Information Technology Policy

Section 1 - Purpose

(1) This policy sets out the requirements for users and the administration of Charles Sturt University's (the University) information and communication technology (ICT) resources.

(2) It is intended to achieve the following objectives:

a. Maintain the security of critical information and digital infrastructure of the University.
b. Establish awareness around correct usage and operation of the University's technology platforms.
c. Raise awareness of and establish requirements for the controls implemented to protect and maintain correct access to University information.
d. State obligations for acceptable use of computing and communications facilities by staff, students and other authorised users.
e. Detail remedies and treatment for breaches and incidents in contravention of acceptable usage or other sources of breach.
f. Meet the University's legislative compliance obligations, including but not limited to those under the Higher Education Standards Framework (Threshold Standards) 2021 (standards 2.1, 3.3 and 7.3) and NSW Cyber Security Policy.

Scope

(3) This policy applies to all authorised users and all University managed ICT resources, as defined in the glossary.

Section 2 - Policy

Part A - Access and use of University ICT resources

Authorities and responsibilities

(4) Delegation Schedule D - Facilities and Information Technology states delegated authorities for approving access to University ICT resources, including:

a. authorities to approve authorised user accounts for staff, students, visitors and external agents, etc
b. authorities to suspend users' access for up to 14 days.

(5) In addition to the delegated authorities, the following authorities and responsibilities for access to ICT systems and resources are given through this policy or as otherwise noted:

Officer or body	Authorities and responsibilities
Chief Information and Digital Officer	Authorise access to CSUNet. Maintain the University's register of non-members provided with CSUNet access. Authorise staff to access personal and/or confidential information when required for the purpose of addressing technical faults. Authorise investigations into breaches of acceptable use of ICT resources.

Application of this part

(6) Access to computing and communications facilities is provided to authorised users for carrying out University work, study and other University-related purposes.

(7) Access to and use of the University's computing and communication facilities is subject to compliance with the Information Technology Procedure - Acceptable Use and Access.

(8) Access to and use of the University's network, CSUNet, will be in accordance with the Information Technology Procedure - CSUNet Access.

Part B - Information security

Authorities and responsibilities

(9) Delegation Schedule D - Facilities and Information Technology states delegated authorities for the security of information systems, including:

a. authority to approve the removal of devices, software and IT services
b. authority to remove offensive, inappropriate or copyright material
c. authority to approve data classifications and standards.

(10) In addition to the delegated authorities, the following authorities and responsibilities for information security are given through this policy or as otherwise noted:

Officer or body	Authorities and responsibilities
Division of Information Technology	Risk management and security of ICT assets managed by the Division of Information Technology. Provision of guidance and advice for risk management and security of all University ICT assets. Ensure appropriate risk assessments are undertaken and mitigation strategies implemented. Provide information security awareness, promotion, education, training and support (including management of information security processes). Implement and operate an Information Security Management System (ISMS). Initiate formal security incident management process. Provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.
Chief Information and Digital Officer	Approve exceptions to the requirements of the Information Technology Procedure - Passwords. Approve alternate authentication mechanisms (other than passwords or personal identification numbers) for applications and systems.
Privacy officer (see the Privacy Management Plan)	Compliance with the Notifiable Data Breaches scheme. Lodge the Notifiable Data Breaches - report a data breach with the Office of the Australian Information Commissioner. Approve information about a University data breach that is to be provided to impacted individuals or other third parties.

Officer or body	Authorities and responsibilities
Director, Security and Resilience (CSO) and/or Chief Information and Digital Officer (or delegate)	Lodge cyber security incident reports for critical infrastructure assets, in accordance with the Security of Critical Infrastructure Act 2018.
System custodians	Work with Division of Information Technology and provide adequate resources to undertake risk assessments and develop and implement risk mitigation strategies and controls. Ensure an information security risk assessment is undertaken for core strategic systems on acquisition or when significant usage or data structure changes occur. Ensure significant security breaches or incidents are reported to IT Service Desk.

Application of this part

(11) The University is a critical education asset under the Security of Critical Infrastructure Act 2018 and subject to mandatory reporting under that Act.

