Classification: Information Management and Technology
Approving Authority: President
Responsible Authority: Vice President of Administration and Finance
Implementing Authority: Information Technology Department
Effective Date: May 2025
Review: April 2028

IT Computer Centers - Policy & Procedures

1.0 Purpose

1.1 The main purpose of the IT Computer Centers Policy is to establish guidelines and regulations for the efficient and secure use of AUIB computer centers. This policy serves as a framework to ensure the proper management, operation, and maintenance of the computer centers.

2.0 Scope

2.1 This policy applies to all users who access and utilize the AUIB computer centers, including but not limited to employees, students, and third-party vendors.

3.0 Definitions

3.1 Acceptable Use Policy - a set of guidelines and rules defining the acceptable and responsible use of computer center resources. The policy outlines the behaviors, activities, and practices that users must adhere to when utilizing computer center facilities, equipment, networks, and data.

3.2 Access control - the process of managing and regulating user access to the computer center resources. Access control includes granting and revoking user privileges, enforcing authentication mechanisms, and implementing authorization policies to ensure that only authorized individuals can access specific resources.

3.3 Computer center - a dedicated facility or area within an organization or institution that houses computer systems, servers, networking equipment, and associated infrastructure required for data processing, storage, and communication.

3.4 Help desk support - the procedures followed by the help desk or technical support team to help and troubleshoot computer-related issues. Help desk procedures may include ticketing systems, escalation procedures, remote assistance, and user communication protocols to efficiently address and resolve user problems.

3.5 Incident response - the structured and coordinated approach to detecting, investigating, mitigating, and recovering from security incidents or operational disruptions within the computer center. Incident response procedures aim to minimize the impact of incidents, preserve evidence, restore services, and prevent similar incidents in the future.

3.6 Network configuration - the process of setting up and configuring computer networks, including routers, switches, firewalls, and network protocols. It involves determining IP addresses, subnet masks, DNS settings, and network access controls to establish a secure and reliable network infrastructure.

3.7 Software deployment - the procedures for deploying, installing, and configuring software applications on computer systems or networks. Software deployment may involve

creating deployment packages, testing compatibility, coordinating rollout schedules, and ensuring proper license compliance.

3.8 System administrator - authorized personnel responsible for the management, configuration, and maintenance of the computer center infrastructure, including servers, network devices, and associated software. System administrators ensure the proper functioning, security, and availability of the computer center.

3.9 System administration - the process of managing and maintaining computer systems, networks, servers, and software applications to ensure their proper functioning, security, and performance. It involves tasks such as user management, software installation, system updates, and troubleshooting.

3.10 System monitoring and performance tuning - the procedures for monitoring computer systems, networks, and software applications to ensure their optimal performance and availability. System monitoring procedures involve collecting performance metrics, analyzing system health, and taking proactive measures to address potential issues or bottlenecks.

3.11 User - an individual who has been granted authorized access to the computer center and its resources. Users may include employees, students, or any other individuals with approved privileges.

3.12 User access management - the procedures related to granting and managing user access to computer systems, networks, and software applications within the computer center. This includes creating user accounts, assigning appropriate access privileges, managing passwords, and deactivating accounts when necessary to maintain system security and protect sensitive information.

4.0 Policy

4.1 Implementation of robust security measures, such as access controls, encryption, intrusion detection systems, and regular security audits, to protect the computer center against unauthorized access, data breaches, and other security threats.

4.2 Users are responsible for maintaining the security of their accounts and adhering to the security policies and guidelines set forth by the organization for the computer center.

4.3 The security of the computer center and its resources is of utmost importance. All necessary measures will be taken to ensure the confidentiality, integrity, and availability of data and systems within the computer center.

4.4 Computer center resources are to be used responsibly and in accordance with the organization's acceptable use policy.

4.4.1 Users are expected to comply with applicable laws, regulations, and ethical standards when utilizing computer center facilities, equipment, networks, and data.

4.4.2 Misuse or unauthorized access of computer center resources is prohibited and may result in disciplinary action.

4.5 The organization is committed to protecting the privacy and confidentiality of data processed and stored within the computer center.

4.5.1 Measures such as data encryption, access controls, secure data transmission protocols, and data classification will be implemented to safeguard sensitive information within the computer center.

4.5.2 Data retention and disposal policies will be established to ensure compliance with applicable data protection regulations and minimize the risk of unauthorized data disclosure within the computer center.

4.6 Regular audits and assessments will be conducted to assess compliance and identify areas for improvement within the computer center.

4.7 Policies, procedures, and controls specific to the computer center will be regularly reviewed, evaluated, and updated to address emerging risks, vulnerabilities, and best practices.

4.8 Feedback from users and stakeholders will be encouraged and considered to drive improvements and enhance the overall effectiveness of the computer center.

