DITM and Records Management Policy Manual

Section 1 - Purpose

(1) The purpose of this Manual is to outline the University of Canberra's (University) principles concerning the use of technology. The two primary areas of focus are IT Security and Acceptable Use, and Enterprise Architecture.

(2) The University's primary functions depend on the quality of information provided by DITM resources. This Policy Manual will ensure the following:

a. availability and reliability in the provision of DITM services;
b. accuracy and integrity in the management and delivery of information;
c. protection of University's assets, including information, knowledge, software, hardware and facilities;
d. information privacy and confidentiality is maintained according to legislative requirements;
e. University's operations are secure from disruption;
f. DITM resources are used in an appropriate manner;
g. protection of the University's reputation.

Section 2 - Scope

(3) This Manual covers all policies relating to Digital, Information and Technology Management and applies to all staff, students and members of the University community.

Section 3 - Principles

Part A - IT Security and Acceptable Use

Acceptable Use

Purpose and Scope

(4) This section provides information on the access available to staff, students and other members of the University community to the University's computer network, and through it to the Internet, and their obligations when using the University network.

Principles

(5) The University network is provided for use for educational, research and administrative business of the University including related social interactions. Limited personal use is permitted but the University network must not be used for personal gain.

(6) Users must comply with all legislation and University policies relating to access and use of the network and other IT resources.

(7) Users must act in a courteous and responsible manner in all technology-enabled communications and must not use these in a manner which misrepresents the University or brings it into disrepute.

(8) The account owner is responsible for all information access and all changes which are carried out while accessing a system through their account/password combination.

(9) The University's systems must not be used to harass, abuse or otherwise seek to offend individuals.

(10) The University's systems must not be used to access, store or transfer illegal material, such as unauthorised copyright material or child pornography.

(11) It is the responsibility of departing staff or affiliates and their Supervisors to ensure that any required electronic business files, documents and emails are appropriately stored, transferred or otherwise made accessible to the Supervisor well in advance of the departing staff or affiliates' termination date.

General IT Security

Purpose and Scope

(12) This section covers assets including, but not limited to:

a. Information assets (e.g. databases, files, electronic documents);
b. Software assets (e.g. applications, software tools, licences); and
c. Physical assets (e.g. computers, servers, network infrastructure, information storage media, printers, communications equipment, AV equipment, projectors, telephones and facilities)

(13) Security breaches or any risk of threats arising from:

a. On-campus devices not approved for network connection;
b. On-campus networks not installed or approved by DITM; and
c. Off-campus networks and devices are within the scope of this Policy insofar as taking any necessary action required to mitigate, remove or neutralise any apparent risk or threat to IT security.

(14) All staff, students and users, including affiliates, alumni and tenants, who are given access to the University's information systems must agree to abide by the University's information security and privacy policies.

Principles

(15) At any point that University IT resources are being used, all relevant University policies will be applicable; whether on or off campus. The University retains the right to monitor and control DITM systems and their content, including network and system activity, in accordance with the University's "Charter of Conduct and Values" and Privacy Policy and in a manner which respects the rights and legitimate interests of those concerned.

(16) The authority to inspect machines, servers and files resides with the Director, DITM. Disclosure to an external organisation will only be considered on production of a legal authority or to the University's vetted and approved vendors covered by contractual obligations (eg, Oracle can do system audits under the agreement we have).

(17) Systems that are deemed to pose a threat to the University network will be disconnected from the network without notice.

(18) The University reserves the right to suspend or terminate access to a user account in cases of suspected security breaches, inappropriate or illegal activity, or unauthorised access. For the avoidance of doubt, this includes staff, student and affiliate accounts.

(19) Security incidents will be handled in accordance with DITM Cyber Security Incident Response Plan.

(20) All major systems and information assets must be accounted for and have a nominated Custodian who is responsible for the implementation and management of this Policy in relation to those assets. Where no custodian is nominated the senior business manager of the area most responsible for the system is accountable.

(21) All DITM managed systems will be maintained to a base line of security through best practice security controls such as regular patching and centralised management.

(22) Network services and software applications which require higher levels of security will only be accessible remotely via the University's Virtual Private Network (VPN).

