Cyber Security Policy

Last Modified | Nōnahea i Whakarerekē	August 2024
Review Date | Rā Arotake	August 2025
Approval Authority | Mana Whakaae	Vice-Chancellor
Contact Officer | Āpiha Whakapā	Director of Digital Security and Risk

Introduction | Kupu Whakataki

This Policy establishes the University's and Users' cyber security risk management responsibilities, which are based on the principle that cyber security is every User's responsibility.

Scope

This Policy applies to all University Staff, students and Users of the University's Information Systems irrespective of location or device ownership, including Users with personally owned devices.

Policy Statement | Kaupapa Here

1. Principles

1.1. Effective management of cyber security helps protect the University from cyber threats that try to take advantage of opportunities in technology, people and/or processes to harm or misuse systems and assets owned or managed by the University.

1.2. The University manages Cyber Risk to safeguard and secure the Confidentiality, Integrity and Availability of its technology, applications and Information Systems and by facilitating a positive culture of cyber security awareness.

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

1.3. The management and awareness of Cyber Risk is the responsibility of both the University and Users, and it requires a combined effort across all University operations.

1.4. The University encourages the prompt reporting of cyber incidents and near misses. Mistakes happen, and our focus is on learning and improving our defences.

1.5. The University's Cyber Security Strategy and risk management responsibilities support the University Risk Management Framework and utilise threat aligned and risk-informed decision making to manage Cyber Risks. Cyber Security Controls are designed to:

- Support the University's education, research and engagement activities;
- Facilitate individual Users' cyber security awareness to enable accountability and trust;
- Be proportionate to the Information Value of the system, application and/or Information Systems;
- Support compliance with the University's legal obligations, including in relation to information protection and privacy and security of trusted research;
- Uphold Confidentiality, Integrity and Availability of Information Systems;
- Allow for protective plans and actions to detect, prevent and respond to Cyber Security Incidents and/or cyber security threats.

2. Key Requirements

Cyber Security Framework

2.1. The University leverages the Cyber Security Framework to establish rules and responsibilities required to maintain an appropriate level of cyber security to protect University Information Systems.

2.2. The Cyber Security Framework is supported by the following four pillars;

- **Cyber Security Strategy:** provides an effective, adaptable and risk-based approach to the management of cyber security to support the University in its mission.
- **Cyber Security Management**: ensures the monitoring and management of Cyber Security Risk and resilience of technology across the University's footprint.
- **Cyber Security Controls:** implement a multilayered cyber security (defence-in-depth) approach to information and Cyber Security Controls to protect infrastructure and information.
- **Cyber Security Certification:** the maintenance of a suite of cyber security industry-recognised certifications and compliance memberships to implement best practice cyber security management processes and controls.

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

2.3. The University maintains information technology and Standards (UC Only) to facilitate the effective implementation of Cyber Security Controls and management across all Information Systems.

2.4. Standards are developed in consultation with key University stakeholders to support business requirements, provide adequate Cyber Risk mitigation, and align with the cyber security framework.

2.5. The University continuously improves cyber security**,** recognising it as an ongoing process vital for protecting against evolving Cyber Risks and threats, thereby ensuring trust and confidence in the University's Information Systems.

Cyber Risk Management

2.6. The University identifies Cyber Risk via a range of monitoring methods and addresses Cyber Risk with a range of controls.

2.7. The Digital Security and Risk Team will maintain a register of key Information Systems and Cyber Risks, including the related controls.

- These registers must be reviewed annually at a minimum and also following any significant Cyber Security Incident or threat or change to organisational requirements.
- Top Cyber Risks must be reviewed at a minimum every quarter.

2.8. University Staff must assess the cyber security and privacy risks associated with all new activities that use the University's Information Systems and when there is a change to existing activities. These risks must be assessed, and associated mitigations must be incorporated as part of the planning stages for these activities.

2.9. Staff should ensure that the Digital Security & Risk Team is consulted on all proposed contracts relating to the University's Information Systems between the University and a vendor or third party to ensure that the system meets the University's Cyber Security Controls and Standards.

- Staff must also ensure that they have the contractual delegated authority to enter into a contract relating to the University's Information Systems (see "information technology products and services" in the Contracts Delegation Schedule).

- All contracts must clearly outline the vendor or third party's security responsibilities for storing or processing the University's information and the protection of the University's information. Contracts must include at a minimum:

    - Adequate consideration of cyber security based on risk;
    - Assurance to the University about the external system's cyber risk management activities; and

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

- Mandatory reporting to the University of any actual or suspected breach(es) impacting or potentially impacting the information held in the University's Information Systems, to be made as soon as possible after detection.

3. Information and Technology Management

3.1. The University will protect the information and assets that it holds and will have controls in place to maintain its Confidentiality, Integrity and Availability.

3.2. The security classification of Information Systems are managed according to the impact the University would incur in the event of an incident affecting any, or all, Security Attributes of the Information System.