4.9 Clear lines of communication will be established, and information sharing will be promoted to ensure timely coordination, incident response, and problem resolution within the computer center.

4.10 Regular meetings, training programs, and feedback channels will be utilized to foster teamwork and maintain effective communication within the computer center.

5.0 Procedures

5.1 The Computer Center Manager/Director oversees the computer center's operations, establishes and enforces policies, and provides strategic direction aligned with organizational goals. They allocate resources, monitor system performance and security, and collaborate with other departments to ensure seamless integration of services and support within the computer center.

5.2 System administrators manage computer systems, networks, servers, and software applications within the computer center, ensuring proper functioning and security through installation, maintenance, monitoring, and user account management. They also collaborate with other IT teams to maintain integrated systems and network infrastructure within the computer center.

5.3 Network administrators design, implement, and manage the computer center's network infrastructure, configuring and maintaining network devices and optimizing performance within the computer center.

5.4 Help Desk/Technical Support Staff offer technical support and assistance to computer center users, promptly responding to inquiries, troubleshooting problems, and documenting requests and incidents using a ticketing system within the computer center.

5.4.1 Establish a help desk system within the computer center to receive, track, and address user inquiries, issues, and requests.

5.4.2 Assign and prioritize support tickets within the computer center based on severity and impact.

5.4.3 Respond to user inquiries and provide technical assistance in a timely and professional manner within the computer center.

5.4.4 Escalate complex or unresolved issues within the computer center to the appropriate technical teams for further investigation and resolution.

5.4.5 Maintain a knowledge base of common issues and resolutions specific to the computer center to facilitate self-service user support.

5.5 Create and manage user accounts for employees using the computer center, ensuring appropriate access levels and permissions within the computer center.

5.5.1 Activate and deactivate user accounts based on employee onboarding, transfers, and departures within the computer center.

5.5.2 Enforce strong password policies and periodic password resets to enhance account security within the computer center.

5.5.3 Provide user account-related support, including password resets, account unlocks, and access troubleshooting within the computer center.

5.6 Schedule regular maintenance windows to perform system updates, patches, and upgrades within the computer center.

5.6.1 Test and validate updates in a controlled environment before deploying them to production systems within the computer center.

5.6.2 Document maintenance activities, including backup procedures, rollback plans, and change logs specific to the computer center.

5.6.3 Communicate planned maintenance to users in advance, minimizing disruptions to services within the computer center.

5.7 Develop and implement a data backup strategy to ensure regular and secure backups of critical data within the computer center.

5.7.1 Define backup schedules, retention periods, and backup storage locations specific to the computer center.

5.7.2 Perform periodic data backups and verify their integrity and recoverability within the computer center.

5.7.3 Test and document data recovery procedures to ensure timely restoration in the event of data loss or system failures within the computer center.

5.8 Establish an incident management process to respond to and resolve IT-related incidents within the computer center.

5.8.1 Classify incidents based on severity and impact within the computer center to prioritize response efforts.

5.8.2 Investigate and diagnose incidents within the computer center, identifying root causes and potential solutions.

5.8.3 Document incident details, resolutions, and lessons learned for future reference and improvement within the computer center.

5.8.4 Communicate incident updates to affected users and stakeholders within the computer center in a transparent and timely manner.

5.9 Implement a change management process to control and manage changes to IT systems and infrastructure within the computer center.

5.9.1 Evaluate and assess proposed changes within the computer center, considering potential risks, impacts, and benefits.

5.9.2 Plan and schedule changes within the computer center, ensuring appropriate testing, approvals, and communication.

5.9.3 Implement changes in a controlled and coordinated manner within the computer center, minimizing disruptions and ensuring proper documentation.

5.9.4 Conduct post-change reviews and analysis within the computer center to assess the effectiveness and impact of implemented changes.

5.10 Maintain an inventory of IT assets specific to the computer center, including hardware, software, licenses, and warranties.

5.10.1 Track asset details specific to the computer center, such as purchase dates, locations, and assigned users.

5.10.2 Conduct regular asset audits within the computer center to ensure accuracy and compliance with licensing agreements.

5.10.3 Properly dispose of retired or obsolete assets within the computer center following appropriate data sanitization and environmental guidelines.

5.11 Develop and enforce IT security policies and procedures specific to the computer center to protect systems, networks, and data.

5.11.1 Implement security controls specific to the computer center, such as firewalls, antivirus software, and intrusion detection systems.

5.11.2 Regularly update security measures to address emerging threats and vulnerabilities.

5.11.3 Conduct security awareness training for employees to promote safe computing practices.

5.11.4 Monitor and investigate security incidents, responding promptly to mitigate risks and prevent future occurrences.

Related Policies and Documents

Acceptable Use Policy
Access and Permissions Policy
Data Collection and Handling Policy
Incident Response Policy
Information Security Policy
Privacy and Confidentiality Policy