(23) Members of the University community who use public access or other non-University IT services to access University resources are obliged to respect the University's policies as well as the relevant security policies of the remote service.

(24) To ensure that no private or confidential information is exposed, any user accessing a secure system remotely should do so only on trusted networks.

(25) University-owned data or information may not be stored using public cloud services, i.e. Dropbox or similar, except under a University-approved contractual arrangement nor can it be forwarded to separate email accounts outside the University.

(26) Any data breaches, or suspected data breaches, must be reported to the Service Desk immediately upon discovery.

(27) Access to the University's network services by students will be granted six months prior to their course commencement date, and the network account will be removed thirty days from their discontinuation date, or graduation date. Access to the University's network services by staff or affiliates, will be removed three days after their termination date.

User Account and Password

Purpose and Scope

(28) This section will define the principles governing the creation, use and ongoing management of user accounts and passwords for any IT system associated with the University.

Principles

(29) Users must activate a password protection method to secure their workstation or devices with University network access or content. All devices should be locked prior to leaving them unattended. Where a Multi-factor Authentication (MFA) is available in a system it must be used.

(30) All mobile devices, including phones, tablets and laptops, that are used to access or store University data or information must be password or passcode protected. This applies whether the device is a University asset or a personal device.

(31) Members of the University will be issued with a University Network Account user ID, which will be based on the University staff, student or affiliate ID number.

(32) All general access to University corporate systems should be configured to utilise the University Network Account and associated password.
Exceptions to this rule are:

a. Systems that do not store or transmit the password in encrypted format. Such systems must NOT use the University Network Account and password.
b. Systems that that are not under the control of the University and which are not operating under a contract or agreement with the University. Such systems must NOT use the University Network Account and password.
c. Systems which require an additional level of security which warrants a separate password due to elevated levels of access in accordance with the Privileged Account Guide.

(33) The onus of protecting the University Network Account password is on each individual. The University password must not be used on other systems, shared or disclosed with anyone, including assistants or family.

(34) The possession of an account and a password that enables access to read or update particular information does not constitute the authority to do so. Such authority must be explicitly granted by a System Custodian. It is the responsibility of the System Custodians to audit key corporate system privileges and ensure they are commensurate with current staff roles.

(35) Password complexity for University account passwords is determined by the strongest accepted rules of our weakest system and subject to change as systems mature or are updated. The strongest password that can be used within the restrictions of that particular facility, system or service shall be used.

(36) It is recommended that user-level passwords be changed at least every six months. User-level passwords must be changed if the accounts with MFA do not meet the University's complexity requirements or are known to other individuals.

(37) Passwords for privileged accounts must be changed at intervals as follows:

a. Corporate Systems Group members and System Custodians: Every 8 weeks in addition to the requirements for user-level passwords.
b. System-level passwords (e.g. root, administrator): As per user-level passwords and otherwise changed every 6 months automatically where possible. Where auto changes are not supported, system-level passwords must be changed every time a staff member with access to the password leaves the University.

(38) All passwords must:

a. Contain eight characters or more.
b. Contain lower-case letters, upper-case letters, numbers, and non-alphanumeric characters.

Special Case Data Access

Purpose and Scope

(39) This section covers the access of staff members' files or data under special circumstances.

Principles

(40) Access to a current staff member's electronic data, which includes email, and documents stored centrally (e.g. H: drive and Microsoft Office 365) or locally (e.g. C: drive), is only permitted if accompanied by a business case, approved by the relevant Dean/Director and approved by the Director, DITM. A record of access including the business case and authorising Dean/Director must be created and kept.

(41) Where reasonable grounds exist to justify accessing a former staff member's email or electronic files, access may be provided to the Supervisor or other nominated staff as approved by the Dean or Director after consideration of a business case by the Director, DITM.

Email Use

Purpose and Scope

(42) This section covers the use of email originating from University email accounts for staff or students.

Principles

(43) University staff will utilise email for University-related communication with staff, students and affiliates.

(44) Email copies of highly sensitive information must be encrypted when transferring to an external entity or recorded to an external data storage device.

