Information Security Policy

1. Purpose

1.1 The Information Security Policy (the policy) aims to reduce the risks to personal, sensitive and proprietary information that is held on UTS systems, devices and locations by maintaining robust information security through its people, processes and technology.

1.2 This policy outlines the university's framework for the management and protection of:

- UTS information technology (IT) infrastructure and resources
- UTS operations and general functions
- corporate data, and
- personal information held by the university.

2. Scope

2.1 This policy applies to UTS staff, students, affiliates and visitors (hereafter users) as well as any person with access to UTS IT resources.

2.2 UTS controlled entities may use this policy or develop their own. The policies and practices of controlled entities must be equivalent to the standards and expectations outlined in this policy and the Provision and Acceptable Use of Information Technology Resources Policy.

2.3 The security of corporate data should be managed in line with this policy, the Provision and Acceptable Use of Information Technology Resources Policy and the Data Governance Policy.

2.4 The security of personal information should be managed in line with this policy and the Privacy Policy.

2.5 Research data should be managed in line with this policy and the Research Policy (and associated procedures).

3. Principles

3.1 IT resources, infrastructure and corporate data are vital assets of the university, critical to the effectiveness and success of its core business. UTS is committed to the protection of these assets by having appropriate security mechanisms in place.

3.2 Information security is a collective challenge requiring a collective response. Information security cannot be addressed through technology alone. People and

processes are equally as vital. UTS seeks to build a 'cyber aware' culture to increase user awareness of potential risks and threats and to establish appropriate responses.

3.3 UTS will continually review and update its security processes to address industry standards and best practice (for example the Guidelines to Counter Foreign Interference in the Australian University Sector). This is also in line with compliance requirements (refer UTS Governance (Staff Connect)).

3.4 When acquiring, developing and maintaining new and existing IT resources, UTS will identify, assess and mitigate security risks, to the extent possible, in line with the Risk Management Policy.

4. Policy statements

Cyber threat and awareness

4.1 The UTS Cybersecurity Framework supports the university in managing cyber risk. It is managed and published by the Information Technology Division (ITD) on behalf of the Chief Information Officer (CIO). The framework comprises this policy, the Cybersecurity Standards (available at Beyond the Firewall: UTS Cybersecurity (SharePoint)) and related governance instruments including but not limited to:

- the Provision and Acceptable Use of Information Technology Resources Policy, which outlines requirements for the acquisition, use and expectations of behaviour around IT resources
- the Data Governance Policy, which outlines the management and classification of data
- the Privacy Policy, which outlines requirements for complying with relevant privacy legislation
- the Risk Management Policy, which guides the identification, assessment and treatment of risks and opportunities at UTS, and
- IT security, incident reporting, access and risk guidance approved by ITD or the CIO from time to time.

4.2 ITD will provide users with access to information and training (for staff and students) to minimise information security risks and support compliance with this policy. The Cybersecurity Standards and this policy will be continuously reviewed and improved to align with the ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements.

4.3 Deans and directors are responsible for ensuring that:

- staff knowledge and skills are kept up to date
- information security responsibilities are reflected in business planning and individual workplans, and
- all local procurement and management of IT resources complies with this policy and the Cybersecurity Standards (available at Beyond the firewall: UTS Cybersecurity (SharePoint)).

4.4 The UTS User Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint)) supports this policy and the Provision and Acceptable Use of Information Technology Resources Policy by consolidating the security obligations of all users. All staff are required to take steps to ensure they are informed about cyber risks that may impact their work and how to recognise them.

4.5 These user standards are aligned with ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements and include information on:

- securing UTS information and data
- managing passwords and other access information
- managing and protecting devices and accounts (including personally owned devices)
- protection and security of UTS information and the UTS network
- how UTS seeks to prevent cybersecurity incidents, and
- reporting cyber incidents.

4.6 The UTS Infrastructure Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint)) supports this policy by outlining the security requirements and standards for the university's physical and other IT resources, data and network.

Prevention and risk management

4.7 ITD will regularly assess the university's information security posture and conduct cyber hygiene checks. ITD will also maintain a forward plan that ensures continuous improvement. For insurance purposes, ITD will facilitate external assessments annually (or as otherwise requested) to identify and assess UTS vulnerabilities.

