جامعة عجمان
AJMAN UNIVERSITY

I.T. Policies and Procedures

Office of IT

CONTENTS

Definitions:

The following definitions apply for the purpose of this policy:

- AU: Ajman University
- IT: Information Technology.
- IT Resources: IT resources include but not limited to the following:
  - Systems such as Archiving System, and Library system.
  - Software
  - Hardware and services.
  - AU Computer labs
  - Staff computers, Desktop or Laptop.
  - Terminals.
  - Modems.
  - Printers.
  - Networks (wired and wireless).
  - Telecommunication devices (landline and mobile phones, PABX, faxes).
  - Storage media and related equipment, and data files owned or managed by the University.
  - Information systems, and;
  - Services such as those on AU network, (for example, internet access).
  - Email (Students and staff).
  - AU systems: All main AU services are running through a series of Applications that are all connected to Databases. These Databases and the applications are supported by a specialized team in the Office of I.T.
- Network and Security: Network hardware and the services operating on the hardware or utilizing the hardware to perform tasks. AU utilizes both wired and wireless networks.
- Passwords/User Account: The mode of secured personal access to pre-determined IT resources.
- User: Any person who makes use of any IT system, hardware or service owned or leased by AU.
- Video Conferences: Providing audio and video facility for the running events in AU and do the control and management during the event
- CCTV: CCTV is (Close Circuit Television) managing two class rooms with the CCTV.
- Technical Support: Providing maintenance service for all staff members and students in AU with it the I.T. resources.
- Application Support: Providing software support for all AU Applications such as SIS, HR, and ERP Systems.
- Help Desk : Help Desk is an information and assistance resource that troubleshoots problems faced by Faculty members, administrative staff and students related to I.T. resources, Network and Security, and Password/User Account.

Office of Information Technology:

Ajman University (AU) provide 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 in both campuses, Ajman and Fujairah. The authorized Office for running these resources is the I.T:

1. **Support Unit:**
   This unit consists of two teams:
   - Technical Support team: Responsible of troubleshooting, their main task is to resolve technical problems reported by users to the Help Desk.
     - Service Desk team: Responsible of serving as first point of contact for users' technical assistance over the phone or email, log all the requests/complaints, categorize them, and then assign the technician/engineer for the advanced/unresolved cases.

2. **Programming and Development Unit:**
   This unit is responsible of creating and maintaining database applications in support of different AU services for both campuses, Ajman and Fujairah, 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.

3. **Systems & Network Administration Unit:**
   The main responsibilities of this unit consists of maintaining the IT infrastructure, configuring AU systems to operate in a network in both campuses, Ajman and Fujairah, configuring the network services, and perform day-to-day management of the network, network interfaces, and network services. This includes maintaining the following:
   - LAN connection between the two campuses, Ajman and Fujairah.
   - LAN connection between campus's buildings
   - Internet Connections, with Internet Service Provider (ISP) such as Leased line and ADSL connections.

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

4. Teaching & Learning Unit:

The primary role is to manage and facilitate the implementation of institutional strategy for excellence in teaching and learning and the AU student experience working with 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 AU community, staff and students.

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

- The technology used on 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 of the following:

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

I.T. Services:

1. IT Account Services
2. Helpdesk and Support
3. Campus LAN/WAN Network.
4. Video Conferencing.
5. Software and Applications.
6. Internet
7. Teaching and Learning.
8. IT Security, Compliance and Governance.

Terms and Conditions of using I.T. services

1. Office of I.T considers all temporary and permanent connections via the University network, to be subject to the provisions of this policy.
2. Computing resources not owned or approved by AU may not be connected to the University's network.
3. 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.
4. Office of I.T. has the right to monitor the traffic of all transmissions on networks maintained by the offices at all times.
5. 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.
6. 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.
7. 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.
8. 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.
9. Violations of information technology Policies & Procedures typically result in University disciplinary action, which may have serious consequences, and in some cases, may result in a legal action.
10. Copying software is an act of copyright infringement, and is subject to civil and criminal penalties. It is considered Software piracy, and It's illegal whether you use the copied software yourself, give it away, or sell it. And aiding piracy by providing unauthorized access to software or to serial numbers used to register software can be illegal.

Policies and procedures of 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 in an efficient and effective manner. These policies and procedures have been classified into the following categories:

1. **IT Account Services:**
   The Office of IT is providing number of 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 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:

     1. Computer labs.
     2. Wi-Fi
     3. Email
     4. E-Learning Management System (Moodle)
     5. Online Registration System (ORS).

2. **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 Help Desk has three levels to handle the user requests.
     1. First Level:
        Provides resolutions that often belong to a knowledge base accumulated from previous experiences.
     2. 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.
     3. Third Level:
        AU also have 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.

3. 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 security of the campus wireless network to the maximum extent possible.

