'Cyber Security Working Group' - Membership and Terms of Reference

This is not a current document. It is no longer in force and the committee has been subsumed by the Technology Committee.

Section 1 - Establishment

Background

(1) The Cyber Security Working Group (CSWG) is a sub-committee of the Technology Governance Committee (TGC).

(2) The CSWG is responsible for the governance of the cyber security activities of the University to provide assurance on the identification and management of the University's cyber risks and vulnerabilities.

(3) The duties of the CSWG shall apply to all matters associated with cyber and information security governance pertaining to the quality of technology, processes and training provided to, and on behalf of, the University.

Purpose

(4) The CSWG shall undertake the duties listed under Section 4, to allow it to ensure quality and governance oversight of the University’s cyber security and risk management activities.

(5) Plan and oversight the implementation of a robust set of business processes and controls to assure the cyber security of the University.

Section 2 - Glossary

(6) For the purpose of this document:

a. CSWG or working group - means Cyber Security Working Group.
b. TGC – means the Technology Governance Committee.

Section 3 - Membership

(7) The membership of the working group is set out below:

a. Director, IT Infrastructure and Security - Division of Information Technology (Presiding officer)
b. Manager, ICT Security - Division of Information Technology
c. Chief Security Officer – Executive Director, Safety, Security and Wellbeing
d. Director, Business Services - Division of Finance
e. Director, Workplace Relations and Partnerships - Division of People and Culture
f. Director, Risk and Compliance, Office of Governance and Corporate Affairs

g. University Ombudsman - Office of Governance and Corporate Affairs
h. Faculty Administration Manager nominated by the Deputy Vice-Chancellor (Academic)
i. A member of the academic body with cyber security expertise.

(8) Right of attendance:

a. Head Enterprise Architect, Enterprise Architecture – Division of Information Technology

Section 4 - Functions and responsibilities

(9) The objective of the CSWG is to oversee the confidentiality, integrity and availability of the University's technology and information assets through the application and governance of appropriate cyber security controls.

(10) The CSWG has the responsibility for making decisions and providing multi-disciplinary input to manage institutional effort required to robustly follow/deliver robust cyber security controls aligned with the ASD Essential 8.

(11) The CSWG will fulfil responsibilities as outlined in the ICT Security Policy and is responsible for reviewing and ratifying:

a. organisational information security risks
b. information and communications technology (ICT) security strategy
c. annual ICT security reports
d. operation of the Information Security Management System (ISMS)
e. ICT security program, and
f. other ICT security risk mitigation strategies.

Working group responsibilities

(12) The working group shall:

a. adopt a risk-based approach to the assessment of University risk and strategic/tactical priorities
b. provide assurance on the identification and management of the University's risks and vulnerabilities
c. provide assurance on the identification and management of the University's compliance obligations, including legislative
d. provide overarching governance of the University's cyber program and IT security, including reviewing, ratifying and proposing inclusions and direction
e. oversee the development of critical incident response plans
f. provide governance of the implementation and operation of the University's ISMS, and
g. guide the development and implementation of information management and ICT security policy, and associated procedures, systems and processes in alignment with the Essential 8 and ISO standards.

(13) Membership across university portfolio areas is required to inform the CSWG of good governance, security, ethics and risk awareness in decisions and advice. Members will be required to provide understanding and insight of University obligations that inform and influence information utilisation and security, for example, legislation, privacy, copyright, state records, research, etc.

Member responsibilities

(14) Members shall:

a. maintain a good understanding of the concepts and purpose of the University's Information Technology Policy, ASD Essential 8 and associated Information Security Guidelines
b. review and approve the ICT security strategy and program
c. promote the adoption of ICT security controls to ensure integrity, availability and confidentiality
d. promote the adoption and upholding of practices within the organisation that enhance best practice and quality through the design, implementation and monitoring of solutions and business processes, and
e. be available to assist in emerging University risk assessment and treatment recommendation, in line with the scope of this working group between regular meetings as required.

Advisory role and referral of matters

(15) The working group shall:

a. provide strategic advice to the TGC on proposals for improvement in the University's information systems and cyber security controls
b. report to the TGC at least annually on reviewed and prioritised cyber security risks and mitigation strategies, and
c. report the operations of the working group and ICT security to the TGC and University executive, including Chief Operating Officer, as required.

Section 5 - Meetings

Quorum

(16) A quorum shall be a majority of the regular members of the working group or their delegates.

(17) A regular member may appoint another person to attend a meeting or meetings on their behalf, or to act on their behalf for a specified timeframe. A person so appointed will be deemed to be a regular member of the working group for the specified time and may vote as a regular member.

(18) The working group will be appropriately represented across the University to enable members to play a key role in educating, communicating and promoting the importance of good ICT security and data asset management. The CSWG will be supported by the Enterprise Architect, Information and Manager, ICT Security from within the Division of Information Technology.

Meetings

(19) At least four meetings will be planned annually. These will normally be one hour in duration.

Agendas and minutes

(20) Agendas and minutes of the previous meeting will be distributed within one week prior to a scheduled CSWG meeting.

Conflicts of interest

(21) Where a member has a perceived or material conflict of interest, they must declare this to the presiding officer and at the working group meeting prior to discussion of the item of business.

Variations

(22) Variations to the terms of reference and/or membership of the working group must be approved in accordance

with Delegation Schedule A - Governance and Legal.

Status and Details

Status	Historic
Effective Date	6th April 2022
Review Date	6th April 2025
Approval Authority	Chief Operating Officer
Approval Date	5th April 2022
Expiry Date	4th May 2023
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Mark Duffy Executive Director, Division of Information Technology
Enquiries Contact	Office of Governance and Corporate Administration +61 2 63384207