4.8 IT resource owners are responsible for providing details of locally owned resources to ITD for inclusion on central registers. IT resources must be procured in line with the Provision and Acceptable Use of Information Technology Resources Policy, Procurement Policy and UTS Delegations.

4.9 IT resource owners must perform an annual risk assessment for all IT resources under their ownership and/or remit of responsibility in line with the Risk Management Policy. This risk assessment is designed to:

- identify any information security risks (potential or known risks)
- help owners develop the appropriate security controls
- prompt collaboration with ITD to document and learn from risks and risk mitigation strategies.

4.10 Identified risks should be managed locally where possible, with advice on risk management and mitigation sought from ITD when required.

4.11 IT resource owners must implement security controls in line with the User Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint)) and report these to ITD as part of the risk management process.

4.12 ITD will maintain a register of IT and cyber risks to develop a knowledge base for risks and associated responses as part of the continuous improvement cycle.

Information security governance

4.13 The Cybersecurity Steering Committee, established by the CIO and managed by the Chief Information Security Officer (CISO), is responsible for reviewing information security risk assessments and providing guidance and advice to the CIO.

Access controls and password security

4.14 UTS acknowledges the security information described in the Guidelines to Counter Foreign Interference in the Australian University Sector and will seek to meet recommendations wherever possible.

4.15 Background checks will be conducted for staff in roles that involve elevated access to UTS information systems before employment, promotion or the granting of increased access as appropriate. Guidance on appropriate probity, reference checks and background checks for access and security purposes is available at Background checks (SharePoint).

4.16 Access to UTS information systems is restricted to authorised users in line with the Data Governance Policy, Privacy Policy and Information Security Classification Standard (available at Information security (SharePoint, staff only)).

4.17 Storage of corporate data and access to university records must be managed in line with the Records Management Policy.

Use of non-UTS resources, BYOD and remote working

4.18 Personal devices (bring your own device (BYOD)) may be used to undertake UTS business or duties, however, the requirements of this policy and the User Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint)) must be followed.

4.19 ITD will provide support and information on software issues encountered while using personal devices for UTS business purposes. It is the user's responsibility to ensure that this support does not constitute a breach of contract or warranty associated with the personal device.

4.20 Users who have been provided with a UTS device are expected to use this device for work and other UTS business purposes in line with the Provision and Acceptable Use of Information Technology Resources Policy.

4.21 Users must exercise additional caution when working remotely, including:

- minimising temporary local storage of information (digital or print) in line with the User Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint))
- primarily using UTS controlled file sharing/record management systems or, where this isn't possible, transferring information to a UTS controlled file sharing/record management system in a timely manner (normally within a week of access or creation)
- only using home networks where appropriate security controls are in place (for example wi-fi password protection and antivirus software), and

- taking appropriate measures to mitigate cyber risks associated with international travel.

4.22 All users who work or study remotely must comply with the Provision and Acceptable Use of Information Technology Resources Policy and any guidance provided by ITD from time to time and published at Beyond the firewall: UTS Cybersecurity (SharePoint) (for staff) and Supporting online study (for students).

Incident management and reporting

4.23 Information security incidents (including data breaches, loss of networked device, ransomware), regardless of whether they occur on campus or at another location, must be immediately reported to the ITD Cybersecurity Team to ensure a quick response and to initiate insurance coverage (as required) in line with the IT Security Incident Reporting Procedure (available at Beyond the firewall: UTS Cybersecurity (SharePoint)). These procedures must be accessible to all staff and students.

4.24 Any user may report an incident. Corrective action must be taken as soon as an incident is identified in line with the IT Security Incident Reporting Procedure (available at Beyond the firewall: UTS Cybersecurity (SharePoint)).

Continuity planning

4.25 Information security considerations must be included in UTS's business continuity planning. Individuals with specific information security responsibilities must have these reflected in their workplans.

Exemptions

4.26 Exemptions to this policy and the Cybersecurity Standards are not normally approved. Where absolutely necessary, and where extenuating circumstances apply, exemption requests may be submitted by the dean, director or IT resource owner (with appropriate delegated authority) in writing to the CIO outlining the:

- nature of the exemption and the specific control requiring adjustment
- rationale and extenuating circumstance
- risk that is introduced as a result of the proposed exemption and the alternative controls that will be put in place to manage or mitigate the risk
- endorsement from the Chief Data Officer (in consultation with the Privacy Officer) that any data privacy risks have been sufficiently considered and managed, and
- steps that will be taken to ensure future compliance with this policy and the User Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint)).

