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. 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:

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;

- Mandatory reporting to the University of any actual or suspected breach(es) impacting or potentially impacting the information held in the 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;

7.6. An annual assessment of C

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

Related Documents and Information |

Legislation | Whakaturetanga

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

UC Regulations |

UC Policy Library |

- 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

External |

- NIST Cyber security Framework
- NIST 800-53