Information Technology Policy

Policy Owner	Director of IT	Responsible Office	Office of IT
Approved By	Chief Operating Officer	Effective Date	Nov. 2019
		Next Review Date	Jul. 2022

Office of IT

Ajman University (AU) provides computing, networking, information, and telecommunication resources to the University community to support teaching and research, and efficient administrative processes. Access to Information Technology resources is granted to members of the University community who are enrolled students, employees, or academic members. The authorized Office for running these resources is the I.T:

Helpdesk Service

Helpdesk is responsible for serving as the first point of contact for users' technical assistance over the phone or email, logging all the requests/complaints, categorizing them, and then assigning the technician/engineer for the advanced/unresolved cases.

Support Unit

The support unit consists of two teams below; their daily operational task is to resolve technical problems reported by users through the Helpdesk.

a) **Technical Support team:** Responsible for installing, configuring, and troubleshooting new end-user devices such as, but not limited to, PC and printers.

b) **AV/IT technician Team:** Responsible for installing, configuring, and troubleshooting AV equipment such as, but not limited to, datashow, smart screens, CCTV system, Queue system, and Access Door system.

Programming and Development Unit

This unit is responsible for creating and maintaining database applications in support of different AU services and attending to the needs and requirements of the users. Examples of these services include Admissions & Registration, and databases developed for the Office of Finance.

Systems & Network Administration Unit

The main responsibilities of this unit consist of maintaining the following:

- **IT Network/Telecomm infrastructure**: Configuring the network services, and performing day-to-day management of the network, network interfaces, and network services.

This includes but is not limited to LAN connection between campus's buildings, if available, and Internet Connections, with Internet Service Providers (ISP) such as Leased line and ADSL connections.

- IT Systems infrastructure: Installing, configuring, troubleshooting, and managing systems' infrastructure, physical, virtual environment, and Cloud environment, if available. This includes managing the OS systems such as, but not limited to, Win Servers, Linux, databases.
- IT Security: Installing, configuring, troubleshooting, and managing systems' security such as, but not limited to, the antivirus/Antimalware systems, Network Firewall, Application Firewall, and systems' patching and updates.

Another task of this unit is to solve problems that might arise while using the network and systems' services.

Teaching & Learning Unit

The primary role is to manage and facilitate the implementation of institutional strategy for academic and administrative staff across the University.

The Teaching and Learning section at the Office of IT is working closely with the Vice Chancellor of Academic Affairs (Teaching, Learning, and Students), and with Faculties, and other administrative offices.

The main responsibility is to provide support and guidance on how to use AU Applications/systems, including the E-Learning Management System, to the AU community, staff, and students.

The objectives of the teaching and learning team are the following:

- The technology used in the classrooms and computer labs.
- Tools to enhance the communication between the faculty and students.
- E-Learning Management System, including training to faculty members on how to use it.
- E-Assessment which includes the following assessment activates each semester:
  - Advisor
  - Course
  - University's service.
  - And;
  - IT Orientation documents for AU's members, students and staff, on all AU's services and Applications, and how to access/use them.

This section is responsible for the following:

- Create, update and maintain the IT orientation manuals for AU staff and students.
- Give individual and group training sessions.
- Organize training sessions with the Office of HR for faculty members on the newly introduced technology.

Information Technology Services

a. IT Account Services
b. Helpdesk and Support
c. Campus LAN/WAN Network.
d. Video Conferencing.
e. Software and Applications.
f. Internet
g. Teaching and Learning.
h. IT Security, Compliance, and Governance.

Terms and Conditions of using I.T. services

- Office of I.T considers all temporary and permanent connections via the University network, to be subject to the provisions of this policy.

- Computing resources not owned or approved by AU may not be connected to the University's network.

- Office I.T. currently maintains a variety of UNIX, Win 2012 servers, and above. MS Windows systems exist to facilitate software distribution and printing for office and student lab environments.

- The Office of I.T. has the right to monitor the traffic of all transmissions on networks maintained by the offices at all times.

- Operating systems currently supported (for the desktop) include Windows 8 and Windows 10. There are special requirements for Unix workstations in the School of Engineering. Upgrading will take place in a controlled manner.

- Software and hardware to be installed should be requested by the Dean or Manager/Director of Office and it may not be installed or connected to University systems without the approval of the IT Committee. This includes the data and telephone networks.

- All University affiliates (faculty, staff & students) are permitted to use the University network and selected computing resources at all times while the network is available.

- IDF rooms are under the authority and responsibility of the Office of IT. Everyone within the AU Network community who uses University computing and communications facilities has the responsibility to use them in an ethical, professional and legal manner.

- Violations of information technology Policies & Procedures typically result in University disciplinary action, which may have serious consequences, and in some cases, may result in legal action.

