جامعـــة الشـــــارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Acceptable Usage	Last Review date	19/5/2021
	Policy Number	IT-01	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

This policy is set to define the acceptable usage of information assets and processing facilities which may include internet, intranet, e-mails, systems, storage media, operating systems, and application software and business information of the University of Sharjah.

Scope

This policy details specific requirements for the use of all computing and network resources at the University of Sharjah. Information resources and technology at the University of Sharjah support the educational, instructional, research, and administrative activities of the University, and the use of these resources is a privilege that is extended to members of the University of Sharjah community. As a user of these services and facilities, you have access to valuable University resources, legally restricted and/or confidential information, and internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legally compliant manner.

In general, acceptable use means ensuring that the information resources and technology of the University are used for their intended purposes while respecting the rights of other computer users, the integrity of the physical facilities, and all pertinent license and contractual agreements. If an individual is found to violate the Acceptable Usage Policy, the University may take disciplinary action, including restriction of and possible loss of network privileges or more serious consequences, up to and including suspension, termination, or expulsion from the University. Individuals may also be subject to federal, state, and local laws governing many interactions that occur on the University's networks and the Internet. These policies and laws are subject to change as state and federal laws evolve.

Purpose

This policy applies to all users of computing resources owned or managed by the University of Sharjah. Individuals covered by the policy include (but are not limited to) University faculty and visiting faculty, staff, students, alumni, contractors, volunteers, guests or agents of the administration, and external individuals and organizations accessing network services via the University's computing facilities.

Processing facilities include all University-owned, licensed, or managed hardware and software, University assigned user accounts, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology whether administered in individual departments and divisions or by central administrative departments. They apply to personally owned computers and devices connected by wire or wireless to the University network, and to off-site computers that connect remotely to the University's network services.

Policy

Acceptable use

1. **Employees** have a responsibility to, promptly, report the theft, loss, or unauthorized disclosure of the University of Sharjah's information.
2. Employees are responsible for the reasonableness of personal use of University of Sharjah information systems.
3. Under no circumstances is an employee of the University of Sharjah authorized to engage in any activity that is illegal under local, federal or international law while utilizing the University of Sharjah owned resources.
4. When using company resources to access and use the Internet, users must realize they represent the University of Sharjah. Whenever Employees state an affiliation to the University of Sharjah, they must also clearly indicate that "the opinions expressed are their own and not necessarily those of the UoS.
5. University of Sharjah's information is considered confidential. As such, Employees will refrain from revealing any University of Sharjah information, Academic transcripts, documents with publishing right, research patents, Health records, trade secrets, or any other material related to the University of Sharjah when engaged in blogging, exchanging information, or posting information on public forums or social media.(Ref. UoS information exchange policy).
6. Employees shall withhold from making any negative public comments or statements to the media or on any social media networks or to others bodies on issues pertaining to the University of Sharjah or its policies or programs that might cause harm to the University of Sharjah's image and reputation or the Authority as a whole.
7. Faculty, Employees, Students or third party involved in sharing views with external users on websites shall be aware of this policy and should exercise extreme caution prior to publishing information related to UoS and inconsideration to the below.
    a. Violate the legal and privacy rights.
    b. Transmit, upload or download any material that potentially contains viruses, Trojan horses, worms, time bombs, or any other malicious code.
    c. Post messages that is in-appropriate and/or has the potential to cause any harm to UoS.
8. Users are expected to back up their data and information regularly. Users are advised to store data in approved IT storage media which are backed up by IT. Data stored in hard

disks are not backed up and risk is owned by the user. Ref backup and storage policy for details

9. Abide by the Uos Information Security Policy. Users shall not share any classified information outside the organization. Refer Data classification policy.
10. Users shall secure the computer screens of their systems when away from their desks. Ref Clear desk policy for details.

Unacceptable Use

System and Network Activities: The following activities are strictly prohibited, with no exceptions:

1. The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University of Sharjah.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the University of Sharjah or the end-user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting University of Sharjah business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software, or technology, in violation of international or UAE laws, is illegal.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
7. Using a University of Sharjah computing asset to, actively, engage in procuring or transmitting material that is in violation of laws in UAE.
8. Making fraudulent offers of products, items, or services originating from any University of Sharjah account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Conducting information security breaches or disruptions of network communication. Technical scanning of assets is prohibited.
11. Executing any form of network monitoring that will intercept data not intended for the Employee's host.

12. Circumventing user authentication or information security of any host, network, or account.
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet, such as denial of service attack.
14. Providing information about, or lists of, University of Sharjah's Employees to the parties outside the University of Sharjah.

Internet Usage

1. Users shall ensure that the internet facility is used strictly for official purposes.
2. Users shall ensure that they make use of the internet facility for carrying out their job responsibilities, and not try to establish unauthorized means of accessing the internet such as communication devices, unauthorized wireless access points, etc.
3. Users shall ensure that they do not access the corporate internet facility with the credentials of another user.
4. Users shall ensure that they do not allow another user to access the corporate internet facility with his/her credential.
5. Users shall not use the internet to download and distribute malicious software in the University of Sharjah's corporate network.
6. Users shall not share classified information with external websites unless otherwise authorized by the management Users shall not use corporate internet facilities to access any illegal or unethical websites propagating information on gambling, obscene material, violence, weapons, drugs, racism, hate, and other similar explicit contents.
7. Users shall be held responsible for any misuse of Internet access originating from their account.

Email and Communication Activities: The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Conducting any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within University of Sharjah's networks of other Internet / Intranet / Extranet service providers on behalf of, or to advertise, any service hosted by the University of Sharjah or connected via University of Sharjah's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Violations and Breaches

1. Any violation of the terms and requirements of this policy should be reported immediately to the "Information Security Team"
2. Compliance with existing policies, laws, or any other legislation pertaining to Information Security is expected to be concurrent with this policy.
3. Any breach of the terms of this policy will render the employee non-compliant and will be held responsible for the outcome of his / her action.
4. Employees will be subject to disciplinary action as per the Violations and Penalties Policy of the University of Sharjah to the extent of involving legal proceedings and allegations as per United Arab Emirates laws and according to the severity of the breach.

Reference

Standard	Control
ISO 27001:2013	A.8.1.3