THE UNIVERSITY of ADELAIDE

# IT Acceptable Use and Security Policy



## Overview

The University of Adelaide seeks to provide the University community with secure and timely access to Information Technology (IT) equipment and the online services and resources necessary for undertaking their work and study. This Policy sets out the principles applicable to the use of University IT and expresses the commitment of the University to providing and maintaining secure, effective and reliable IT infrastructure and services to support the University's operations in research, teaching, learning, and administration. By observing the acceptable use and security requirements, University IT users and custodians can help to prevent service disruptions and data breaches caused by cyberattacks and other threats.

## Scope and Application

This Policy applies to all users of University IT. This Policy also applies to users connecting personally owned devices (BYOD) such as laptop computers, smartphones and tablets to the University network, and/or storing any University data on such devices.

## Policy Principles

### 1. Acceptable and Unacceptable Use of IT

a) University IT must be used in a lawful, ethical and responsible manner, and in accordance with the IT Acceptable Use Procedures, other applicable University policies, and any additional terms of use that may apply to particular software or services.

b) University IT is provided for use in the academic, administrative, commercial and community activities of the University. Some reasonable non-commercial personal use may be allowed, but as a privilege and not a right, and if that privilege is abused it will be treated as a breach of this Policy.

c) Account holders must take all reasonable steps to protect their account from unauthorised use and never share their passwords and other login credentials with others.

d) Users are expected to report actual or suspected breaches of this Policy or other security incidents that may be a threat to the security of University IT in a timely manner.

e) Users must undertake any cyber security training on topics including, but not limited to, obligations and expectations with respect to handling and protection of identity, devices, data and privacy, commensurate with job responsibilities as determined by the University and by their supervisor.

f) Only University authorised and certified IT should be used to conduct University business or store and process University data unless an exemption has been granted by ITDS.

g) Users must obtain approval from ITDS as well as comply with policies, standards and procedures defined in the Cyber Security Framework before:
    i. Developing or purchasing new software, including cloud services, that will store or process University data.
    ii. Connecting any new devices to the University campus network.
    iii. Engaging third parties who will access or process University data on behalf of the University.

**2. Accessing University IT**

a) The University is committed to providing users access to University IT in a timely fashion to enable learning, research and administrative activities.
b) Provisioning and de-provisioning of University of Adelaide User IDs and other access to University IT is governed by formal business rules administered by ITDS, Human Resources and DVCA.
c) The University may impose volume quotas (e.g. mailbox, printing, file storage, downloads) and security measures on the use of University IT.
d) Normal operation and maintenance of University IT includes logging of usage and activity on University IT. The University may monitor and analyse such logs where it is reasonable for the University to do so, and to meet the University's legal obligations.
e) University IT can be accessed from on-campus network access points or by using one of the authorised methods for remote access protected by multi-factor authentication. Other forms of personal remote access such as desktop remote access are prohibited.
f) The University reserves the right to suspend user accounts, disconnect devices from the network, or block internet traffic where there is an actual or perceived risk to the security of other users or University IT.

**3. Security of University IT**

a) The University will take all reasonable steps to protect the security of University IT, including its confidentiality, integrity, and availability.
b) The University will implement and operate the Cyber Security Framework, an information security governance framework in order to effectively manage the security risks of University IT.
c) All custodians of University IT, including ITDS, must comply with this policy, the IT Security Procedures, as well as the security standards and procedures as set out in the Cyber Security Framework.
d) The Chief Information Officer is responsible for the governance and oversight across all University IT, including Centralised, Distributed and Specialist IT, to ensure security controls are applied in a consistent manner in compliance with the IT Security Procedures and standards defined in the Cyber Security Framework.
e) IT Custodians are responsible for implementing and operating the required security controls as specified under the various standard defined in the Cyber Security Framework.
f) To implement an effective defence against multifarious threat actors including organised crime and nation-states, ITDS will develop and maintain a Cyber Security Strategy that prioritises initiatives aligned to the University strategic objectives, threat modelling, industry best-practices, and any regulatory or contractual compliance obligations.
g) Where there is a threat to University IT infrastructure or security, or if the use of University IT presents a risk to the University, the University may take any necessary action to mitigate the risks without prior notice.

**4. Breaches of this Policy**

a) Breaches of this Policy may result in suspension of access to University IT and/or;
    i. In the case of University employees, may constitute misconduct which will be addressed in accordance with the University's Enterprise Agreement or relevant University disciplinary procedures.
    ii. In the case of students, may constitute misconduct under the Student Misconduct Rules.
b) Breaches of this Policy may also be reported to external parties as required under law.
c) Any actual or suspected breach of this policy should be notified to the Chief Information Officer and the Chief Information Security Officer.

