


<b>Category</b>	IT Infrastructure and Services	<b>Policy Number</b>	SUP-ITS-103	 جامعة زايد ZAYED UNIVERSITY
<b>Distribution</b>	External	<b>Version</b>	2.0	
<b>Responsible Office</b>	CAFO	<b>Policy Owner</b>	IT Department	
<b>Date Approved</b>	17 June 2021	<b>Effective Date</b>	17 June 2021	
<b>Date Last Reviewed</b>	8 June 2021	<b>Due Date for Next Review</b>	8 June 2022	

## **POLICY**

### **Bring Your Own Device**

#### **1. Purpose**

This policy establishes the rules of use for personally owned devices (POD) to access and store Zayed University data for academic and administrative use.

#### **2. Scope of Application**

This policy applies to all ZU students and third-party users (external to ZU).

#### **3. Policy**

**3.1** This policy is intended to protect the security and integrity of ZU data and technology infrastructure.

**3.2** ZU students and third-party users must abide by the rules for the proper use of personally owned devices (POD) configured to use ZU's services (Internet, emails, internal portals, applications, etc.) to protect the confidentiality and integrity of sensitive data and applications and the availability of services at the university, protecting both POD and their users, as well as corporate assets, and the continuity of university business.

**3.3** ZU students and third-party users must agree to the terms and conditions set forth in this policy and associated procedures to connect their devices to the university network.

**3.4** Students are required to bring a working POD with a minimum hardware specification as specified by the respective college.

**3.5** POD users must have the latest Anti-Virus program running on their devices with updated signatures before connecting to the ZU network.

**3.6** POD users must ensure that the POD operating system is updated before connecting to the ZU network.

**3.7** POD users must ensure to separate their personal data from business data. Personal data is the sole responsibility of the users.

**3.8** In the event of service provisioning, ITD might require access to the device. The user is obliged to hand over the device along with the necessary passcode.

**3.9** Details specific to the device support of this policy are included in the accompanying procedures, guidelines and manuals.

- 3.10** Exceptions to this policy must be considered on a case-by-case basis and a written endorsement is required to be submitted for approval from either the CAFO or Provost.
- 3.11** ZU reserves the right to revoke this POD privilege if users do not abide by this policy and the rules of use. ZU will never access sensitive personal information from a user device or make it available to a third party.
- 3.12** This policy will be reviewed by the Information Technology Department (ITD) and approved by ITD Director on an annual basis.

**4. Related Policies and Laws**

SUP-ITS-203 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**

Date	Revision
11 February 2023	Administrative change: <ul style="list-style-type: none"> <li>• Updated the information header and policy numbers to be in line with the new format.</li> <li>• Updated the policy number from SUP-ITS-16 to SUP-ITS-103.</li> </ul>
17 June 2021	President’s Decision issued (PD#31 of 2021).
8 June 2021	Approved by the University Council.
25 May 2021	Reviewed by Academic Council and endorsed for further approval.
10 March 2021	Following Changes made under points 3.7 and 3.8 <ul style="list-style-type: none"> <li>• Personal data is sole responsibility of the users.</li> <li>• ZU will never access sensitive personal information from user device or make it available to the third party.</li> <li>• Added point 3.11</li> <li>• In the event of service provisioning, ITD might require access to the device, the users are obliged to hand over the device along with the necessary passcode.</li> </ul>
16 December 2020	Reviewed by the CAFO Management Council Substantive Changes: <ul style="list-style-type: none"> <li>• The policy now applies only to ZU Students and third-party users who are external to ZU. ZU employees have been removed from this policy as they are provided equipment from ZU.</li> <li>• Device categories were replaced with POD (personally owned devices) and guidelines for these are mentioned in points 3.5,3.6 &amp; 3.7</li> <li>• Reviews will be done by the ITD.</li> </ul> Non-substantive change: <ul style="list-style-type: none"> <li>• Added Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities in Related Policies and Laws section</li> </ul>
4 October 2020	Non-substantive change approved by CAFO.

6 January 2020	Updated the policy number to SUP-ITS-16 from SUP-ITS-13.
12 March 2018	New policy approved by the University Council.