

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Policies Manual		Policy Number	IT-01
			Effective Date	12-Aug-2018
	Subject Acceptable Use of Information Technology Resources		Most Recent Review Date	15-Apr-2018
			Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer		Page Number	1 of 1

1. Acceptable Use of Information Technology Resources

Overview

Defines acceptable use of information technology resources, rights and responsibilities of different parties involved in the use of such resources.

Scope

Applies to all users within the United Arab Emirates University.

Objective

This policy ensures that:

1. The integrity of data and systems at UAEU is safeguarded.
2. The use of electronic communications complies with UAEU Policies.
3. The UAEU meets its legal obligations for controlling data access.
4. The use of cloud computing services complies with UAEU cloud computing policy.

Policy

1. Computers and other information technology resources are essential tools in accomplishing the University's mission. Information technology resources are valuable community assets to be used and managed responsibly to ensure their integrity, confidentiality, and availability for appropriate research, education, outreach and administrative objectives of the University. University community members are granted access to these resources in support of accomplishing the University's mission.
2. These resources are valuable community assets to be used and managed responsibly to ensure their integrity, security, and availability for appropriate educational and business activities. All authorized users of these resources are required to use them in an effective, efficient, and responsible manner.
3. Users should be aware of the UAEU's user rights and responsibilities. This document outlines liability for personal communication, privacy and security issues, and sets out the consequences of violations.
4. Users should be aware of the public cloud services user rights and responsibilities. This document outlines liability for personal communication, privacy and security issues when using public cloud services.
5. Users of information technology resources are responsible for the content of their personal communications and may be subject to liability resulting from that use. The University accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Procedures Manual	Related Policy	IT-01
		Effective Date	12-Aug-2018
	Subject	Most Recent Review Date	15-Apr-2018
	Acceptable Use of Information Technology Resources	Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer	Page Number	1 of 6

Procedures of Policy No. (1) - Acceptable Use of Information Technology Resources

1. Definitions

a) Acceptable Use

- (1) Information/data and systems may only be used by authorized individuals to accomplish tasks related to their studies, job responsibilities, or other authorized activities as members of the University community. Use of the information and systems for personal gain, personal business, or to commit fraud is prohibited.
- (2) UAEU Information and Data must not be disclosed without authorization. Unauthorized access, manipulation, disclosure, or secondary release of such information constitutes a security breach, and may be grounds for disciplinary action up to and including termination, and lead to legal prosecution by government authorities.
- (3) Users should be aware of the UAEU's user rights and responsibilities. This document outlines liability for personal communication, privacy and security issues, and sets out the consequences of violations.
- (4) Internet should be used only for business purposes.
- (5) It is prohibited to enter banned sites or that contain Blocked content under the policy of the UAEU.
- (6) Users are prohibited from entering to abusive sites or contributing to it or download its files. These abusive sites include, but not limited to sites that promote racism, sites that contain religious feelings derogatory or offensive language or libelous or assaulted or abused for any individual or group and sites with pornographic content.
- (7) Internet users should not participate in any activity that would lead to suspension of computer systems operations.
- (8) Users should not upload, download or install software from the Internet, without prior approval of the DoIT.
- (9) Users should not install / use any VPN or proxy software which bypasses the university's network security policy.

b) Authorized User

An authorized user is the individual or entity permitted to make use of UAEU computer or network resources. Authorized users include students, staff members, faculty members, alumni, guest, sponsored affiliates, and other individuals who have an association with UAEU that grants them access to UAEU information technology resources. Some users may be granted additional authorization to access institutional data as authorized by the data owner or custodian.

c) Data Custodian

Data custodians are representatives of UAEU with assigned responsibilities delegated by the respective department directors to serve as a steward of UAEU data in a particular area. They are responsible for decisions in creating, maintaining, and using UAEU data, according to UAEU Policies and Procedures.

 UAEU	Information Technology Procedures Manual	Related Policy	IT-01
		Effective Date	12-Aug-2018
	Subject	Most Recent Review Date	15-Apr-2018
	Acceptable Use of Information Technology Resources	Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer	Page Number	2 of 6

d) Information Technology Resources

Resources include facilities, technologies and information resources that are used for UAEU information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communication devices and services, such as modems, wireless access points, e-mail, networks, telephones, voice mail, fax transmissions, video, multimedia, instructional materials. This definition is not all-inclusive but rather reflects examples of UAEU equipment, supplies and services.

e) Security Incident

An intentional or accidental occurrence affecting information or related technology in which there is a loss of data confidentiality or integrity, or a disruption and/or denial of availability.

f) Security Measures

Processes, software, and hardware used by system and network administrators to ensure the confidentiality, integrity, and availability of the information technology resources and data owned by UAEU and its authorized users. Security measures may include reviewing files for potential or actual policy violations and investigating security-related issues.

g) Public cloud computing

Public cloud computing such as but not limited to (google Drive, Dropbox ...etc.) also called software as a service, is defined as the use of third party remote servers and software that allows centralized data storage and online access to computer services or resources, or information technology hosting of any type that is not controlled by, or associated with, the University. These rules and required procedures apply to all United Arab Emirates University employees.