3.3. To ensure continuity of essential system functions in the event of a Cyber Security Incident, all Faculties, schools, departments and service units who manage Information Systems that form part of a Core Service must include the following in their Business Continuity Plan:

- Identification of systems that provide Core Services;
- Strategies for backup and recovery of information to restore system operations quickly and effectively; and
- Details of how to lead system recovery and reconstitute the system after a Cyber Security Incident.

4. Security Awareness

4.1. The University promotes a positive security culture to improve its overall cyber security through education and training.

4.2. Staff are expected to undertake cyber security awareness education and training from time to time. All new staff and students must undergo relevant training as part of onboarding to the University.

4.3. Students should refer to the Cyber Safety Awareness website to facilitate the safe use of the University's Information Systems.

4.4. The University performs security testing against systems, processes and people to determine its vulnerability to cyber threats. The results of these test will be used to measure and improve the management of the University's Cyber Risks and controls to prevent cyber threats.

5. Incident Management

5.1. All Users must immediately report known or suspected Security Incidents here.

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

5.2. In the event of a Cyber Security Incident, the University will follow the UC cyber incident response plan (UC Only) to manage and comply with applicable legal and insurance requirements, to minimise harm to impacted individuals and to minimise damage, business disruption, and risk to the University.

5.3. In cases where University Information Systems and/or University information are threatened, the Digital Risk and Security Team will act to secure the resource and may limit or disconnect access.

6. Exception Management

6.1. Exceptions to the cyber security Standards may be temporarily granted by the Director of Digital Security and Risk. However, because exceptions can inherently weaken the security of University Information Systems and University information, exceptions will not be granted for convenience or when appropriate alternative security controls cannot be found to mitigate the risks posed.

6.2. Requests for exceptions to this Policy will be considered and determined by the Vice-Chancellor in consultation with the Director of Digital Security and Risk.

6.3. An exceptions register will be kept by the Digital Security and Risk Team and will be reviewed and reported to the University's Risk Advisory Committee every quarter.

7. Roles and Responsibilities

7.1. The **Director of Digital Security and Risk** is responsible for maintaining oversight of the **overall University's** Cyber Risks and ensuring active management.

7.2. The **Chief Digital Officer** is responsible for maintaining oversight of Cyber Risk and ensuring active management of the University Information Systems managed by Digital Services.

7.3. The **Executive Dean** is accountable for Cyber Risk, where faculties manage specific University Information Systems that Digital Services do not manage**.** The **Head of School** is responsible for maintaining oversight of the respective school's Cyber Risk and ensuring active management, monitoring and reporting to the Executive Dean and Director of Digital Security and Risk.

7.4. The respective **Senior Leadership Team member** is accountable for Cyber Risk, where Service Units manage specific University Information Systems that Digital Services do not manage**.** The **Senior Leadership Team member** is responsible for maintaining oversight and ensuring active management, monitoring and reporting to the Director of Digital Security and Risk.

7.5. Where **Associated Entities** manage their own Information Systems, and those Information Systems utilise the University's network or connect to a University Information System, responsibility for maintaining oversight and active management of Cyber Risk lies with the **Chief Executive Officer** or equivalent of that entity.

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

7.6. An annual assessment of Cyber Security Controls must be undertaken in relation to all University Information Systems. The Digital Security and Risk Team will coordinate the annual assessment. Where requested by the Digital Security and Risk Team, the relevant faculties, schools, departments, institutes and service units will provide assistance during the annual assessment process.

7.7. Staff members within all faculties, schools, departments, institutes and service units are required to report any significant cybersecurity incidents as soon as they arise.

7.8. Associated Entities, vendors, or any other third parties, must conduct an annual self-assessment of cybersecurity controls in relation to any Information Systems which are not University Information systems managed and are controlled by third parties outside of the University. Within 20 working days of the annual self-assessment, a written report must be provided to Director of Digital Security and Risk detailing the outcomes of the assessment.

.

7.9. The Director of Digital Security and Risk is responsible for overseeing the implementation of Cyber Security Controls, the management of cyber security incident response and the development and maintenance of the University's Cyber Security Strategy.

The Director of Digital Security and Risk will provide regular Cyber Security Metrics and reports to the University's Risk Advisory Committee, Senior Leadership Team, Audit and Risk Committee and University Council, as requested.

7.10. Senior Leaders and Heads/Managers are responsible for ensuring that all Staff comply with this Policy and for facilitating the assessment of Cyber Risks and the implementation of Cyber Security Controls as directed by the Digital Security and Risk Team.

7.11. All Users are responsible for complying with all cyber security policies, controls, Standards, procedures and guidelines.

8. Breach of Policy

8.1. Users must report any potential or actual breaches of this Policy to the following email address: ciso@canterbury.ac.nz

8.2. Failure to comply with this Policy may equate to misconduct or serious misconduct, depending on the circumstances.

8.3. Non-compliance by staff may be dealt with in accordance with the Employee Disciplinary Policy (if the breach involves a University employee) or as deemed appropriate by the University.

8.4. Non-compliance by students may be dealt with in accordance with the Behavioural Misconduct Regulations or as deemed appropriate by the University.