(12) The security of information and digital infrastructure is critical to the University. Information security protects and preserves the confidentiality, integrity, and availability of information. It also protects and preserves the authenticity and reliability of information, ensuring accountability. This policy and supporting procedures ensure information systems are maintained, securely and confidentially as necessary to:

a. prevent unauthorised or fraudulent access to private or sensitive information
b. demonstrate compliance with the Higher Education Standards Framework and other relevant legislation.

(13) The University acknowledges the requirement to manage cyber risk arising from criminal activities, internal threats, and local and foreign interference.

(14) The University will maintain compliance with the core requirements of the NSW Cyber Security Policy including the operation of an information security management system (ISMS) as per the guidelines defined in ISO/IES 2700 Information Security Management System.

(15) To achieve this:

a. information security risk management will be undertaken as per the University's Risk Management Policy
b. risk mitigation strategies will be implemented to ensure appropriate legal, regulatory and contractual compliance to protect information assets against breaches of:
    i. confidentiality
    ii. failures of integrity
    iii. information interruptions.

(16) The University will provide education, training and awareness for information security as appropriate to individual's roles and responsibilities.

(17) The University will report information security breaches or incidents that may involve criminal activity to relevant law enforcement agencies, in line with relevant state and Commonwealth reporting requirements.

(18) The University will implement an ISMS and supporting program of investment to ensure appropriate security standards and measures are established, implemented, monitored, reviewed and improved as required to meet business and compliance objectives are met.

(19) Detailed information security requirements and processes are set out in the:

a. Information Security Guidelines
b. Information Technology Procedure – Passwords
c. Information Technology Procedure – Personal Data Breaches

Part C - New technologies, purchases and disposals

Authorities and responsibilities

(20) Delegation Schedule D - Facilities and Information Technology states the delegated authorities for:

a. approving ICT software and service agreements
b. purchasing ICT infrastructure and devices
c. allocating mobile phones for staff
d. disposal of technology.

(21) Delegation Schedule C - Finance sets out the expenditure delegations relevant to the procurement of ICT.

(22) In addition to the delegations, the following authorities and responsibilities for the introduction of new technologies and the purchase or disposal of ICT resources are given through this policy or as otherwise noted:

Officer or body	Authorities and responsibilities
Chief Information and Digital Officer (or delegate)	All information technology, software and hardware procurement approvals.

Application of this part

(23) All University ICT equipment must be purchased through the Computer Shop, unless an exemption applies, in accordance with the Information Technology Procedure - Purchasing and Disposals.

(24) Information technology procurement, initiatives or projects may require review and assessment by the Project Review Board and/or Technology Governance Committee, in accordance with their terms of reference or as otherwise determined by the Chief Information and Digital Officer.

Section 3 - Procedure

(25) The following procedures support this policy:

a. Information Technology Procedure – Acceptable Use and Access
b. Information Technology Procedure – CSUNet Access
c. Information Technology Procedure – Passwords
d. Information Technology Procedure - Personal Data Breach
e. Information Technology Procedure - Purchasing and Disposal

Section 4 - Guidelines

(26) Information Security Guidelines

Section 5 - Glossary

(27) For the purpose of this policy, the following terms are defined:

a. Authorised user - includes:
    i. staff
    ii. students - persons enrolled in a course or subject
    iii. persons who are affiliated or associated with the University who are granted a temporary access account and provided with authentication credentials. Examples include:
        - research associates
        - community groups
        - vendors and contractors
        - board members
        - visiting fellows
        - eduroam users from other educational institutions.

b. ICT resources - include:
    i. computers and peripherals (e.g. printers)
    ii. communication devices (e.g. mobile devices, desk phones)
    iii. infrastructure (e.g. servers)
    iv. computing facilities and utilities (e.g. conferencing facilities, internet)
    v. information storage media (e.g. USB drives)
    vi. systems and software (e.g. email, eduroam)
    vii. services (e.g. IT Service Desk)
    viii. physical computing facilities (e.g. data centres, communication closets, structured cabling
    ix. vendor or cloud provided hosting/application services utilised by the University.

Status and Details

Status	Current
Effective Date	1st August 2022
Review Date	1st August 2025
Approval Authority	Chief Operating Officer
Approval Date	30th July 2022
Expiry Date	Not Applicable
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Vanessa Salway Manager, Policy and Records
Enquiries Contact	Division of Information Technology