(45) The content of email sent by University staff and students must not be offensive, harassing, discriminatory or illegal. In addition, University email accounts must not be used for personal gain or commercial purposes.

(46) While the University will make every endeavour to ensure that email delivered to University accounts is free from spam and malware, it takes no responsibility for any damage caused by the failure to detect spam or malware or the inadvertent blocking of a legitimate email.

(47) Students are required to use their student email when contacting the University via email for pastoral, administrative, or academic matters.

(48) Staff are expected to use the University-provided email account for all University email correspondence and may not automatically forward their email to private addresses unless authorised by the Director, DITM.

(49) All staff members are required to include a signature on all emails sent externally, which should be aligned with the University's standardised signature block.

Privately Owned Devices

Purpose and Scope

(50) This section defines University policy with respect to privately owned devices which are brought onto the University campus, connected to the University network and/or used for University business.

Principles

(51) Privately owned devices may be connected to the University network (wired or wireless) provided that these meet basic levels of security as determined by the University.

(52) The University reserves the right to inspect all privately owned devices which are connected to the University network to investigate suspected security breaches, inappropriate or illegal activity, or unauthorised access.

(53) Privately owned devices that are deemed to pose a threat to the University network will be disconnected from the network without notice.

(54) The University accepts no responsibility for any loss or damage to either the physical device or data contained within it as a result of bringing the device onto the University campus, connecting it to the University network and/or using it for University business.

(55) The University accepts no responsibility for the support and maintenance of privately owned devices whether or not they are used for University business. This includes privately owned data storage media connected to staff or student workstations.

(56) University-owned data or information must not be stored on privately owned equipment.

Third Party Contract and Access Security

Purpose and Scope

(57) This section sets out the conditions that are required to maintain the security of the University's IT resources when contractors, outsourced providers, service suppliers or any other third-party providers are involved in the University's operations. This may include, but is not limited to, the following circumstances:

a. third-party system design, development or operation of University services;
b. access granted from remote locations where computer and network facilities may not be under the control of the University; or
c. when authorised third-party providers are given access to information or information systems.

Principles

(58) All third-party providers who require access to the University's information systems must agree to comply with all relevant University policies at the time of contract signing. Should the said policies change within the contract period, a deed of variation will be drawn up and third-party providers must agree to comply.

(59) Due to the confidentiality, sensitivity or value of the information that may be accessed, the University may require third-party providers to sign a confidentiality agreement to protect its information assets.

(60) All contracts with third-party providers for the supply of services to the University must be monitored and regularly reviewed to ensure that information security requirements are being satisfied.

(61) Authorised third-party providers must be given minimum access privileges to meet their contractual requirements. They are not permitted to copy or store any University information for any reason other than that required to complete the terms of their contract.

(62) All third-party providers must report any instance, including physical, of unauthorised access, transmission, or loss (or suspected loss) of University data by a third-party. In addition, third-party providers must report IT security incidents that may impact systems connected to the University's systems.

IT Physical Security

Purpose and Scope

(63) This section sets out the minimum standards for implementing physical control measures to protect the University's IT architecture. IT assets are generally associated with the physical devices on which information resides and includes, but is not limited to, workstations, servers and the physical network infrastructure.

Principles

(64) Physical access controls around computing locations are to be applied in a manner that reflects the business value and criticality of IT services hosted in the location and the value of the data stored.

(65) Computer laboratories and other locations that house DITM assets must employ physical access controls such as electronic or physical locks.

(66) No computer equipment is to be removed from any office, work area or computer laboratory unless specific authorisation has been received from DITM.

(67) Persons who are issued with portable information technology assets, such as laptops, must agree to bear personal responsibility of the equipment. When not in use, all portable information technology assets must be adequately secured.

Part B - Enterprise Architecture

Scope

(68) This section of the Policy Manual outlines the Universities principles for the design and implementation of technology.

Design Principles

Principles

(69) DITM offers support for re-designing of University's systems and assesses new technologies to ensure cohesive and effective alignment of business, information, process and technology.

(70) Cloud services will be adopted first, as long as they are fit for purpose, provide better value for money, provide appropriate security and risk measures and have adequate back-out and Disaster Recovery measures.