- Copying software is an act of copyright infringement and is subject to civil and criminal penalties. It is considered Software piracy, and it is illegal whether you use the copied software yourself, give it away, or sell it. Aiding piracy by providing unauthorized access to software or to serial numbers used to register software can be illegal

Policies & Procedures for using I.T. services

The policies and procedures of the Office of IT have been developed and implemented with the main aim of providing IT resources and services to all its users efficiently and effectively. These policies and procedures have been classified into the following categories:

a. IT Account Services

The Office of IT is providing several services mentioned below that are personalized to AU staff and students. Accounts are intended to be personal. The individual to whom the account has been created is responsible for ensuring that his/her username and password remain confidential. No one is allowed to use another person's username and password.

➢ AU User Account (Staff members)

AU full-time members should have Passwords/User Account. It will be created automatically after adding the employee to the HR system. The employee should receive a letter and email with his/her Password/User Account details and how to use it. The created password will be used at the first login only, and then the user should reset it.

Part-timers may request Password/User Account for each service independently. It will be created temporarily for one semester, and then it will be disabled automatically. The user may call the Helpdesk to reactivate it. The Helpdesk should contact the Office of HR first to confirm that the user is still working for AU. The staff members may contact the Helpdesk to reset the password in case of losing it.

The cancelation process for the full-time employees will be done automatically when the employee completed the clearance process and his/her status is changed to inactive on the HR System. However, the Office of IT may disable the access to AU’s services before completing the clearance process without notice under the below conditions, when there is a risk of sabotaging the data, corrupting, or abusing any of the systems/services:

The employee has Admin privilege or power user on any of AU systems.

The employee has been dismissed for ethical reasons.

The line manager requested to disable the User Account of resigned/dismissed employee.

AU user may use the AU User Account to access the below services:

- AU LAN/WAN Network
- Email
- AU Applications and shared resources.

AU Student User Account

All freshmen students should receive by email an identification letter with their Password/User Account details and how to use it after the drop/add period of each semester.

The student may use the user account to access all the below AU web services:

- Computer labs.
- Wi-Fi
- Email
- E-Learning Management System (Moodle)
- Online Systems, such as ORS (E-Request) system and Banner Registration system.

The student email remains active as long as the student is enrolled at an academic program. The email will be either transferred to alumni email service after graduation or will be disabled if the student is discontinued.

The Alumni email service is managed by the Alumni Office at AU.

b. Helpdesk and Support

The user should contact the helpdesk to log a request either over the phone or by email, then accordingly, a work order should be queued in the tracking system, and the user request will be processed within a predefined time assigned by the tracking system automatically according to the request priority. The request will be escalated management level in case it is not resolved within the assigned time.

The Helpdesk has three levels to handle the user requests.

- ***First Level:***

Provides resolutions that often belong to a knowledge base accumulated from previous experiences.

- ***Second Level:***

In case the request has not been completed, it will be escalated to the second, higher, level that has the necessary resources to handle more difficult specialized requests.

- ***Third Level:***

AU also has a third, higher, level, line of support which often deals with software-specific needs, such as updates and bug fixes that affect the client directly.

The assigned technician should log the case details, and how he/she has resolved it, and then close the order.

The tracking system will send to the user an email automatically upon closing the order informing them that the request has been resolved and the order is closed.

Please see the below documents for more details on the Helpdesk (Service Desk) processes:

- How the Helpdesk (Service Desk) manage the Incidents: Please see the Incident Management Policies and Procedures
- How the Helpdesk (Service Desk) manage the problems: Please see the Problem Management Policies and Procedures
- How the Helpdesk (Service Desk) handles the Change request: Please see the Change Management Policies and Procedures.

c. Campus LAN/WAN Network

The IT Network policy and procedures have been developed to provide students, faculty, and staff access to a reliable, robust, and integrated wireless network and to enhance the security of the campus wireless network to the maximum extent possible.

- All campus users are subject to the following wireless guidelines as well as existing guidelines for the wired network. The wireless network is an extension of the existing network and therefore falls under the control and supervision of the Office of IT. Due to the complex nature of wireless technologies, users of the wireless network must follow the guidelines and policies outlined in the following.
- All campus network users must register with the Office of IT to obtain a user account and a password. The purpose of user accounts and passwords is for authentication of users and tracking users and devices, not to limit access. An employee or Faculty/Office/Unit must register guests and part-timers. Guest/part-timer user account shall be issued for a limited period.