1. 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, it is imperative that users of the wireless network follow the guidelines and policies outlined in the following.
2. 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.
3. 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.
4. 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.
5. Wireless should only be used for mobile computing. Any time wired access is available; it should be used for increased performance.
6. 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 AU network and an appearance before the appropriate disciplinary board.

4. The Internet

Internet is a vast, global network linking computers at universities, high schools, science labs, and many other sites. Using 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 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, 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:

1. No obscene or offensive material shall be entered into or sent through the AU Internet connection, web sites, whose access is prohibited by ETISALAT in UAE, are also prohibited in the Internet labs.
2. Users shall not deliberately attempt to degrade system performance or capability.
3. 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.
4. Reconfiguring the hardware arrangement by unplugging cables and moving hardware from one workstation to another is absolutely prohibited.
5. Online chatting, food, drinks, and smoking is forbidden in the computer lab.
6. Only one person at a time can use the lab computer, and No one has the right to reserve a PC for anyone.
7. 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.
8. Users have the right to complain about the Internet lab supervisor if you see any abuse of the above rules, complaints are to be submitted to the network manager, the help desk phone 06 - 7056500.

5. 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, an 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:

1) 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.
2) 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.
3) 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 web sites.
4) All users of the LMS must not 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.
5) 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.
6) Faculty and staff hosting a course on Moodle shall comply with all the UAE laws and all institutional rules, policies, and procedures in force.
7) 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 administrator whose duty is to monitor the content continuously.

User Management and Access to LMS

1. All users of LMS must access the system through a designated account which is provided by by the AU IT Office, and is the same as the user's University User Account (network username and password).
2. 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.
3. Official student enrollments will be managed from SIS including adding new students, student withdrawals, and drops.

4. For purposes of program curriculum management and continuous quality control, 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.
5. 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.
6. 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.

6. IT Security, Compliance and Governance:

6.1. 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.

6.2. 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 in regular bases.
- Limited the Admin privilege to the Technical team who are responsible of installing software and applications.

6.3. Password Policy

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

Applied Settings for Network Password Policy:

- Minimum Password Length is 8 characters

Applied Password Policy on Desktop in Computer Labs:

Enable Password Screen saver option after 10 minutes of 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 login with his/her network account.

Account lockout policy:

Account lockout policy disables a user's account if an incorrect password is entered for 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: 60 minutes
- Account Lockout Threshold: 50 invalid logon attempts
- Reset account lockout counter after: 30 Minutes.

6.4. 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:

1. 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.
2. It is prohibited to connect any personal computer, server, printer, firewall, network router, network switch, or other electronic device to the AU data network without the express approval of the IT & Networks Director.
3. When any use of information technology at the University presents an imminent threat to other users or to the University's technology infrastructure, network & systems administrators may take whatever steps are necessary to isolate the threat, without notice if need be.
4. The Office of IT does everything in its power to prevent viruses from entering the AU network. Measures taken include virus scanners on the 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.
5. Any attack or bid to attack the AU systems or networks will result in prosecution of the attacker according to the federal laws of the UAE.
6. Access to IDF rooms and server rooms is limited to IT staff only.
7. Intentional denial of computing service to other users.
8. Exploitation of insecure accounts or resources.
9. Attempting to guess, crack or otherwise determine another user's password.
10. Interception of network transmissions with hardware or software "sniffers".
11. Forging of electronic mail or electronic news or otherwise misrepresent themselves or other individuals in any electronic communication.
12. 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.
13. IT staff may not transfer resources (hardware, software, documentation, etc.) from designated locations without the explicit permission of their supervisor.

14. 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.
15. 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.
16. IT management reserves the right to audit University owned workstations and servers without warning for verifying software-licensing compliance.
17. AU employees or students may not load or install any software that may abuse the bandwidth of AU Network/Internet.
18. All computer and network access is 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.
19. 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.
20. The password, used with the account, is the equivalent of an electronic signature for the user. The use of User Account and password authenticates the identity and gives an on-line affirmation the force of a legal document. The user should guard the password and account as he/she would his/her check book 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 persons account, whether the attempt is successful or not.
21. 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.
22. 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.
23. 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.

24. 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.
25. 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.
26. 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.
27. 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 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 Policy

The Office of IT is responsible of 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:

1. 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.
2. University computer systems shall not be used for commercial purposes without written authorization of the university's management.

3. 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.
4. Students should notify the supervisor if the PC is slow or not working properly; consequently supervisor to notify help desk if he/she is unable to resolve the issue.
5. Users cannot install any programs from the Internet.
6. The lab supervisor is the person in charge of enforcing the Internet lab policy.
7. All users must log off when their time is over and/or they have to leave the lab.
8. All PCs are managed by IT, including the security settings and Virus Protection policy.
9. Any software need to be installed on computer labs should be reported to Office of IT. The installation shall be processed as the per the request process of the Helpdesk and Support services.
10. Anyone who does not abide by the rules above will be referred to the student's affairs.