(71) Where appropriate, the University will utilise cloud services to enable testing and development of IT systems.

(72) Out of the box solutions for both cloud and in-house systems should be adopted in favour of systems that aren't quite fit for purpose which then require further customisation.

(73) The fundamental concepts of least privilege, default to deny and defence-in-depth must be applied to all devices connected to the University network.

(74) In support of the use of privately owned devices on campus, the University is committed to providing ubiquitous power and WiFi access campus-wide within the constraints dictated by budget and resources.

(75) Unless specifically required, all new services and applications must be designed to be accessible for users regardless of the network being used, resulting in the same experience whether on campus or off.

(76) The University will design infrastructure that is flexible and scalable, future-proofed to allow for migration to other platforms (including cloud) and capable of future orchestration. Where hardware must be purchased, it should be reusable and efficient.

(77) Modifications to any system or network are only permitted where authorised by DITM.

(78) The addition of any new technology systems must be reviewed by the University's Legal team and by completing the New Product Questionnaire prior to procurement. Any new technology systems must also be approved by the Change Advisory Board (CAB), prior to implementation, to ensure these systems do not conflict with the University's environment.

Records Management

Purpose and Scope

(79) The purpose of this section is to provide direction to all staff on the management of University records and applies to all records created and/or captured during the conducting of University business.

(80) The University is obliged to comply with all requirements of relevant legislation. Therefore, adherence to the requirements in this Policy and the accompanying Records and Archives Management Procedures is mandatory for all

staff.

(81) All staff employed by the University in any capacity are responsible for recordkeeping.

Principles

(82) The Records Management Program is to conform to the Territory Records Act 2002, as well as the Territory Recordkeeping Standards for Records Management. In cases where recordkeeping issues arise which are not covered by this Policy, the University will follow advice from the Territory Records Office and be guided by the Australian Standard on Records Management, AS ISO 15489.

(83) Recordkeeping will be a routine part of conducting business and will be closely aligned to the University's business processes. An analysis of these processes within the context of business needs, legal and regulatory obligations, as well as meeting broader community expectations is to be used as the basis of design for a recordkeeping system. These needs and obligations will be reviewed on an annual rolling review plan or as the result of significant change.

(84) All records created or captured by the University Community are corporate assets that are owned by the University and managed accordingly.

(85) No records are to be destroyed without an approved Records Disposal Schedule.

(86) The University is to use a controlled language system to title its records. The business classification system (thesaurus) is to be based on the functions and activities that it carries out. This includes using the Territory Records Administrative Disposal Schedule terms for common administrative functions such as Financial Management, Personnel and Occupational Health & Safety.

(87) Everyone employed by or contracted to the University is to make and keep full and accurate records that are incorporated into the University's recordkeeping system. That is, the University's recordkeeping practices will ensure that its records are adequate for:

a. facilitating action by employees at any level, and their successors;
b. making possible a proper scrutiny of the conduct of business by anyone authorised to undertake such a scrutiny; and
c. protecting the financial, legal and other rights of the University, its clients and any other people affected by its actions and decisions

(88) Records management methods and recordkeeping systems are to be reviewed every 24 months to ensure their continuing suitability and effectiveness. The Director, DITM may initiate an earlier review when significant functional or other changes affecting recordkeeping occur. Records of these reviews are to be maintained by the Records Management unit.

(89) Records and Archives Management Procedures are to be designed to detail the way all staff will make, modify, use, handle and care for records, as well as how and for how long records will be kept. The procedures are also to describe how to identify, search for and retrieve records as well as gain access to them.

Backup Policy

Purpose and Scope

(90) This section mandates and communicates the University's principles relating to the backing up and retention of corporate data assets.

(91) Any non-corporate data assets are considered out of scope of this backup policy.

Principles

(92) All corporate data is to be stored on University managed facilities, which are regularly backed up.

(93) A full backup from each year is retained for a minimum of seven years.

(94) Where a data custodian has identified or requested a different set of backup requirements, some data sets may be backed up outside of the standard practice described above.

(95) The physical and logical security of the backup media must be at least equivalent to the security required for the access to the data on the server itself, as dictated by the Records Management section of this document.