- Wireless networks are NOT a replacement for wired networks. The purpose of the wireless network is to extend the wired network by providing Web browsing and e-mail access in areas of transient use such as common areas. Wireless networks have a much smaller bandwidth than wired networks; therefore, applications that require a large bandwidth may overload the wireless network. Wireless networks work best when the number of users is limited - the more users, the smaller the share of the bandwidth available to each.
- Only wireless hubs installed and managed by IT will be allowed for use on the AU wireless network. Students and faculty are not permitted to install their own wireless networking equipment. Offices wishing to implement a wireless network must notify the Office of IT. The Office of IT will survey the site and determine the feasibility of a wireless connection. Only switches pre-evaluated and installed by the Office of IT will be used.
- Wireless should only be used for mobile computing. Any time wired access is available; it should be used for increased performance.
- Any effort to circumvent the security systems designed to prevent unauthorized access to any AT wireless network may result in the suspension of all access to the AU network and an appearance before the appropriate disciplinary board.

d. The Internet

Internet is a vast, global network linking computers at universities, high schools, science labs, and many other sites. Using the Internet, one can communicate with people all over the world through a number of discussion forums, as well as through electronic mail. In addition, educationally valuable files are available for downloading on the Internet. Because of its enormous size, Internet's potential is boundless. However, with such great potential for education also comes some potential for abuse. It is the purpose of the Office of IT to provide guidelines as well as the contract for use of the AU Internet connection. This is to ensure that all who use the AU Internet connection, both students and faculty, use this valuable resource in an appropriate manner.

The most important prerequisite for someone to receive an account on the AU Internet connection is that he/she take full responsibility for his/her own actions. AU Office of IT, along with the other organizations sponsoring this Internet linkup, will NOT be liable for the actions of anyone connecting to the Internet through this hookup. All users shall assume full liability — legal, financial, or otherwise — for their actions.

Individuals who use the computer facilities of the AU Internet connection must use these resources in an appropriate manner. Misuse of computer facilities is a violation of the AU IT "Acceptable Use Policies" and may also be a violation of the law if data of other computer users are disturbed or the privacy rights of individuals are violated. In addition, the AU Office of IT takes no responsibility for any information or materials transferred through the AU Internet connection.

All users of AU Internet connection are therefore required to comply with the following:

- No obscene or offensive material shall be entered into or sent through the AU Internet connection, websites, whose access is prohibited by ETISALAT in UAE, are also prohibited in the Internet labs.
- Users shall not deliberately attempt to degrade system performance or capability.

- Loopholes in computer systems, knowledge or special passwords shall not be used to damage a system or file, or to change or remove information in a system or file without authorization.
- Reconfiguring the hardware arrangement by unplugging cables and moving hardware from one workstation to another is absolutely prohibited.
- Online chatting, food, drinks, and smoking are forbidden in the computer lab.
- Only one person at a time can use the lab computer, and No one has the right to reserve a PC for anyone.
- The Student may use the printer in the computer lab, if available, and print up to 20 pages per day any material related to his/her subject of study, under the supervision of a lab supervisor.
- Users have the right to complain about the Internet lab supervisor if they see any abuse of the above rules, complaints are to be submitted to the network manager, the Helpdesk phone 06 - 7056500.

e. Teaching and Learning

The University aims to provide higher education of a quality and kind that will enhance the capabilities, potential and intellectual independence of its students, on a life-long basis. The University's continued commitment to respect, preserve and enhance knowledge, skills, and competencies, through a student-centered teaching and learning approach demonstrated through integrity and quality in the delivery of quality learning content, applied research supervision and assessment of student learning outcomes in both the undergraduate and graduate programs.

The University has a number of policies and procedures that govern teaching and learning practice:

- All users of the learning and teaching tools and resources must adhere to the University's Appropriate Use of Campus LAN/WAN Network policy, and IT Security, Governance, and Compliances Policies mentioned in this document.
- Delivery and access to copyright materials of teaching and learning, including the Learning Management System (Moodle) and orientation documents, must adhere to guidelines in compliance with Copyright Law in effect in the United Arab Emirates. In addition, all other copyright use must comply with University Policy.
- Ajman University is not responsible for the misuse, accuracy, integrity, and/or legality of the content uploaded to the LMS by its students, staff, or faculty. The University is not responsible for content linked to LMS to external websites.
- No users of the LMS must use the system for purposes other than teaching-learning activities approved by the official university bodies. Only sponsored agencies connected to the University including accrediting agency representatives, presenters, and course observers may be granted access to Moodle with approval from the appropriate channels including academic Chairs and Deans or other University Executives including the Vice Chancellor for Academic Affairs or the Chancellor. The Information Technology Office staff should notify the course owner when any external agent is added to the system.
- Access to the LMS is granted to currently enrolled students, instructors, and academic administrators on record for published term courses. Course rosters are generated via official

enrollments in Student Information System (SIS). Course owners and administrators should not grant course access to students not listed in the official roster using student email addresses.