**Delegations of Authority**

| *Key* | *Authority Category* | *Authority* | *Delegation Holder* | *Limits* |
|---|---|---|---|---|
| University Operations | Information Technology | Authority to approve exceptions to this Policy | Chief Operating Officer (COO)Chief Information Officer (CIO) | |
| University Operations | Information Technology | Authority to grant visitor access to the University IT facilities and services | Area Managers<br>Heads of Schools<br>Branch Heads<br>or their delegates | |
| University Operations | Information Technology | Authority to authorise the creation of generic, casual, and external visitor accounts | Area Managers<br>Heads of Schools<br>Branch Heads<br>or their delegates | |
| University Operations | Information Technology | Authority to authorise a change to the level of access for staff, titleholder or visitor account | Area Managers<br>Heads of Schools<br>Branch Heads<br>or their delegates | |
| University Operations | Information Technology | Authority to request examination of an account holder's use of IT Facilities | Area Managers<br>Heads of Schools<br>Branch Heads | |
| University Operations | Information Technology | Authority to approve Peer to Peer software for lawful purposes | Area Managers<br>Heads of Schools<br>Branch Heads | |
| University Operations | Information Technology | Authority to order the immediate suspension or termination of a staff, title-holder or visitor account | VC & President, DVCs and VPs<br>Executive Director, Human Resources | If account holder is also a student, approval of Executive Director, Student Experience is also required |
| University Operations | Information Technology | Authority to order the immediate suspension or termination of a student account | DVCs and VPs<br><br>Executive Director, Student Experience | If account holder is also a staff member or title-holder, approval of Executive Director, Human Resources is also required |
| University Operations | Information Technology | Authority to immediately suspend or disconnect any account or IT Facility based on an immediate threat to the University. | Area Managers<br><br>CIO<br><br>Director, IT Operations & Digital Services, ITDS<br><br>Director, IT Strategy, Planning & Governance, ITDS<br><br>Chief Information Security Officer, ITDS | |
| University Operations | Information Technology | Authority to approve changes to the stand alone procedures related to this Policy. | Chief Operating Officer | |

| | |
|---|---|
| **RMO File Number** | 2021/8007 |
| **Policy Custodian** | Chief Operating Officer |
| **Responsible Officer** | Chief Information Officer |
| **Endorsed by (Academic Board or VCE)** | Vice-Chancellor's Executive on 6 April 2022 |
| **Approved by** | Vice-Chancellor and President on 10 May 2022 |
| **Related Procedures** | IT Acceptable Use Procedures<br>IT Security Procedures<br>Information Classification and Handling Guideline<br>Third Party Hosting Security Guideline |
| **Related Documents and Policies** | Behaviour and Conduct Policy<br>Code of Conduct Policy<br>Copyright Policy<br>Information Management Policy<br>Privacy Policy<br>Student Misconduct Rules |
| **Related Legislation** | Copyright Act 1968 (Cth)<br>Criminal Code Act 1995 (Cth)<br>Privacy Act 1998 (Cth)<br>Security of Critical Infrastructure Act 2018 (Cth)<br>Spam Act 2003 (Cth)<br>Telecommunications (Interception and Access) Act 1979 (Cth)<br>Tertiary Education Quality and Standards Agency Act 2011 (Cth) (TEQSA Act) ss 114A and 114B |
| **Superseded Policies** | IT Acceptable Use and Security Policy (2016) |
| **Effective** | 10 May 2022 |
| **Next Review Date** | 9 May 2025 |

**GLOSSARY:
**Account holder** means a person who has been provided with a password protected account to access University IT.

**Area Managers** means the Deputy Vice-Chancellors, Vice Presidents, Pro Vice-Chancellors, Executive Deans, Director Human Resources (and a person acting in these positions) and Institute Directors as defined in the University of Adelaide Enterprise Agreement.

**Business Owner** means the person or a party that is ultimately accountable for the security of data and/or services provided by a University IT.

**BYOD (bring-your-own device)** means computing devices, including personal computers, smartphones, tablets and storage devices owned and managed by an individual which are used to connect to the University network, and/or to store any University data.

**Centralised IT** refers to all IT assets and services that the central ITDS branch owns and manages on behalf of the broader University.
**Distributed IT** refers to any IT assets and services that are currently owned and managed outside of the central ITDS branch. "Distributed IT" consists of a combination of "Specialist IT", as well as remaining local IT assets and services that are candidates for future centralisation within the ITDS branch.

**IT Custodian** means any person that is responsible for the acquisition, implementation, and/or ongoing operations and maintenance of University IT under the direction of the respective Business Owner. They are also accountable for ensuring the security of University IT by complying with the ITAUSP and the CSF. The CIO is the custodian of Centralised IT.

**Information Technology (IT)** is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services.

**ITDS** means the Information Technology and Digital Services branch of the Division of University Operations

**Specialist IT** refers to particular IT assets and services that require specific local discipline knowledge and expertise in order to directly support learning, teaching or research activity. Responsibility for owning and managing "Specialist IT" rests with the applicable local University areas, with the central ITDS branch responsible for the provision of "Specialist IT" Level 1 Service Desk support, Service Management support and Cyber Security and Solution Architecture services.

**Standard Operating Environment (SOE)** is a client computing device (Windows or MacOS) that has been pre-configured by ITDS with necessary software and security settings.

**University of Adelaide User ID** – a unique seven-digit number prefaced by ‘a’ provided to University of Adelaide account holders.

**University IT** means any;

1) computing or communications device or infrastructure;
2) computer or communications program or software;
3) service that provides access to the internet or information in electronic format;
4) computer network, website or online forum, including social media; or
5) electronic data stored or processed in any of the above.

that is owned, managed, hosted or provided by the University (whether through ITDS or other organisational units within the University) or a third-party provider on the University’s behalf.

**User** means any person who accesses University IT whether they are account holders or not.