IT infrastructure.

Related Policies and Documents

Acceptable Use of Computing, Information, and Technology Resources Policy & Procedures
Data Standards Policy & Procedures
Privacy and Confidentiality Policy & Procedures
Record Retention and Management Policy & Procedures