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

8.5. Non-compliance by Associated Entities or other third parties (including individuals who have access to University Information Systems but are not employees) may result in termination of contract and removal of access to University Information Systems.

Definitions | Tautuhinga

Associated Entity – An organisation or company that is connected to the University and may have access to the University's Information System.

Availability – Ensuring that authorised parties can access the relevant information when needed.

Confidentiality – Ensuring that information is not made available or disclosed to unauthorised individuals, entities or processes.

Core Service – Means the Information System must be available to conduct the most basic core business activities of the University. Interruptions have an immediate, University-wide impact.

Cyber Risk(s) – The potential of loss or harm related to technical infrastructure, the use of technology or Information Systems. Examples include but are not limited to:

- Phishing scam emails: Phishing is a way that cybercriminals steal confidential information, such as online banking logins, credit card details, organisation login credentials or passwords/passphrases, by sending fraudulent messages (sometimes called 'lures').

- Malware (short for malicious software) is software that cybercriminals use to harm your computer system or network. Cyber criminals can use malware to gain access to your computer without you knowing, in targeted or broad-based attacks.

- Ransomware is a type of malicious software (malware). When it gets into your device, it makes your computer or its files unusable. Cybercriminals use ransomware to deny you access to your files or devices. They then demand you pay them to get back your access.

- A distributed denial of service attack is an attempt to make an online service unavailable by overwhelming it with traffic.

Cyber Security Controls – These seek to reduce cyber security risk by either reducing the likelihood or impact of an incident, or both. These can include cyber security standards, procedures, processes and guidelines.

Cyber Security Framework - The University has selected the National Institute of Standards and Technology Cyber Security Framework (NIST-CSF) to provide structure and context for the security controls deployed across the organisation. The definition of controls

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

is based on ISO27001 and where needed, NIST 800-53 and the New Zealand Protective Security Requirements.

Cyber Security Incident – An event that results in a breach of an explicit or implied digital security policy that requires corrective action as it threatens the confidentiality, availability and/or integrity of an information system or the information that the system processes, stores or transmits.

Cyber Security Metrics – Metrics include but are not limited to the current risk level, security control effectiveness and maturity of the University's approach to cyber security against best practice frameworks.

Information Value – The value given to an Information System consistent with the financial and reputational impact that would be felt should any threats be realised.

Integrity – The maintaining of consistency, accuracy and trustworthiness of information over its entire life cycle.

Information System(s) – Information Systems include information resources, processes and technologies, used in storing, processing or handling information, including but not limited to:

- Hardware: The material physical components of a system
- Software: Computer programs and associated data that may be dynamically written or modified during execution.
- Networks: the interconnected infrastructure that allows communication and data exchange among users, devices, and services
- Cloud services: infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet.
- Devices

Risk Assessment – The overall process of identifying, analysing and evaluating risks. It may also be referred to as a risk analysis or risk evaluation or risk profile and may involve a qualitative and/or quantitative assessment.

Security Attributes – The three principles of confidentiality, integrity and availability used within organisations to support the prevention of unauthorised access, use, disclosure, modification or destruction of Information Systems.

University - This means Te Whare Wānanga o Waitaha | University of Canterbury.

University Information System(s) - Any Information System which is managed and controlled by the University. For clarity, this includes Information Systems which are managed and controlled by specific faculties, schools, departments, institutes or service areas but excludes Information Systems managed and controlled by third parties outside of the University.

Staff or Staff Member - an individual employed by the University on a continuing or fixed term full or part time basis and includes volunteers.

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

Standard(s) – Guidance to support policies and can be based on external guidance or industry standards and generally define minimum or baseline levels.

User(s) – All persons who (or processing systems that) are authorised to access or use the University's Information Systems.

Related Documents and Information | He kōrero anō

Legislation | Whakaturetanga

- Crimes Act 1961
- Education and Training Act 2020
- Harmful Digital Communications Act 2015
- Privacy Act 2020

UC Regulations | Ngā Waeture

UC Policy Library | Te Pātaka Kaupapa Here

- Business Continuity Management Framework (PDF, 426KB)
- Information Records and Data Policy (PDF 286 KB)
- Intellectual Property Policy (PDF, 538KB)
- IT Policy Framework (PDF, 285KB)
- Privacy Policy (PDF, 157 KB)
- Risk Management Framework (PDF, 1MB)
- Staff Code of Conduct (PDF, 481KB)
- Student Code of Conduct (PDF, 303KB)

UC Website and Intranet | Te Pae Tukutuku me te Ipurangiroto o UC

- Cyber security Strategy
- Te Whare Wānanga o Waitaha, University of Canterbury Strategic Vision 2020 to 2030

External | Mōwaho

- NIST Cyber security Framework
- NIST 800-53
- Protective Security Requirements
- Trusted Research – Guidance for Institutions and Researchers

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence

Document History and Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
1.00	Policy creation	Vice-Chancellor	2 Aug 2024
1.01	Hyperlinks updated	Policy Unit	3 Oct 2024

© This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.

Classification: In-Confidence