(96) The backup medium must be of a type that will remain readable and be accessible for the length of time for which the backups are to be retained.

(97) Backups of corporate data assets are distinct from the University's records management system and are purely a disaster recovery mechanism.

Section 4 - Responsibilities

(98) Information security of each system/application will primarily be the responsibility of its custodian.

WHO	RESPONSIBILITY
Deans of Faculty or Directors of Unit	Responsible for ensuring that this Policy is implemented and adhered to within their respective Faculty or Unit.
Data Custodian	Ensure that processes are in place for backing up the data in the domain of custody.
DITM	To work collaboratively with various units of the University, that provide services related to information security, both directly and indirectly, on generation of standards and implementation of this Policy.
Director, DITM	Ensure that all University owned corporate servers are backed up as required by this Policy statement. The execution of backup processes is shared between DITM and the current outsourced service provider.

Section 5 - Procedure

(99) Nil.

Section 6 - Definitions

Abbreviation or Term	Meaning
Account owner	Any person granted a user account with the University.
Activities	Activities are the major tasks performed by the University to accomplish each of its functions. Several activities may be associated with each function. Activities are often described as actions or verbs, such as Reporting.
Approved Devices	University-owned and DITM-configured devices.
Archival Record	Archival records are those records that have been appraised as having long-term, enduring or permanent value such as Council Minutes, University Research Reports (of major national or international significance) and Examination Results.

Abbreviation or Term	Meaning
Authorized User	Any user who has been authorised by the relevant Supervisor/officer to access a system or IT facility, and includes (but is not limited to) staff of the University or any company in which the University has an interest or any company or organisation with which the University is pursuing a joint venture, students, consultants, visitors, Honorary appointees.
Availability	Availability refers to the ongoing operations and delivery of intended services by a system (e.g. finance or payroll) and its components.
Business Information Systems (BIS)	• Organised collection of hardware, software, supplies, policies, procedures and people, which stores, processes and provides access to the University's business information. • Automated systems that create or manage data about the University's activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers – for example, the student management system, finance or human resources systems, an e-commerce system, and purpose-built or customised databases.
Confidentiality	Confidentiality refers to the need to ensure that information is accessible only to those authorized to have access.
Corporate Data	Data which forms a part of the University's records for internal, external or public use pertaining to the University's business including operational, administrative, teaching and/or research activities. For example: All Home Drive Data (H:\) – Staff and Students All Group Shares (\\ucstaff\dfs\...)
Data Custodian	The custodian is the individual responsible for the content of any data file or system. Note that it is not usually the creator of a document or a system operator.
Database Data	The content and configuration of all databases.
Default to deny	Means the setting of norm to denying access so that specific instruction must be provided to all access.
Designated authority	The person with the authority to formally assume responsibility for the action or decision in question
Email Data	All email and calendar items in all subfolders of staff email accounts.
Full Backup	Back up of all targeted files.
Functions	Functions are "the largest unit of business activity". They represent the major responsibilities that are managed by the University of Canberra to fulfill its goals. Functions are high-level aggregates of the University's activities. Functions are often described as things or with nouns, such as Teaching and Learning, Research and Student Management.
Incremental Backup	An incremental backup is a type of backup that only copies files that have changed since the last backup. For example; if you had 10 files on your desktop which you backed up to a USB drive, making a copy of all 10 files is termed as a FULL backup. If you have made changes to 2 of those files since your last FULL then copying only the two files that have changed to your USB drive is termed an INCREMENTAL backup. The strength of incremental backups include; significant time savings and effective use of storage. The downside is that an incremental is dependent on the last successful full backup.
Integrity	Integrity refers to the veracity of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.
IT services and systems	All information technology hardware, software, networks, processes and procedures utilised by University. 'IT services and systems' includes all stored data and information regardless of their storage or presentation media. 'IT services and systems' includes all environmental and support facilities.
DITM	Digital, Information and Technology Management
DITM applications	Includes all software owned or licensed by the University.

