


<b>Policy Group</b>	IT Services	<b>Policy Number</b>	SUP-ITS-07	 جامعة زايد ZAYED UNIVERSITY
<b>Responsible Office</b>	Office of the CAFO	<b>Distribution</b>	External	
<b>Date Approved</b>	4 October 2020	<b>Effective Date</b>	4 October 2020	
<b>Date Last Reviewed</b>	30 September 2020	<b>Due Date for Next Review</b>	30 September 2023	

## **POLICY**

### **Email Security**

#### **1. Purpose**

The objective of this policy is to minimize the risks associated with usage of the Zayed University email system, and to define controls against the threat of unauthorized access, usage, or theft of information, and the malicious disruption of services.

#### **2. Application**

This policy applies to all ZU employees, students, contracted personnel and any third-party representatives who have been provided access to the information assets of the university.

#### **3. Policy**

##### **3.1 Email Security**

- a) Access to ZU email shall be duly authorized by Human Resources Department and provisioned by the IT Department (ITD).
- b) All emails must be identified with a user's name or email ID to allow for individual tracking.
- c) All ZU email users are responsible for the contents of their email.
- d) All ZU email users must use the ZU email system for official correspondence, and it is strictly prohibited for users to use third-party email domains for the same.
- e) It is strictly prohibited to synchronize ZU emails to any external non-ZU email services.
- f) An antispam server will scan all incoming and outgoing emails, attachments, and URL for spam and malware. Spam and virus infected emails will be automatically deleted without notice. Suspected emails will be quarantined for one month.
- g) Users shall not be allowed to send or redirect, transfer, distribute or reply to emails which contain statements or include abusive comments concerning race, sex, color, disability, age, pornographic images or other comments, contents or materials related to religious or political beliefs and practices except for the purposes of reporting such emails.
- h) Users must not open attachments from any unknown source without scanning them for viruses or malware first. In case of doubt, or if an unsafe attachment has been received multiple times, the user must report the incident to the ZU Service Desk as a possible virus/malware threat.
- i) It is prohibited to use official email for personal purposes.

- j) It is prohibited for users to participate, or share, in dispatching emails for personal, commercial, religious, or political reasons.
- k) Users are not allowed to share or participate in distributing emails for charitable causes without prior permission from the Office of the Vice-President or federal authorities like the Telecommunications Regulatory Authority (TRA).
- l) It is prohibited for an email-system user to impersonate any other person.
- m) The ITD has attempted to block all commercial marketing emails. Any exclusions to allow marketing email shall be duly authorized by the IT Director with proper justification.
- n) The default mailbox size for each user shall be restricted according to the Grade level.

### **3.2 Confidentiality and Disclaimer**

- a) ZU users must treat email messages and files as confidential information. Email must be handled as a confidential and direct communication between a sender and a recipient.
- b) All email messages sent by employees are the records of ZU. If there is due cause, the Vice-President or federal authorities reserve the right to examine employee emails. Email messages will be monitored for any of the following reasons:
  - i) To ensure internal organization policy, legal, and regulatory compliance;
  - ii) To support internal investigations for suspected criminal activity;
  - iii) To assist with the management of the ZU information system.
- c) ITD will ensure the backup of email messages in accordance with TRA regulations.
- d) Users must not send confidential or sensitive information via email, unless the information is encrypted using an ITD-approved encryption technique.
- e) All email messages issued electronically by ZU users must be footnoted with a disclaimer paragraph.

### **3.3 Naming Convention and Signature**

- a) ZU shall follow a standard naming convention for official email ID's.
- b) Users shall not use any non-standard or unapproved email signatures.

### **3.4 Email Settings**

ZU employees, contractors, or third-party vendors using ZU facilities shall not modify the security parameters within the email system. Users making or requesting unauthorized changes to the email security parameters are in violation of this policy.

### **3.5 Mail Relay**

Mail relay is only permitted for application hosted internally or on the cloud authorized by ZU ITD.

### **3.6 Email Retention**

All emails in employees' mailboxes will be archived with a fixed retention period.

- 3.7 Zayed University will not store emails from personal email systems in the Email Archiving System.

## **4. Related Policies and Laws**

SUP-ITS-03 Access Control

SUP-ITS-04 Information Security

Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities

**5. Administration**

This policy is administered by the Information Technology Department.

**6. Revision History**

<b>Date</b>	<b>Revision</b>
4 October 2020	President's Decree issued (PD #90 of 2020).
30 September 2020	Approved by the University Council.
31 May 2020	Non-substantive change: Added External Distribution.
10 October 2019	Reviewed by VP, CAFO, Legal Advisor and Internal Audit with no changes.
7 May 2019	Reviewed by CAFO Management Council and endorsed for further approval. Revisions as per requirement from Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities: Added Email Retention Policy section.
12 March 2018	Approved by the University Council New policy.