• Faculty and staff hosting a course on Moodle shall comply with all the UAE laws and all institutional rules, policies, and procedures in force.

• Illegal content or content that is in violation of the University's policies or contractual agreements shall be removed from a course account, when requested by the instructor of record or other appropriate academic administrators whose duty is to monitor the content continuously.

User Management and Access to LMS

- All users of LMS must access the system through a designated account, which is provided by the AU IT Office and is the same as the user's University User Account (network username and password).
- The instructor(s) of record (IOR) and students enrolled in a course as listed in SIS will have access to the course site in the LMS.
- Official student enrollments will be managed from SIS including adding new students, student withdrawals, and drops.
- For purposes of program curriculum management and continuous quality control, the College Dean and Head of Department may request course access from AU IT Office and will be granted access to courses to review and perform assessment activity including, but not limited to, viewing learning outcomes, course analytics, and usage.
- Faculty may not create courses/sections on behalf of external users and former students and extend system access to said users for the purposes of pursuing activity unrelated to official University business. Any such accounts discovered will be removed by the IT staff.
- Access to the LMS may be disabled or suspended for users who display inappropriate behavior per the University's Acceptable Use Policy and other guiding policies that define appropriate conduct for University employees and students. Students who misuse the LMS will be referred to the Student Affairs Disciplinary Committee.

f. IT Security, Compliance and Governance

Security:

To increase the level of security at AU Account (Network and email) and AU System, and minimize the level of attacks of viruses, worms, Trojans, and hackers.

Virus Protection:

Viruses and other malware are a constant threat to all computer users. They can be picked up in many different ways. Therefore, the Office of IT applied the below group policy on all AU users and PCs:

- Installed Antivirus and antimalware in all AU's PCs.
- Set policy to push the updates on a regular basis.
- Limited the Admin privilege to the Technical team who are responsible for installing software and applications.

Password Policy and Settings:

The Office of IT has implemented the following security measures on passwords:

- Applied Password Policy and Settings on Network/Email Account:
- Password Policy
- Enforce password history 10 passwords remembered (Password should be different than last 10 used passwords).
- Maximum password age 180 days (Password should be reset after 180 Days).
- Minimum password age 0 days.
- Minimum password length 8 characters.
- Password must meet complexity requirements Enabled (Password should be complex)
- Multi-Factor Authentication (MFA) is enabled.

- Account lockout policy:

Account lockout policy disables a user's account if an incorrect password is entered a particular number of times over a specified period. These policy settings help us to prevent attackers from guessing users' passwords, and they decrease the likelihood of successful attacks on our network.

- Account lockout duration 20 minutes.
- Account lockout threshold 5 invalid login attempts (Account will be locked after the 5th invalid attempt)
- Reset account lockout counter after 20 minutes (the locked account will be unlocked automatically after 20 minutes).

- Applied Password Policy on Desktop:

  Enable Password Screen saver option after 10 minutes of the idle session. This option would force the user if he/she did not use the computer for 10 minutes to re-enter the password. In case another user comes to use the computer, he/she should restart the computer and log in with his/her network account.

Compliance and Governance:

The Office of Information Technology (IT) is neither an investigative nor a disciplinary entity in its primary responsibilities. However, in cases where University resources and privileges are abused or otherwise threatened, the office may be asked to take appropriate steps. Immediate revocation of access and subsequent prosecution by the authorities, for example, might be directed. Such revocation may be appealed to the IT committee.

Another example would be to both discipline and hold accountable an individual who damages IT resources. Improper access or modification of AU information in a computer system may also bring a stiff penalty.

Prohibited acts include but are not limited to the following:

- Threats to the security of information and the integrity of networks at AU and elsewhere include viruses, hackers, and unauthorized persons. Consequently, it is the responsibility of the user not to disclose his/her password to any person.
- It is prohibited to connect any personal computer, server, printer, firewall, network router, network switch, or other electronic devices to the AU data network without the express approval of the IT & Networks Director.