Abbreviation or Term	Meaning
DITM architecture	The University's information, DITM applications, and DITM infrastructure
DITM assets	Include all computers, terminals, telephones, end host devices, licences, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.
DITM Authorised Staff	University staff authorised by the Director, DITM to monitor accounts, files, stored data and/or network data, and to disconnect IT equipment in the event of an Information Security breach.
Least privilege	Means that each user be granted the most restrictive set of privileges needed for the performance of authorised tasks.
Member of the University	University staff, students and other individuals who have a role within the University that entitles them to a University Network Account and/or to the use of University DITM resources.
Monitoring	Refers to tasks (including testing and scanning) undertaken by DITM authorised staff to ensure maintenance of security of IT services and systems within the University's domain.
Network Resources	Include any networks connected to the University's backbone, any devices attached to these networks and any services made available over these networks. These include network servers, peripheral equipment, workstations and personal computers.
Normal Administrative Practice (NAP)	A process established to allow for the destruction of ephemeral, duplicate or transitory material of no evidentiary or continuing value. Examples include: Working papers consisting of rough notes, calculations, diagrams, used for the creation of records; Duplicates and copies of documents where the original is safely retained within the University's recordkeeping system and Personal material such as invitations, tickets, and brochures.
Offsite storage	Offsite storage is prescribed in consideration of geographical factors, with adequate separation being determined by distance, propensity of fire, flood, structure and materials. Storage at or above ground level, in fireproof containment, within buildings with only concrete and steel structure, in areas of low vegetation will deliver far lower risk than only considering distance. Therefore, this offsite storage policy statement will be superior to industry standards based on separation alone. Given this, the majority of buildings on the University campus will fulfill this requirement and therefore can be used as Offsite Storage sites if required.
Outsourcing	A contractual arrangement whereby services to or on behalf of the University that would otherwise be carried out internally are provided by an external organisation. Examples are financial, personnel, fleet or facilities management functions.
Physical and Virtual Server Data	Files and configuration required for the normal operation of each server.
Privacy	Privacy refers to restriction of access and appropriate use of personal information as defined by law.
Privately Owned Device	A privately owned device is a device that is not fully owned, leased or controlled by the University. It could be owned by an individual staff member or student of the University or by a third party. Devices which are funded by research or consultancy funding are regarded as University owned.
Public cloud	A platform that provides resources such as applications or storage to users remotely. The public cloud services may be free or offered through subscription or other pricing models such as pay-pay-usage.
Public Information	Information that, from time to time, is available for general access without the requirement for authentication.
Record	A record, in written, electronic or any other form, under the control of the University or that it is entitled to control, kept as a record of its activities, whether it was created or received by the University. According to Records Management 2002, records "reflect what was communicated or decided or what action was taken".
Recordkeeping Systems	Information systems that capture maintain and provide access to records over time. While the term is often associated with computer software, Recordkeeping Systems also encompass policies, procedures, practices and resources which are applied within the University to ensure that full and accurate records of business activity are made and kept.
Responsible IT Security Officer	University staff delegated to be responsible for IT security matters.

Abbreviation or Term	Meaning
Security	Security is defined as "the state of being free from unacceptable risk".
System Custodian	The staff authorised as the person responsible for the system and/or its information content.
Threat	Threats are the potential causes of loss or damage. These threats may be human or non-human, natural, accidental, or deliberate.
Trusted Network	A network that are only open to authorised users, requiring authentication through login credentials and encryption of data.
Unauthorised User	Any user who is not an Authorised User and who is accessing information other than Public Information.
University Network Account	The computer account provided by the University to all current staff, University visitors and students, which has a user ID based on the staff or student ID number, and which is used for user authentication for most IT systems via a corporate directory system.
User account	A defined user code with an associated set of privileges for access to information and update functionality. Access to the account is controlled by security measures which commonly include a password. The password is the confidential part of the logon process and must be protected by the account holder.

Status and Details

Status	Current
Effective Date	16th February 2024
Review Date	31st December 2024
Approval Authority	Chief Digital Officer
Approval Date	26th October 2022
Expiry Date	To Be Advised
Custodian	Craig Mutton Chief Digital Officer
Responsible Manager	Stef Batts-Cirilli Deputy Director, Digital, Information and Technology Management
Author	Geraldine Styles Senior Compliance Coordinator
Enquiries Contact	Policy