


Category	IT Infrastructure and Services	Policy Number	SUP-ITS-104	 جامعة زايد ZAYED UNIVERSITY
Distribution	External	Version	1.1	
Responsible Office	CAFO	Policy owner	IT Department	
Date Approved	27 April 2021	Effective Date	27 April 2021	
Date Last Reviewed	27 April 2021	Due Date for Next Review	27 April 2024	

POLICY

Acceptable Usage

1. Purpose

The purpose of this policy is to outline the acceptable use of computer and communication equipment at Zayed University and to provide directives and guidelines towards usage of assets, services and systems.

2. Scope of Application

The scope of this policy covers all the Information Systems environments managed by the ZU IT Department (ITD). This policy applies to all ZU employees, contractors, consultants, students, and temporary employees.

3. Policy

3.1 General Use and Ownership

- 3.1.1 ZU IT network administration shall provide a reasonable level of privacy over information/data created and transmitted over ZU IT systems and infrastructure. However, the data created on ZU systems remains the property of ZU.
- 3.1.2 The information contained on the ZU Intranet/Extranet is classified as per the ZU Information Classification Guidelines.
- 3.1.3 Under no circumstances is a ZU user authorized to engage in any activity that is illegal under local or international law while utilizing ZU-owned IT resources.
- 3.1.4 Users of ZU's information systems shall ensure that classified information is managed as per the ZU Information Classification Guidelines. Examples of classified information include but are not limited to: corporate strategies, customer details, student records, investigation reports and analysis data.
- 3.1.5 Employees shall take all necessary steps to prevent unauthorized access to information/data that they access, use, and/or manage.
- 3.1.6 ZU information system resources provided to employees are to assist them in carrying out their duties relevant to their institutional responsibilities. It is prohibited to use ZU information system resources for any business purposes other than those related to the university.

3.2 General Security Requirements

- 3.2.1 All software used on a ZU system shall be validly licensed. ZU ITD shall have a valid license for all software installed on ZU systems by ITD personnel. Users will be accountable for ensuring any software they have installed on a ZU laptop/tablet/desktop or other similar device is legally licensed. The possession of valid licenses shall be audited regularly.
- 3.2.2 All systems used by ZU employees that are connected to the ZU network, shall continually execute ITD-approved virus-scanning software with current virus signatures unless overridden by departmental or group policy.
- 3.2.3 Sensitive and/or confidential data/information shall not be stored on ZU desktops or laptops unless encrypted.

3.3 Details of the activities that fall into the category of acceptable usage are included in the accompanying procedures, guidelines and manuals.

3.4 Any employee found to have violated this policy shall be subject to disciplinary action.

4. Related Policies and Laws

- SUP-ITS-203 Information Security
- Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities
- ZU Information Classification Guidelines

5. Administration

This policy is administered by the Information Technology Department.

6. Revision History

Date	Revision
11 February 2023	Administrative change: <ul style="list-style-type: none">• Updated the information header and policy numbers to be in line with the new format.• Updated the policy number from SUP-ITS-01 to SUP-ITS-104.
27 April 2021	Non-substantive changes approved by the Vice-President as Acting CAFO.
20 April 2021	Reviewed policy with no changes required
6 January 2020	Updated the policy number to SUP-ITS-01 from SUP-ITS-11.
12 March 2018	New policy approved by the University Council.