Information and Communications Technology Security Policy

August 2022 – This policy is rescinded and is replaced by the Information Technology Policy (Part B).

Section 1 - Purpose

(1) Computer and information systems underpin the University's activities and are essential to the teaching, learning, research and administration functions of Charles Sturt University (the University).

(2) This policy sets out the University's information security obligations regarding the integrity, confidentiality and availability of all information and communication technology (ICT) infrastructure, systems and processes.

(3) This policy defines in broad terms the framework within which information security risk is to be managed.

(4) The University acknowledges its obligation to ensure the security of all information, infrastructure and processes it owns and controls. Every member of the University shares this obligation to varying degrees.

Scope

(5) This policy applies to all authorised users who own, manage, access or use the University's ICT services.

(6) This policy covers all:

a. ICT systems and data attached to University computer or telephone networks;
b. University systems;
c. communications sent to or from the University; and
d. data owned by the University, either internally or on systems external to the CSU network.

References

(7) This policy should be read in conjunction with:

a. Information Security Guidelines;
b. NSW Cyber Security Policy;
c. Code of Conduct;
d. Compliance Risks Identification Guidelines;
e. Information Technology Procedure - Acceptable Use and Access; and
f. Risk Management Policy.

Section 2 - Glossary

(8) For the purpose of this policy:

a. Authorised users – means all:
    i. continuing and fixed term professional, academic and executive staff;
    ii. visiting and adjunct appointments;
    iii. casual academics;
    iv. casual professional staff;
    v. students;
    vi. visitors, vendors, contractors and associated bodies with authorised access to information systems.
b. Availability - means information assets are accessible to authorised parties at appropriate times.
c. Computer system(s) – means any University system used for the processing of information, either within the University premises, or at an off-site location. This includes private and/or third-party equipment, if such equipment is used to access University information.
d. Confidentiality - means access to information assets is only by authorised parties.
e. Core strategic systems - means ICT information systems essential to the primary business functions of the University.
f. Data Governance Committee - means the committee established under the Technology Governance Committee.
g. ICT security breach - means incident or action that impacts the confidentiality, integrity or availability of the University's information assets.
h. ICT security risk - means a vulnerability with an associated threat that if exploited could impact the operations of the University.
i. Information and communications technology (ICT) - includes:
    i. computers and peripherals (e.g. printers);
    ii. communications infrastructure;
    iii. computing facilities and utilities;
    iv. information storage media; and
    v. systems and software.
j. Information security - encompasses:
    i. ICT security policies;
    ii. organisation of information security;
    iii. ICT asset management;
    iv. information security compliance obligations;
    v. information security components of human resources management;
    vi. ICT communications and operations management;
    vii. Information security components of business continuity management;
    viii. ICT services access control;
    ix. ICT security incident management;
    x. ICT systems acquisition, development and maintenance; and
    xi. ICT asset physical and environmental security.
k. Information Security Management System (ISMS) - refers to the University's ISMS as per ISO/IES 2700 Information Security Management System.
l. Integrity - means the quality and accuracy of information assets.
m. Security risk assessment - means analysis that occurs to test the effectiveness of current University security controls that protect information and ICT assets of the University. This assessment includes a determination of the probability of losses to those assets.
n. Significant risk - means a risk determined to be outside the University's Risk Appetite Statement as determined

in the Risk Management Policy.

o. System custodian - means University executive staff with responsibility and ownership of information or ICT assets as identified and listed in the University's Applications Portfolio, or the Primary Budget Centre Manager responsible for non-listed systems.

p. Technology Governance Committee – has cross-University representation and is chaired by the Chief Financial Officer. Responsible for providing direction, oversight and governance of the Portfolio of Technology Initiatives.

Section 3 - Policy

(9) 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.

(10) In order to achieve compliance with this Policy, information security risk management will be undertaken as per the University's Risk Management Policy.

(11) The University will implement risk mitigation strategies to ensure appropriate legal, regulatory and contractual compliance to protect information assets against breaches of:

a. confidentiality;
b. failures of integrity; and
c. information interruptions.

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

(13) All authorised users must report ICT security incidents, breaches or significant risks to the IT Service Desk.

(14) The University will report information security breaches or incidents that may involve criminal activity to relevant law enforcement agencies.

(15) Failure to comply with this Policy may result in disciplinary action as per the University's misconduct process referred to in the Code of Conduct.

Responsibilities

(16) The Division of Information Technology is responsible for:

a. risk management and security of ICT assets managed by the Division of Information Technology;
b. provision of guidance and advice for risk management and security of all University ICT assets;
c. ensuring appropriate risk assessments are undertaken and mitigation strategies implemented;
d. providing information security awareness, promotion, education, training and support (including management of information security processes);
e. implementing and operating an Information Security Management System (ISMS);
f. initiating a formal security incident management process;
g. reporting significant information breaches that compromise personal data to the University Ombudsman as the University's Privacy Officer;
h. reporting significant security incidents and suspected breaches of this policy to the Office of the Chief Financial Officer;
i. reviewing this policy on an annual basis; and

j. providing clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

(17) The Data Governance Committee is responsible for reviewing and prioritising:

a. data security risks; and
b. risk mitigation strategies.

(18) System custodians are responsible for:

a. working with Division of Information Technology and providing relevant adequate resources to undertake risk assessments and develop and implement risk mitigation strategies and controls;
b. ensuring an information security risk assessment is undertaken for core strategic systems on acquisition or when significant usage or data structure changes occur; and
c. ensuring significant security breaches or incidents are reported to IT Service Desk.

(19) All authorised users are responsible for ensuring:

a. the University's personal computing systems including desktop, mobile and personal devices are used in accordance with the Information Technology Procedure - Acceptable Use and Access;
b. security incidents, breaches or significant risks are reported to the IT Service Desk; and
c. identification and management of risk concerning usage of personal data and reporting of these risks to the IT Service Desk.

Section 4 - Procedures

(20) Nil.

Section 5 - Guidelines

(21) Nil.

Status and Details

Status	Historic
Effective Date	18th July 2019
Review Date	18th July 2022
Approval Authority	Chief Financial Officer
Approval Date	25th June 2019
Expiry Date	1st August 2022
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Timothy Mannes
Enquiries Contact	Division of Information Technology

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to the CSU Policy Library for the latest version.