4.27 All approved exemptions must be:

- granted for a specific time period, usually up to a maximum of one year
- maintained on a register, which may be reported to the Audit and Risk Committee at the request of the committee or Council, and
- reviewed annually.

4.28 The CIO (or the CISO) may seek advice from UTS Legal or the Director, Risk in considering an exemption application in line with this policy.

4.29 Exceptions granted in line with this policy should be reported to the Cybersecurity Steering Group and used as part of the continuous improvement cycle.

Policy breaches

4.30 Breaches of this policy will be managed in line with the Provision and Acceptable Use of Information Technology Resources Policy.

4.31 Data breaches must be managed in line with the Privacy Policy and Data breach response procedures (Staff Connect).

5. Policy ownership and support

5.1 **Policy owner:** The Deputy Vice-Chancellor (Corporate Services) is responsible for policy enforcement and compliance, ensuring that its principles and statements are observed. The Deputy Vice-Chancellor (Corporate Services) is also responsible for the approval of any associated university-level procedures.

5.2 **Policy contact**: The Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) are responsible for the day-to-day implementation of this policy and act as primary points of contact for advice on fulfilling its provisions. The CIO is also responsible for approving exemptions, approving and publishing the User Cybersecurity Standard (available at Beyond the firewall: UTS Cybersecurity (SharePoint)) and any training associated with this policy.

5.3 **Others**:

- Users are responsible for being aware of and acting on information security risks in line with this policy.
- The Cybersecurity Steering Committee is responsible for providing guidance and advice to the CIO for action in line with this policy.
- The Chief Data Officer is responsible for managing corporate data in line with the Data Governance Policy.

6. Definitions

The following definitions apply for this policy and all associated procedures. These are in addition to the definitions outlined in Schedule 1, Student Rules.

BYOD is a commonly used acronym that means bring your own device.

Corporate data is defined in the Data Governance Policy.

Cybersecurity and **information security** are used interchangeably/synonymously. Policies will refer more to information security to align with ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements. Both terms refer to the various mechanisms used by UTS to protect its information and IT resources (see information security below).

Cybersecurity Standards means the collection of procedures, forms and guidelines managed and published by ITD at Beyond the firewall: UTS Cybersecurity (SharePoint) for users to implement the provisions outlined in this policy.

Data breach is defined in the Privacy Policy.

Information security means the various mechanisms used by UTS to protect its information by preventing, detecting and responding to information security attacks.

Threats to the security of UTS information and systems include, but are not limited to:

- deliberate unauthorised access allowing for potential malicious activity (for example theft, manipulation or misuse of information). This could be from organised criminal groups, individual attackers, nation state actors, competitors and/or UTS staff
- accidents and errors in sharing or providing access as a result of low user awareness of good practice or intended consequences
- attacks that deny access of legitimate users to the systems and information for a period of time and, in the worst case, requires complete replacement of systems and huge loss of information.

Information technology (or IT) infrastructure means the university's framework of software, hardware, networks and other components.

IT resources is defined in the Provision and Acceptable Use of Information Technology Resources Policy.

IT resource owner means the director, dean or other senior manager responsible for the faculty, unit or other business area that is the owner of an IT resource.

7. Approval information

Policy contact	Chief Information Officer and Chief Information Security Officer
Approval authority	Vice-Chancellor
Review date	2022
File number	UR21/822
Superseded documents	Information Technology Security Vice-Chancellor's Directive 2014 (UR12/1005)

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	26/07/2021	12/08/2021	New policy.

Web version

Information Security Policy

References

Cybersecurity standards

Beyond the firewall: UTS Cybersecurity (SharePoint):

- User Cybersecurity Standard
- The Information Classification Handling Matrix for Users
- Infrastructure Cybersecurity Standard
- IT Security Incident Reporting Procedure
- Cybersecurity Vendor Questionnaire
- UTS and Vendor Security Responsibilities for Cloud Services

Information Classification Standard (available at Information security (SharePoint, staff only))

UTS policies and rules

Data breach response procedures (Staff Connect)

Data Governance Policy

Privacy Policy

Provision and Acceptable Use of Information Technology Resources Policy

Records Management Policy

Research Policy

Risk Management Policy

UTS Delegations

External documents

Guidelines to Counter Foreign Interference in the Australian University Sector

ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements