Australian National University

Procedure: Bring your own device

Purpose

To define the obligations for users who choose to connect a personally owned device to the University's network or who use their personal device to access the University's information technology (IT) services, data and networks.

Definitions

Definitions of additional terms used in this document are provided in the overarching policy, *Acceptable use of information technology*.

Bring Your Own Device (BYOD): the use of any electronic device not owned or leased by the University, and which is capable of storing data and connecting to a network (e.g. wireless, 4G, physical connection), to access or connect to the University's IT services, data and networks. This includes but is not limited to mobile phones, smartphones, tablets, laptops, notebooks and portable storage devices.

Encryption: A cryptographic function used to ensure the confidentiality of data. The University considers an appropriate level of encryption to be the standards specified in the Australian Government Information Security Manual. See section "ASD Approved Cryptographic Algorithms".

Firmware: permanent software programmed into a read-only memory that provides control, monitoring and data manipulation within the device.

Operating system: the low-level software that supports a device's basic functions, such as scheduling tasks and controlling peripherals.

Security patch: a piece of software designed to update a computer program, or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bug fixes, and improving the usability or performance of a device.

Software: computer software is designed to assist end users to carry out useful tasks. Examples of software may include the Microsoft Office suite of products or smartphone applications such as Google Maps.

Threat: any potential cause of harm, technological, natural, or otherwise, to an information asset; including software bugs, unlocked rooms, or well-known passwords.

Procedure

1. Authorised users may bring their own device to access or connect to the University's IT services, data and networks, provided they meet the obligations of this procedure.

2. This procedure applies to all users and all devices that connect to the ANU network, other than ANU owned, leased or supported devices.

3. Devices which are specifically designed for network access, such as switches, WiFi access points and hubs may not be attached to the University's network infrastructure.

4. The University aims to make ANU systems and interfaces accessible across a wide range of devices and platforms however cannot guarantee that any particular combination of system and device will operate.

5. Access to any highly sensitive University data is vested in the relevant system owner. System owners may change or restrict access to data from devices that are not University owned at their discretion.

6. The University reserves the right to inspect and verify that University data has been removed from the device at the end of its use within the University environment or when a device is at end of life.

7. The University may perform a remote wipe of ANU data in order to prevent unauthorised access.

8. By choosing to BYOD, the user gives consent for the University to interrogate such devices to ensure appropriate use, as defined by the *Acceptable use of information technology policy* and the *Information technology security policy*.

9. The University is not responsible for any damage or loss that occurs to any personal device.

10. Limited support may be provided to assist users in accessing University systems and services.

User responsibilities

11. Users who choose to BYOD must:

    a. ensure that the operating system, firmware and installed software is obtained from an authorised source, is up to date and that required security patches have been applied to protect against known vulnerabilities;

    b. employ security solutions where available, including anti-virus, firewall and threat intelligence capabilities;

c. not perform system administration of any University enterprise system using a BYOD device, without prior approval from the system owner. System administration tasks are those performed by users with privileged or elevated access;

d. not store highly sensitive data on non-University owned devices, as stated in the *Infrastructure security classification standard*;

e. remove or transfer all University data from the device or associated storage when no longer required or when the device is decommissioned;

f. perform regular data backups of all University data;

g. immediately inform the ITS Cyber and Digital Security Team if any personal device carrying University data is lost or stolen by emailing it.security@anu.edu.au;

h. assume sole responsibility for operating system, the device and any personal applications running on the device;

i. ensure the software and services being used on the device for work related to the University are compliant with the conditions of use specified in the software license or within any license agreement between the University and the vendor;

j. ensure the device supports password or pin authentication and that this is enabled; and

k. ensure that the device has the automatic lock enabled.

Document information

Title	Bring your own device
Document Type	Procedure
Document Number	ANUP_016809
Version	7
Purpose	This procedure defines the obligations for all authorised users who choose to connect a personally owned device to the University's network or who use their personal device to access the University's Information Technology (IT) services, data and networks. This procedure aims to protect University systems and data from unauthorised access, use or disclosure.
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Technology
Subtopic	Usage
Effective Date	2 Apr 2019
Review Date	5 Apr 2024
Responsible Officer	Director, Information Technology Services
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Information Technology Services (cio@anu.edu.au)
Authority	1092601639 Information Infrastructure and Services Rule 2020 AS ISO/IEC 27002:2015 Australian National University Act 1991 Australian Government Protective Security Policy Framework Public Governance, Performance and Accountability Act 2013 Public Governance, Performance and Accountability Rule 2014 Australian Government Department of Finance and Deregulation Finance Circular No. 2009/08 Crimes Act 1914 (Cth) Privacy Act 1988 Telecommunications Act 1997 Telecommunications Regulations 2021

	1504249903
Printed On	5 Jun 2023