2. Responsibilities

a) User's Rights and Responsibilities

(1) Members of UAEU community are granted access to information technology resources in order to facilitate their UAEU-related academic, research, and job activities. However, by using these resources, users agree to abide by all relevant UAEU Policies and Procedures. These include but are not limited to UAEU Policies and Procedures related to harassment, plagiarism, commercial use, security, and unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws.

(2) When visitors are granted access to information technology resources, they must abide by the same UAEU Policies that are granted to regular users.

b) Users are responsible for:

(1) Reviewing, understanding, and complying with all Policies, Procedures and Laws related to access, acceptable use, and security of UAEU information technology resources.

 UAEU	Information Technology Procedures Manual	Related Policy	IT-01
		Effective Date	12-Aug-2018
	Subject	Most Recent Review Date	15-Apr-2018
	Acceptable Use of Information Technology Resources	Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer	Page Number	3 of 6

- (2) Asking system administrators or data custodians for clarification on acceptable access, use or other issues not specifically addressed in UAEU Policies, Rules, Standards, Guidelines, and Procedures.
- (3) Reporting policy violations to the appropriate entities or management authority.

c) Liability for Personal Communications

Users of UAEU information technology resources are responsible for the content of their personal communications. UAEU accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

d) Privacy and Security Awareness

Users should be aware that although UAEU takes reasonable security measures to protect the security of its computing resources and accounts assigned to individuals, UAEU does not guarantee absolute security and privacy. Users should follow the appropriate security procedures.

e) Public cloud computing

Use of Public cloud computing resources must comply with all other University policies and procedures. It is the responsibility of the employee using such services to ensure that the use is consistent with those policies. In addition to other University rules and policies, the following are required procedures, which must be followed in the use of cloud computing services:

a. Privacy and data security

Cloud computing may not be used for information that is classified, per the University's data classification policy, as restricted/confidential, private, personal, or sensitive.

b. Other Requirements

UAEU faculty, staff, and students must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage institutional data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. Virtually all cloud services require individual users to accept click-through agreements. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice. Risks with using self-provisioned cloud services include:

- (1) Unclear, and potentially poor access control or general security provisions
- (2) Sudden loss of service without notification
- (3) Sudden loss of data without notification
- (4) Data stored, processed, or shared on cloud service is often mined for resale to third parties that may compromise people's privacy
- (5) The exclusive intellectual rights to the data stored, processed, or shared on cloud service may become compromised.

 UAEU	Information Technology Procedures Manual	Related Policy	IT-01
		Effective Date	12-Aug-2018
	Subject Acceptable Use of Information Technology Resources	Most Recent Review Date	15-Apr-2018
		Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer	Page Number	4 of 6

f) Consequences of Violations

Access privileges to UAEU's information technology resources will not be denied without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its computers and networks or to protect itself from liability, UAEU may temporarily deny access to those resources. Alleged policy violations will be referred to appropriate UAEU authority. Depending on the nature and severity of the offense, policy violations may result in loss of access privileges, UAEU disciplinary action, and/or criminal prosecution.

g) UAEU's Rights and Responsibilities

- (1) As owner of the computers and networks that comprise UAEU's technical infrastructure, UAEU owns all official administrative and academic data that resides on its systems and networks, and is responsible for taking necessary measures to ensure the security of its systems, data, and user accounts. When UAEU becomes aware of violations, either through routine system administration activities or from a complaint, it is the responsibility of UAEU to investigate as needed or directed, and to take necessary actions to protect its resources and/or to provide information relevant to an investigation.
- (2) Individual units within UAEU may define additional conditions of use for resources or facilities under their control. Such additional conditions must be consistent with UAEU overall Policies but may provide additional details, guidelines, and/or restrictions.
- (3) Roles and responsibilities for specific UAEU entities and individuals are defined in greater detail below:
 - a) Chief Information Officer (CIO)
 - (1) Establishes, disseminates and enforces rules regarding access to and acceptable use of information technology resources.
 - (2) Establishes reasonable security policies and measures to protect data and systems.
 - (3) Monitors and manages system resource usage.
 - (4) Investigates alleged violations of UAEU information technology Policies.
 - (5) Refers violations to appropriate UAEU offices for resolution or disciplinary action.
 - b) Colleges and Departments
 - (1) Create, disseminate and enforce conditions of use that are consistent with UAEU-wide Policies for UAEU facilities and/or resources under their control.
 - (2) Monitor the use of UAEU resources under their control.
 - (3) Refer violations to appropriate UAEU offices for resolution or disciplinary action. Policy violations should be reported to the CIO.
 - c) Data Custodians
 - (1) Grant authorized users appropriate access to the data and applications for which they are stewards, working with UAEU Information Technology Sector (DoIT) personnel to limit access to authorized users with a legitimate role-based need.
 - (2) Review access rights of authorized users on a regular basis.
 - (3) Respond to questions from users relating to appropriate use of data.

