Information Security and Access Policy

Section 1 - Preamble

(1) Charles Darwin University (CDU) routinely gathers, stores, maintains, processes, transmits and disposes of records containing information that must be protected. This information plays a vital role in supporting the University's business processes and customer services by contributing to operational and strategic business decisions and conforming to legal and statutory requirements.

(2) The University acknowledges an obligation to ensure appropriate security for all Information and Communication Technology (ICT) data, equipment, and processes in its domain of ownership and control so that information can be protected to a level commensurate with its value to the organisation, while still being made available to those who need it.

Section 2 - Purpose

(3) This Policy provides definitive instruction on safeguarding information, protecting the University from the adverse impact on its reputation and operations and from failures of confidentiality, integrity and availability.

Section 3 - Scope

(4) This Policy applies to:

a. all staff members, students, contractors, consultants and volunteers who may use or have access to University information assets;
b. all University Associates and other members of the University community;
c. all information assets encompassing facilities, data, software, paper documents and personnel;
d. all clients of ICT equipment owned or leased by the University; and
e. all equipment connected to the University's data and voice networks.

(5) This policy applies irrespective of the location of the user accessing the data, including from outside of Australia.

Section 4 - Policy

(6) The University is committed to protecting information and providing access to information in support of its teaching, research, administrative and service functions. This Policy ensures that the University can protect the confidentiality, integrity and availability of information and services.

(7) For the purposes of this Policy, "information security" is defined as "protecting information from unauthorised access and disruption".

Information Security Principles

(8) This Policy is based on the following information security principles:

a. Logical Access and Physical Access Security: Logical access and physical access to information assets is granted on the "least privilege" principle, whereby each user is granted the most restricted set of privileges needed for the performance of relevant tasks.
b. Information Security Risk Management: Information security related risks must be identified, reported to concerned stakeholders and adequate controls must be recommended to manage the risk.
c. Operational Security: Operational security practices must be in place to manage information security related risks.
d. Information Security Incident Management: Information security incidents must be actively managed in a defined manner in line with the University's incident management process.
e. Information Classification: Information maintained in the university's information systems and in printed format is protected based on the assigned information classification level.
f. Audit and Compliance: The established information security management processes must be conducted in line with regulatory requirements and be regularly audited to promote improvements in practices.
g. Human Resource Security: The University must have processes in place to screen candidates, on-board and off-board employees, and educate employees on security awareness.

Information Security Governance

(9) Adequate information security governance will be achieved to ensure that:

a. information assets are adequately protected based on their classification and sensitivity;
b. risks are managed;
c. compliance with regulatory, legislative and contractual requirements are achieved; and
d. strategic business objectives are accomplished.

(10) A business risk approach towards information security risk will be adopted. The University's Enterprise Risk Management Policy ensures that risks are properly identified, analysed, evaluated, tracked, managed and reported.

Human Resources Security

(11) Adequate human resources processes (e.g. recruitment, on-boarding, off-boarding and disciplinary) will be established to reduce the risk of insider threats and unauthorised disclosure of information.

(12) Employees, contractors or third-party service providers seeking access to the University's information assets will have background verification checks carried out in accordance with University policies and procedures, relevant laws, regulations and ethics before being granted access.

(13) Students, employees, contractors and third-party service providers accessing or using the University's information assets will be subject to awareness and education activities including topics such as policies, responsibilities, consequences of non-compliance, potential security threats and how to prevent them.

(14) Management will require students, employees, contractors and third-party service providers to apply information security principles in accordance with this Policy and supporting IT Security Standards.

(15) Work agreements and contracts with employees, contractors and third-party providers will apply during and after employment.

Asset Management

(16) Information assets will be adequately used and protected based on the information they store, process or transmit.

(17) All information assets will be identified, classified, labelled and recorded in a centralised inventory, and will be subject to periodic reviews to confirm their existence, adequacy of implemented controls and appropriateness of defined classifications.

(18) Information assets will be securely removed, transferred, sanitised, destroyed and disposed of based on their classification and established procedures. All students, employees, contractors and third-party service providers will return University assets in their possession upon termination of their attendance, employment, contract or agreement.

(19) The use of removable media will be controlled based on the classification of assets and guidance from Digital Technology Solutions (DTS).

Access Control

(20) Adequate processes to provision, modify, revoke and revalidate user accounts will be established to reduce the risk of unauthorised access to information assets.

(21) Access to information assets will be authenticated based on a business need (need to know principle) and allocated the minimum required privileges (least privilege principle). Requests for elevated access must be documented with adequate and appropriate justification, based on the requester's business need.

(22) Students, employees, contractors and third-party service providers accessing the University's information assets will be uniquely identified. Use of generic user accounts will be strictly controlled.

(23) Unauthorised use of user accounts will be prevented by protecting authentication credentials and implementing technical controls.

(24) Authentication credentials must not be shared.

(25) All user account identification, authentication and authorisation activities will be logged and monitored.

Physical and Environmental Security

(26) Access to physical areas hosting the University's information assets will be controlled to ensure that only authorised employees, contractors and third-party services providers are allowed access.

(27) Information assets will be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

(28) Information processing and communication facilities hosting the University's information assets will be designed to withstand and adequately protected against natural and human-induced disasters as well as malicious attacks.

(29) Keys or equivalent access mechanisms to server, communications and security rooms as well as security containers will be appropriately secured and controlled.

(30) Operational procedures associated with information processing and communication facilities will be documented appropriately.

Operations Security

(31) Changes to production information assets will be controlled through a formal change and transition management

process.

(32) Information asset resources will be monitored and adjusted to requirements as necessary. Projections will be made of future capacity requirements to ensure that current and projected performance is achieved.