- When any use of information technology at the University presents an imminent threat to other users or the University's technology infrastructure, network & systems administrators may take whatever steps are necessary to isolate the threat, without notice if need be.
- The Office of IT does everything in its power to prevent viruses from entering the AU network. Measures taken include virus scanners on desktop computers, file servers, and email servers. However, users still need to be vigilant about protecting themselves from viruses, such as downloading suspicious files and opening suspicious attachments.
- Any attack or bid to attack the AU systems or networks will result in the prosecution of the attacker according to the federal laws of the UAE.
- Access to IDF rooms and server rooms is limited to IT staff only.
- Intentional denial of computing service to other users.
- The exploitation of insecure accounts or resources.
- Attempting to guess, crack or otherwise determine another user's password.
- Interception of network transmissions with hardware or software "sniffers".
- Forging of electronic mail or electronic news or otherwise misrepresent themselves or other individuals in any electronic communication.
- System administrators are not to use their access to examine the private information of other users except in the course of resolving problems and where access to such information is necessary. In these cases, IT staff are required to seek permission and oversight.
- IT staff may not transfer resources (hardware, software, documentation, etc.) from designated locations without the explicit permission of their supervisor.
- AU employees or students may not load any software onto their workstations or servers, which has not been purchased or is not free. Software identified as "shareware" should be examined carefully to ensure there is compliance with any licensing requirements. Under no circumstances will software binaries from unknown or illegal sources be placed on workstations or servers.
- Under no circumstances will AU employees or students share account passwords, key combinations, alarm codes, keys, access cards, or any other access control mechanism for any University resource or facility with any individual in a manner inconsistent with the policies established by their supervisor. In the absence of such policies, employees must have the explicit permission of their supervisor to share any access mechanism to any office resource.
- IT management reserves the right to audit University-owned workstations and servers without warning for verifying software-licensing compliance.
- AU employees or students may not load or install any software that may abuse the bandwidth of AU Network/Internet.
- All computer and network access are denied unless expressly granted. Access is generally granted by the Office of IT in the form of computer and network accounts to registered students, faculty, staff, and others as appropriate for such purposes as research, education (including self-study), or University administration. University accounts are protected by passwords.
- Accounts are assigned to individuals and are not to be shared unless specifically authorized. You, the user, are solely responsible for all functions performed from accounts assigned to you. Anything done through your account may be recorded. It is a violation of University Policy to

allow others to use your account. It is a violation to use another person's account, with or without that person's permission.

- The password, used with the account, is the equivalent of an electronic signature for the user. The use of a User Account and password authenticates the identity and gives an online affirmation of the force of a legal document. The user should guard the password and account as he/she would his/her checkbook and written signature. It is a violation of this Policy to divulge your password to anyone. It is a violation to attempt to learn the password

  to another person's account, whether the attempt is successful or not.

- The User may not attempt to disguise his/her identity, the identity of your account, or the machine that you are using. The user may not attempt to impersonate another person or organization.

- The User may not attempt to monitor other users' data communications; he/she may not infringe the privacy of others' computer files; the user may not read, copy, change, or delete another user's computer files or software without the prior express permission of the owner.

- The User may not engage in actions that interfere with the use by others of any computers and networks. Such conduct includes but is not limited to: the placing of unlawful information on the system, the transmitting of data or programs likely to result in the loss of the recipient's work or system downtime, the sending of "chain letters" or "broadcast" messages to lists or individuals, any other use that causes congestion of the networks or interferes with the work of others.

- The User may not engage in actions that threaten or intentionally offend others, such as the use of abusive or obscene language in either public or private messages, or the conveying of threats to individuals or institutions by way of AU computers and/or networks.

- The User may not attempt to bypass computer or network security mechanisms without the prior express permission of the owner of that computer or network system. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt.

- The User may not alter, copy or translate software licensed to another party. The user may not make available copyrighted materials without the express permission of the copyright holder. Respect for intellectual labor is vital to the academic discourse. Violations of authorial integrity, plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations may be grounds for university sanctions as well as legal prosecution.

- Anyone who does not abide by the rules above will be referred to the university Law Affairs.

To summarize, access to University computing and communications equipment and facilities may be revoked for reasons including, but not limited to:

- Attacking the security of the system;

- Modifying or divulging private information such as file or mail contents of other users without their consent;

- Misusing or abusing Internet/Network by using Internet tools or software that may affect the performance of the Internet/Network;

- Modifying or destroying University data;

- Using the networks/Internet in a manner contrary to the established guidelines;

- Users who are using a different domain other than the AU domain.

- Software Piracy

Finally, users may not read sensitive information simply because it is accessible to them - because of accidental exposure and/or through the malice of others who have broken into a system or are misusing their access privileges. When sensitive information is recognized as such, it should not be examined further, but reported to the keeper of the materials, if known, or reported to management, if not.

