


Category	IT Infrastructure and Services	Policy Number	SUP-ITS-103	 جامعة زايد ZAYED UNIVERSITY
Classification	Public	Version	1.3	
Responsible Office	CAFO	Policy Owner	ITD Director	
Date Approved	22 April 2025	Effective Date	22 April 2025	
Date Last Reviewed	19 November 2024	Due Date for Next Review	22 April 2028	

PROCEDURES

Bring Your Own Device

1. User Security

- 1.1 Due to their portability, personally owned devices (“**POD**”) such as laptops, cell phones and smartphones are particularly susceptible to theft or loss. Users must use reasonable care to protect cell phones and smartphones and avoid accessing or storing confidential data (as defined in the Information Security Policy) on such devices. Users who access Zayed University (“**University**” or “**ZU**”) services using cell phones or smartphones must secure such devices.
- 1.2 To prevent unauthorized access, PODs must be password protected using the features of the device and a strong password is required to access the University network. Phones without a secure PIN or Passcode will not be allowed to register in the ZU mobile device management system to receive the University’s services.
- 1.3 Rooted or Jail Broken devices (devices which have been modified to bypass manufacturer and/or operator restrictions) are strictly forbidden from accessing the network and will not be allowed to register in ZU’s mobile device management system.
- 1.4 A user’s access to ZU IT services is limited based on the user profiles defined by the IT Department (“**ITD**”) and is automatically enforced.
- 1.5 The user’s device may be blocked from accessing ZU services if:
 - a) the device is lost,
 - b) the user’s active association is formally completed in ZU as part of the academic process,
 - c) ITD detects a data or policy breach, a virus or similar threat to the security of the University’s data and technology infrastructure.

2. Device Support

- 2.1 Supported smartphone models include iPhone, Android smartphones, and Windows smartphones.

- 2.2** The native email client can be used in all iPhones, Android phones, and Windows phones.
- 2.3** Supported tablet models include iPad and Android tablets.
- 2.4** Supported laptop models include Windows and Mac devices only.
- 2.5** Connectivity issues are supported by ITD, and users should contact the IT Service Desk in case of any issues in accessing ZU services through defined channels.

3. Risks/Liabilities/Disclaimers

- 3.1** ITD reserves the right to disconnect devices or disable services without notification.
- 3.2** Lost or stolen devices must be immediately reported to ITD to take necessary steps.
- 3.3** The activities of personnel with respect to these procedures are subject to regular internal audits by line managers, the IT Service Desk, and/or the Internal Quality Auditors.

4. Revision History

Date	Revision	Ver.
22 April 2025	Approved by the CAFO.	1.3
19 November 2024	Reviewed with no substantive changes required.	
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-16 to SUP-ITS-103. 	
31 December 2020	Non-substantive changes approved by the CAFO.	1.2
4 October 2020	Non-substantive changes approved by the CAFO.	1.1
6 January 2020	Updated the policy number to SUP-ITS-16 from SUP-ITS-13.	
8 April 2018	New procedures approved by the Vice-President (VPD#65 of 2018).	1.0