(33) Tools and procedures covering the detection of potential cybersecurity incidents will be established and maintained by DTS.

(34) Information backups will be performed on applicable information assets, based on their classification, business availability and integrity requirements.

(35) Information asset events are recorded, retained, archived, protected and correlated in order to detect, investigate and respond to security incidents. Logging and audit configurations will be defined and implemented in consideration of regulatory requirements and best practices.

(36) Managed Operating Environments (MOEs) will be defined, designed and implemented with a common, consistent and secure approach. MOEs and applications will be configured in a way that reduces the risk of cyber-attacks.

(37) Confidentiality, integrity and availability of database systems and their content will be maintained based on their classification.

(38) Up-to-date information about real and potential technical vulnerabilities in the University's information assets will be maintained, and will be evaluated and managed to reduce the risk of cyber-attacks.

(39) Audit requirements and activities involving the verification of operational systems will be carefully planned and agreed to minimize disruptions to business processes.

Communications Security

(40) Networks and information assets will be designed, configured and operated in a secure manner to prevent cyber-attacks and minimise disruptions.

(41) Appropriate security controls will be implemented to minimise unauthorized access and the effects of disruptions on the network and online services. A defence-in-depth approach will be incorporated by implementing multiple layers of controls.

(42) Intrusion detection and prevention controls will be implemented and maintained in order for the University to efficiently detect incidents and respond to cyber-attacks.

(43) Information asset transfers will be protected while at rest and in transit based on classification. Transfer and non-disclosure agreements between Business Owners and the sending or receiving organisations should be in place.

(44) Network traffic, including data being imported to or exported from a University information asset, will be monitored for malicious content and breaches of the policy.

(45) University-managed mobile devices and communication technologies will be controlled, secured and monitored.

System Acquisition, Development and Maintenance Security

(46) Information security requirements will be included in projects delivering new information assets or enhancements to existing information assets.

(47) Software developers will adopt secure programming practices and principles when developing software.

(48) Development environments will be established and protected. The production environments are logically

separated from the development ones.

(49) Information in production environments including anonymised production data will not be used in testing or development environments unless the testing or development environments are secured to the same level as the production environment. The use of production information for testing or development purposes will be approved and risk accepted by the Data Custodian and System Owner.

Supplier Relationships Security

(50) Third-party service providers will be procured following the University's procurement policies and procedures. Third-party service providers that access, store, transmit or process the University's information assets will be subject to thorough information security evaluations before entering into a contract.

(51) Controls associated with the protection of information assets that are entrusted to a third-party service provider, as well as any other requirements for providing the service, will be documented in contracts, memoranda of understanding, or any equivalent formal agreement between parties.

(52) Relationships with third-party service providers will be adequately managed by the Contract Owner.

(53) Third-party service providers will be periodically reassessed for compliance, changes and risk monitoring purposes.

Information Security Incident Management

(54) An Incident Response Plan (IRP) will be established and periodically tested. The IRP will consider common cyber-security incidents in order to ensure an efficient and orderly response to cyber-attacks.

(55) All cyber and information security incidents, such as unauthorised disclosure, access or deletion/destruction of information assets (including applications or network credentials), will be reported to DTS.

(56) All users must report any observed or suspected information security events and incidents, such as unauthorised disclosure or access, deletion/destruction of information assets, or any computing device used for work purposes impacted by ransomware to DTS as soon as possible.

(57) The Chief Information and Digital Officer will authorise specified staff whose duties include monitoring the use of ICT facilities or to investigate suspected security breaches or unauthorised access according to the process ratified under the ICT Acceptable Use Policy.

Business Continuity and Resilient

(58) Adequate measures must be in place to mitigate the impact of a disaster and facilitate the resumption of business services in the event of a disruption and to minimise threats to the University's information assets.

(59) A Disaster Recovery Plan (DRP) must be regularly updated and periodically tested to ensure that core ICT services can be restored during a major extended disruption affecting the University's primary processing facility (i.e. Data Centre) or other service providers' facilities.

(60) Availability requirements are agreed for core ICT services and the required controls to ensure those requirements are met are in place.

(61) Business Owners will define for each of their assets (e.g. business applications) their availability requirements and a DRP.

Compliance

(62) Compliance with established policies and applicable legal and regulatory requirements will be proactively monitored and achieved. This includes intellectual property rights, protection of records, personal information, software licenses, privacy and cryptographic controls.

(63) Compliance monitoring activities will be enhanced with independent reviews and automated processes.

(64) Breaches of this Policy will be identified, analysed, evaluated, tracked, managed and reported.

Section 5 - Non-Compliance

(65) Non-compliance with Governance Documents is considered a breach of the Code of Conduct – Staff or the Code of Conduct – Students, as applicable, and is treated seriously by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures outlined in the Charles Darwin University and Union Enterprise Agreement 2025 and the Code of Conduct – Students.

(66) Complaints may be raised in accordance with the Code of Conduct – Staff and Code of Conduct - Students.

(67) All staff members have an individual responsibility to raise any suspicion, allegation or report of fraud or corruption in accordance with the Fraud and Corruption Control Policy and Whistleblower Reporting (Improper Conduct) Procedure.

Status and Details

Status	Current
Effective Date	31st January 2024
Review Date	3rd November 2024
Approval Authority	Vice-President Governance and University Secretary
Approval Date	31st January 2024
Expiry Date	Not Applicable
Responsible Executive	Rick Davies Vice-President Corporate and Chief Financial Officer
Implementation Officer	Andrew Tully Chief Information and Digital Officer
Enquiries Contact	Andrew Tully Chief Information and Digital Officer