Use of Technology Resources

The Office of IT is responsible for providing and maintaining the IT technologies used in AU's teaching facilities, Classrooms, and Computer labs. Therefore, the Office of IT set the following policy:

- The university ID is to be shown to the computer lab supervisor and the supervisor has the right to check the ID at any time.
- University computer systems shall not be used for commercial purposes without the written authorization of the university's management.
- Files, sign-on, user names, passwords, and computer output belonging to an individual or the institution are considered personal property. Users shall not examine, change, or use another person's files, output, or user names for which they do not have explicit authorization. The same restriction applies to institutional files.
- Students should notify the supervisor if the PC is slow or not working properly; consequently, the supervisor is to notify the Helpdesk if he/she is unable to resolve the issue.
- Users cannot install any programs from the Internet.
- The lab supervisor is the person in charge of enforcing the Internet lab policy.
- All users must log off when their time is over and/or they have to leave the lab.
- All PCs are managed by IT, including the security settings and Virus Protection policy.
- Any software that needs to be installed on computer labs should be reported to the Office of IT. The installation shall be processed as per the request process of the Helpdesk and Support services.
- Anyone who does not abide by the rules above will be referred to the student's affairs.

Maintenance and Replacement of Computing & Network Resources

The policies and procedures of the Office of IT for periodic maintenance, updating, and replacement of computing and network resources are as given below:

1. Periodic Maintenance and Updating:

1.1. The Office of IT is responsible for providing support and maintaining (or arranging maintenance for) all computing and network resources including faculty and staff PCs. It is also responsible for maintaining and upgrading IT resources, hardware, and software, for IT Network infrastructure and AU Data Center.

1.2. In addition to periodic maintenance of computing and network resources provided by the Office of IT, the faculty and staff can contact the Helpdesk of the Office of IT for any needed maintenance. The Office of IT shall respond to the request and carry out the required maintenance job.

1.3. Within its life cycle, as defined in the following section, computers should require maximum of three major software upgrades (operating system or office suite) and should generally not require a hardware upgrade. However, if the user's requirements change, necessitating a change in hardware configuration, only one upgrade (RAM, hard disk, etc.) can be scheduled during the equipment's life cycle.

1.4. For each computing lab:

- The college shall be responsible of obtaining/replacing the PCs in the computer lab and required software in the lab.
- The Lab Supervisor shall be responsible for monitoring the operation of all hardware and software resources in the lab. He/she shall immediately report to the Office of IT of the University about any malfunction of PCs or other computing and network resources. The Lab Supervisor shall also be responsible for general maintenance and for ensuring that students have no difficulty in efficiently utilizing all resources (hardware and software) throughout the semester. In addition, at the end of each semester, all resources in the lab shall be thoroughly evaluated and maintained. In this regard, he/she shall contact the Office of IT for any needed support for periodic maintenance or upgrading at the end of each semester.
- The college shall coordinate with the Office of IT to ensure that all resources in the computing labs of the concerned college are regularly maintained and upgraded, if needed, to the satisfaction of the faculty members, and students.

2. Periodic Replacement :

In general, computers should be replaced in specific situations where the hardware becomes a barrier to the user. This occurs primarily when the University’s standard software suite, or the software required for instruction, service, or research work will not run effectively on the existing hardware. At the same time, it is important to realize that computer replacement is expensive, disruptive and labor intensive for both the end user and the IT staff. Changing computers often requires a migration of data files and ancillary programs from the older units to the new units, and may require relearning software functionality when the computer comes in with newer software versions. Further, adding a new computer with new software versions to an existing office or facility can cause problems when shared files are no longer compatible.

In an effort to balance the need to upgrade with the negative effects of replacement, computer purchasing must be orderly and planned in advance.

The replacement policy outlined here covers all devices used by students, faculty, staff or administrative units.

2.1. Platform and Operating System at AU:

The IT infrastructure at AU is built on Microsoft Technology; therefore, the standard platform and operating systems are as follows:

- Platform:

PC is the standard platform, however, other platforms; such as Apple products, can be supported based on the functional requirements, such as but not limited to; graphic design, video making, and educational purposes.

- Operating System (OS):

  Windows is the recommended OS, however, other OS, such as IOS and Linux can be supported based on the job or educational requirements, under the following conditions:

  a) The device will be connected to internet access and deal as Bring Your Own Device (BYOD).

  b) The access to AU intranet applications, if needed, can be provided with limited options

2.2. Computers purchased should be deployed so they equip entire offices or labs during one purchase cycle. Users within definable networks, classes, offices and areas should all be working with hardware and software of the same vintage, except as follows:

- Some office computers will not have the same software requirements as the rest of the office's equipment. For example, a PC may be a single function device used by a University aide where compatibility or efficiency of use is not a major factor. Here, a recycled PC or a PC replaced less often may be more appropriate as long as the presence of this computer on the network does not inhibit network security or functionality. The computer inventory/replacement schedule will document where these ancillary computers are used.

- Computers should be purchased with enough technical capacity to support the user through the entire life cycle. The selection should seek to balance an increased life cycle resulting from purchasing increased capabilities against the initial cost. The standard PC configuration should not be modified external to the review/approval/involvement of the Office of IT.