 جامعة الإمارات العربية المتحدة United Arab Emirates University 	Information Technology Procedures Manual	Related Policy	IT-01
		Effective Date	12-Aug-2018
	Subject	Most Recent Review Date	15-Apr-2018
	Acceptable Use of Information Technology Resources	Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer	Page Number	5 of 6

- (4) Determine the criticality and sensitivity of the data and/or applications for which they are stewards.
- d) System/Network Administrators
 - (1) Take reasonable actions to ensure the authorized use and security of data and networks.
 - (2) Participate and advise as requested in developing conditions of use or authorized use procedures.
 - (3) Cooperate with appropriate UAEU departments and law enforcement officials in investigating alleged violations of policy or law including the right to access UAEU electronic resources upon appropriate approval.
- e) Information Security Officers

Protect UAEU network, systems, and data. Coordinate with a designated collegiate or a unit technical and security staff to ensure the confidentiality, integrity, and availability of UAEU systems and ensure that appropriate and timely action is taken.

3. Rights, Responsibilities and Authorization of Access

a) Misuse

- (1) A member of UAEU community who suspects a violation of UAEU's or any Department's acceptable use of information technology resources must notify their immediate supervisor.
- (2) The Supervisor is responsible for notifying DOIT Helpdesk or local IT personnel in order to isolate the equipment and create an incident report for documenting any alleged misuse.
- (3) The Supervisor will also notify the incident to the applicable department head to discuss appropriate action.

b) Access Information Technology Resources

- (1) IT resources and related services will be assigned and made available to employees and students. UAEU Human Resources Management and Registration Management offices determine who is a member of the student body, faculty or staff. The head of the employee's or the student's unit will determine rights of access for visiting faculty, hourly staff, and long-term consultants.
- (2) Owners and operators of any computer, servers, IT devices and services within the UAEU network may not grant access to accounts on their IT resources and services to anyone except with proper approvals.
- (3) Installation of unlicensed, non-standard encryption and software is prohibited.
- (4) Network scanning software, software copying, and distribution or intercept information or seizure passwords without a specific permission is prohibited.
- (5) License terms of any software must always be taken into consideration.
- (6) Software is used in accordance with federal or local laws in the country, including in particular copyrights laws and commercial transactions and patents.

 UAEU	Information Technology Procedures Manual	Related Policy	IT-01
		Effective Date	12-Aug-2018
	Subject	Most Recent Review Date	15-Apr-2018
	Acceptable Use of Information Technology Resources	Due Date for Next Review	01-Sep-2021
	Responsible Office: Chief Information Officer	Page Number	6 of 6

c) Special Circumstances

- (1) Departmental access to shared network resources is authorized by the Head of Unit that owns the network resources.
- (2) Requests to access cross-UAEU resources must be authorized by the Head of the Unit that owns the network resources and the CIO.

d) Authority to Access User Data

- (1) Email confidentiality and security are of prime importance. Requests to access any staff, student and faculty mailbox must have written authorization by the Office of the Vice Chancellor.
- (2) Access to a Department's generic mailbox and mailing list must be authorized by the head of the unit or his/her immediate supervisor.
- (3) Requests to access data logs concerning use of information and telecommunications technology must be approved by the CIO.
- (4) Requests to access data within a desktop must be authorized in writing by the head of the applicable unit, the Dean of the applicable College, and the CIO.

e) Loss of Data

Users are responsible for backing up their own files. They should not assume that files on their machines are backed up. Users must maintain and archive backup copies of important work. Deleted email messages / cloud storage data (UAEU provided) that are older than 30 days are not recoverable; recovery of deleted emails/ data is a self-service.

f) Usage and Responsibilities

- (1) User is responsible to protect the desktop / laptop and the information stored on it from damage, lost and steal.
- (2) In the case of theft of a laptop / mobile device, the user must inform the local Police immediately, and inform the DoIT department.
- (3) In case of damage or loss of a laptop / mobile device, the user must immediately inform the DoIT about the loss.
- (4) User should not leave the laptop / mobile device in public without monitoring.
- (5) User have to password protect the lock screen when finishing use of laptop / desktop / mobile devices.
- (6) User should not connect the private personal computers on UAEU network.
- (7) User should not change the administrative functions in the portable computer in any way, such as the operating system in the device or the definition of a system administrator and password.
- (8) User should complete the backup of their data linked with university provided login ID before the last working / graduation day at the university.