IT Acceptable Use and Security Policy

OVERVIEW

The University of Adelaide seeks to provide its IT users with secure and timely access to IT equipment and the online services and resources necessary for undertaking their work and study. This Policy sets out the rules applicable to the use of University IT and expresses the commitment of the University to providing and maintaining a secure, effective and reliable IT infrastructure and services to support the University's operations.

SCOPE AND APPLICATION

This Policy applies to all users of University IT. This Policy also applies to users connecting personally owned devices 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.
d) Use of University IT or BYOD must not jeopardise the fair, secure, and productive IT environment of the University community, nor the University's operations, assets, data integrity or reputation.
e) Users must not install or use unlicensed or malicious software on University IT or BYOD, nor circumvent the University's IT security measures.
f) 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.

2. Administering University IT

a) Provisioning and de-provisioning of University of Adelaide User IDs and other access to University IT is governed by formal business rules administered by Information Technology & Digital Services, Human Resources and Student Services.
b) The University may impose volume quotas (e.g. printing, file storage, downloads) and security measures on the use of University IT.
c) 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.

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 an information security governance framework in order to effectively manage the security of University IT.
c) The Chief Information Officer is ultimately responsible for the security of University IT. For University IT resources not managed by Information Technology & Digital Services, the respective IT custodians are responsible for the implementation and management of this Policy and IT Security Procedures in relation to University IT resources managed by their area.
d) 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, with or without prior notice.
e) Acquisitions of, and changes to, University IT should not expose the University to unacceptable levels of information security risk.
f) The security of University IT is maintained in order to protect the University's operations and information assets. Users should not use systems outside of University IT to conduct University business unless there is a genuine need to do so and such use is compliant with the University's Information Classification and Protection Guidelines.

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.

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 Heads of Schools Branch Heads or their delegates	
University Operations	Information Technology	Authority to authorise the creation of generic, casual, and external visitor accounts	Area Managers Heads of Schools Branch Heads 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 Heads of Schools Branch Heads or their delegates	
University Operations	Information Technology	Authority to request examination of an account holder's use of IT Facilities	Area Managers Heads of Schools Branch Heads	

University Operations	Information Technology	Authority to approve Peer to Peer software for lawful purposes	Area Managers Heads of Schools 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 Executive Director, Human Resources	If account holder is also a student, approval of Executive Director, Academic & Student Engagement is also required
University Operations	Information Technology	Authority to order the immediate suspension or termination of a student account	DVCs and VPs Executive Director, Academic & Student Engagement	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 CIO Director, IT Operations & Digital Services, ITDS Director, IT Strategy, Planning & Governance, ITDS Chief Information Security Officer, ITDS	
University Operations	Information Technology	Authority to approve changes to the stand alone procedures related to this Policy.	COO	

RMO File Number	2018/8025
Policy Custodian	Chief Operating Officer
Responsible Officer	Chief Information Officer, Information Technology and Digital Services
Endorsed by (Academic Board or VCE)	Vice-Chancellor's Executive
Approved by	Vice-Chancellor and President on 5 February 2016
Related Procedures	IT Acceptable Use Procedures IT Security Procedures

	Information Classification and Handling Guideline Third Party Hosting Security Guideline
Related Documents and Policies	Code of Conduct Policy Behaviour and Conduct Policy Student Misconduct Rules Copyright Policy University Records Policy Privacy Policy
Related Legislation	Criminal Code Act 1995 (Cth) Spam Act 2003 (Cth) Copyright Act 1968 (Cth) Telecommunications (Interception and Access) Act 1979 (Cth)
Superseded Policies	5 February 2016
Effective	5 February 2016
Next Review Date	31 December 2018

**GLOSSARY:

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

Business Owner means Head of School, Branch Head, Director or Area Manager ultimately accountable for University IT managed by that area. Information Technology & Digital Services is the Business Owner for all IT infrastructure it provides.

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.

Area Managers means the Deputy Vice-Chancellors, Vice Presidents, Chief Operating Officer, 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.

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.

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,
5) electronic data stored or processed in any of the above,

that is owned, managed, hosted or provided by the University (whether through Information Technology & Digital Services or other organisational units within the University) or a third-party provider on the University's behalf.

University of Adelaide User ID – a unique seven digit number prefaced by 'a' provided to University of Adelaide account holders.

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