3. Ownership and Life Cycle of Computer Devices:

3.1. Computers are the property of the University. When a computer is replaced, it becomes available for reassignment to other uses at the University. Recycling plans are identified in the University’s replacement schedule and will be managed by central and campus staff.

3.2. The standard life cycle of any computer device is five years, including desktop computers, laptops, Mac devices or iPads. The life cycle of lab servers is determined by the application software and shall be established individually.

3.3. Areas that require more contemporary technology may receive new computer devices more often than the standard life cycle. This shall be established in consultation with the College Deans and identified on the replacement schedule.

3.4. The Office of IT is the authorized level to provide technical feedback on the existing devices or recommendations on any requested device. The recommendations include the specifications, platform, OS, model, or brand, which will be primarily based on the user's functional requirements and the use within AU and its IT infrastructure.

According to the above-mentioned Ownership and Life Cycle, the following procedure shall be followed:

- The faculty/staff member is eligible for one device at a time.
- The faculty/ staff member should hand over the old device to the Office of IT upon receiving the new one, where the ownership of the old device will return to AU custody.
- Staff members under the categories mentioned below have the option of choosing between desktop/ AIO or a laptop in coordination with their line managers, while all other categories are eligible for laptops:
  a) Receptionists
  b) Secretaries
  c) Front Desk Staff
- Senior Management, deans, and managers are entitled to request an iPad, in case their job requires such a device.
- Any exception from the above policy shall be reviewed on case by case basis and approved by the top management.

4. Damages/Replacement before the device's standard life cycle:

4.1. Replacement of the device before the end of its life cycle:

The Office of IT will check and provide a technical report, and accordingly, the following policy will be applied:

A. The faculty/ staff member should hand over the old device to the Office of IT upon receiving the new one, where the ownership of the old device will return to AU custody.

B. The user will be responsible for any damage due to misuse.

C. The respective college/ office of the faculty/ staff will be responsible to cover the cost of repair if it is a minor damage (not due to misuse), and the device can be repaired as long as the cost of repair does not exceed 30% of the original cost of the device.

D. The respective college/ office of the faculty/ staff member will be responsible for ordering a new device if the damage is not due to misuse and the cost of repair exceeds 30% of the original cost of the device.

4.2. Replacement of faculty member's laptop after three (3) years:

A. A faculty member sends a request to the Office of IT (helpdesk) to request specifications for the new laptop, with the Ref. No. of the current laptop, and list of needed or used software.
Please note the following:

- Faculty members in the College of Engineering and IT, and Graphic Design in the College of Mass Communications, are eligible for a laptop with higher specifications.
- College Secretary may initiate the request on behalf of the user.

B. The Office of IT Helpdesk will contact the faculty member to check the purchase date of the current laptop to verify the laptop's lifetime, prepare the status report with recommendations, and then send the report to the faculty member/requester.

C. The college secretary should proceed with the purchase processes by issuing the budget request and following the procurement cycle.

D. As soon as the new laptop is delivered, the faculty member should hand over the old laptop and collect the new one from the Office of IT.

5. Replacement and recycling after the maximum life cycle of five years:

5.1. Faculty Members:

The college secretaries will prepare lists of all faculty members who are eligible for new replacement laptops and proceed with the applicable procurement cycle. The Office of Procurement shall verify the eligibility terms and then issue a purchase order after consulting with the Office of IT on the technical specifications.

5.2. Staff Members:

The staff member should contact the Office of IT to check the condition of the device and provide a technical report with recommendations; whether the device needs to be replaced, upgraded, or if it is in a good condition that satisfies the work requirements.

If it is recommended to be replaced, the respective college/ office should proceed with the procurement cycle to purchase the new device.

5.3. The distribution of recycled equipment is to be identified in the replacement schedule and managed by the Office of IT and central representatives for their respective inventories.

5.4. For budgeting purposes, computer replacement should be included as an annual, specifically identified line item in the unit's budget.

5.5. Replacement computers are to be purchased on a University-wide basis.

The Office of IT establishes a standard computer configuration for each purchased device. Some installations require additional options. A procedure will be developed in consultation with the Office of Finance and the Office of Procurement to determine the best options to budget and purchase such devices.

5.6. A replacement schedule will be maintained as part of the University's computer inventory. The inventory/schedule will be maintained through the Office of IT.

5.7. For planning purposes, a computer's projected replacement date should be established when initially acquired.

5.8. Replacement orders will occur within the University's established computer ordering cycles.

5.9. Distribution decisions are made on a University-wide basis in advance of replacement due dates. Upon the installation of a replacement computer, the recycled device is normally returned to the warehouse or campus storage location awaiting redistribution after all new replacement devices are installed.

5.10. Requests for recycled computers should be made to the Office of IT.

5.11. If an additional computer device is needed within an office or college, the unit should first look to acquire a device from stock, of the same vintage as the rest of the unit's equipment. The goal is to keep the entire unit on its initial replacement schedule and all users on the same software versions.

Back up Policy

This policy aims to protect the information assets of AU, and prevent the loss of data in case of accidental deletion or corruption of data, system failure, or disaster. Furthermore, it will help manage and secure backup and restoration processes and the media employed in the process.

Statement

Data Backup is the responsibility of the Office of I.T. who defined which data/information to be backed up, the Recovery Point Objective, and the Retention time.

All backed-up data/information is stored locally.

This policy applies to the below-mentioned servers/systems in the Information Technology Department:

- Oracle Database.
- Library System.
- SIS/ORS Database
- HR.NET Database
- Dynamics AX
- Domain Controller (DC) Servers.
- Windows Servers.
- Archiving System.
- E-Learning System; and
- University Website.

The retention periods of information contained within the system-level backups are designed for recoverability and provide a point-in-time snapshot of information; as it existed during the period defined by system backup policies.

Backup retention periods are in contrast to retention periods defined by the business requirements.

System backups are not meant for archiving data for future reference.

Description

Systems will be backed up according to the below schedule:

Data	Backup Type	Time	Location
Banner	Oracle DB Backup	Daily at 22:00	Data Domain

SIS	SQL DB Backup (Full)	Daily at 20:00	Data Domain
Dynamics-AX	SQL DB Backup (Full)	Daily at 20:00	Data Domain
HR-net	SQL DB Backup (Full)	Daily at 20:00	Data Domain
OAS/ ORS	App Data Full	Twice a week (Mon, Fri 20.00)	Data Domain
Library System	SQL DB Backup (Full)	Daily at 20:00	Data Domain
	App Data Full	Twice a week Tues, Sat 22:00	Data Domain
DC Servers	Full Backup	Twice a week Mon, Fri 02:00	Data Domain
Windows Severs	Full Backup	Twice a week Mon, Fri 2:00	Data Domain
Archiving System.	SQL DB Backup (Full)	Daily At 20:00	Data Domain
	App Data Full	Twice a week Mon, Fri 2:00	Data Domain
University Website	Full backup	Twice a week Mon, Fri 20.00	Data Domain
E-Learning System	Full backup	Weekly Thursday 22:00	Data Domain

Backups will be written to Data Domain Appliance and stored in the Data Center.

Daily backups will be maintained for 30 days

Weekly backups will be maintained for a period of three months.

Weekly backups of the systems mentioned below will be transferred to an off-campus location and replaced, on the Cloud side, through the network:

- Banner
- SIS
- MS Dynamic AX
- HR.NET

Monthly backups will be maintained for 12 months.

Avamar System Manager will clean up old backup according to AU Backup Policy.

Media will be retired and disposed of as described below:

- Prior to retirement and disposal, IT will ensure that:
    - The media no longer contains active-backup images
    - The media's current or former contents cannot be read or recovered by an unauthorized party
    - Backups will be verified periodically

On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

To check for and correct errors.

To monitor the duration of the backup job.

To optimize backup performance where possible.

The IT will identify problems and take corrective action to reduce any risks associated with failed backups.

Random test restores will be done once a week, in order to verify that backup shave been successful

The IT will maintain records demonstrating the review of logs and test restores to demonstrate compliance with this policy for auditing purposes.

Data Recovery

In the event of a catastrophic system failure, off-site backed up data will be made available to users within three working days, if the equipment destroyed has been replaced by that time.

In the event of a non-catastrophic system failure or user error, on-site backed-up data will be made available to users within one working day.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made.

Responsibilities

- Backups and Data Recovery for the below-mentioned systems are done by System team members:
  - Banner Oracle Database.
  - Library System.
  - SIS/ORS Database
  - HR.NET Database
  - Dynamics AX
  - Domain Controller (DC) Servers.
  - Windows Servers.
  - Archiving System.
  - E-Learning System
  - University Website

The Oracle Team members do backups and Data Recovery for the Oracle Database, SIS, ORS, and Applications.

Document History

Version	*Date*	*Update Information*	*Author/ Reviewer*
V 1.0	24/10/2010	Initial Policy	University Central Committee
V 2.0	14/07/2013	New Policy with new regulation and guidelines to cover AU systems and services	Director of IT
V 2.1	03/10/2017	Minor review to back-up, maintenance, internet usage	Director of IT
V 2.2	24/11/2019	Minor Review to Paragraph “ Maintenance and Replacement of Computing & Network Resources” – Replacement of faculty member’s laptop after 3 years	Director of IT