Cyber Security Policy and Procedure

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	Cyber Security Policy and Procedure
Document Title	Cyber Security Policy and Procedure
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	20/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver

Supplemental Policies or Procedures to this Policy

- Cyber Security Policy – Supplemental Policy
- Information Technology Acceptable Use Policy
- Information Security Data Classification and Handling Manual

Cyber Security Policy and Procedure

1. Purpose

The purpose of this policy and procedure is to establish the Company's cyber security risk management framework to prevent, reduce and manage compromised information security.

The company's approach to cyber security is informed by the Victorian Government Protective Data Security Framework and Standards (VPDSF) being the overall scheme for managing protective data security risks, and the Australian Government Information Security Manual.

2. Scope

This policy and procedure apply to all staff, students, third parties (partners, contractors, consultants, etc.) and visitors regardless of location or device ownership and includes any person or entity with authorized use of the company's IT systems, internet and/or email.

3. Definitions

Terms	Definition
control	Is a measure put in place to manage, minimize or eliminate risk.
Cyber security	the methods (policies, strategies, behaviors, and techniques) through which necessary and commensurate measures can be identified, implemented, and maintained to effect information security.
IT and Infrastructure	Is responsible for IT systems at the Company. Noting that in addition to hosting IT systems at the Company some facilities may be hosted externally.
IT systems	All services including data, voice, video, delivered through electronic means. Such technologies encompass systems, software, hardware, communications, and network facilities.

4. Policy

The Company is committed to delivering information security by preventing unauthorised access to, and modification or impairment of, its digital IT systems and the information stored within them; through a combination of preventative measures, cyber security incident management, and the participation of all authorised users in ensuring that security measures are not undermined.

The following Company Cyber Security Strategy is adopted to proactively improve cyber resilience:

- Application whitelisting - Whitelist approved and trusted programs to prevent the execution of unapproved or malicious programs from executing.
- Patching applications - Perform regular patching/updating of applications in your network.
- Office macros - Configure Microsoft Office products to block the execution of un-trusted macros.
- Harden user applications - Tightly control applications that can perform unwanted or potentially vulnerable actions.
- Restrict administrative privileges - Restrict administrative privilege for operating systems and applications based on user duties.
- Patch operating systems – Routinely patch and upgrade your operating systems to the latest versions.
- Use multi-factor authentication - Set up multi-factor authentication to provide higher authentication assurance for privileged, power, and remote user access.
- Backup daily – Create regular backups of your most important data and configuration settings to help you recover quickly from a disruption.

Preventative measures are in place to provide control around the Company's IT systems, including but not limited to:

- Firewall hardware and software to log and protect internet and network usage, including connectivity of all authorised users and IT systems, to prevent known threats and vulnerabilities from being exploited.
- Blocking of certain websites URLs, as their content is considered unsafe, unacceptable, or would put people, IT systems, or the Company at risk. This includes, but is not limited to, malicious, gambling, pornographic, or terrorist content.
- Blocking of certain applications or limiting internet traffic to certain high bandwidth streaming applications to prevent an unnecessary drain on Company IT systems.
- Using antivirus software to ensure the confidentiality, integrity, and availability of its IT systems and detect any malware or similar malicious code. Where possible, its source is traced.
- Automated Spam and Phishing detection to detect spam, phishing messages, and other malicious email entering and leaving Company email servers, to protect against Spam, Phishing attempts, and viral outbreaks.
- Password strength requiring a certain level of complexity in all users' passwords.
- Identification and management of technical vulnerabilities
- Cryptography via digital certificates using a bona fide and valid Certificate Authority *(ISO 27002)*
- Awareness information and training.
- Monitoring of logs to detect signs of external interference.

Security controls at the Company are based on a cloud security plan that:

- Ensure access to appropriately skilled resources to secure the service. This may involve training in-house staff or procuring specialist support.
- Incorporate appropriate Identity and Access Management based on roles, especially for administration duties.
- Ensure secure communications between users and the service.

- Establish a security control regime using third-party tools (Cloud Access Security Broker) to achieve better visibility, data security, threat protection and compliance, as well as to automate security configurations where possible.
- Take full accountability for application and data security in production, staging, development and test (non-production) environments and ensure roles and responsibilities are clear.
- Standardise all cloud deployments on 'hardened' images.
- Ensure that contracts support the ability to revert from the cloud. Clarify data sovereignty and the location of online and offline backups.
- Ensure mechanisms are in place for the service provider to notify the Company of cyber incidents and data breaches.
- Ensure regular independent security auditing of the service. This may be achieved under existing certification and accreditations such as ASE-3402 or PCI DSS certification.

5. Procedure

The Company's Cyber Security Strategy and preventative measures will mitigate risk and help protect critical information against cyber threats through compliance with this policy and procedure, and its local operating procedures, standards, guidelines, and systems. This includes technical cyber security controls and a cyber security awareness program to reduce vulnerability of staff to cyber security threats by fostering a culture that encourages cyber security.

Risk management will centre around cyber security controls that seek to reduce the likelihood or impact of an incident, or both. Cyber security risk management will be measured by:

- Maintaining a register of key information assets.
- Establishing a framework for performing cyber security risk assessments.
- Incorporating cyber security risk identification and assessment into processes impacting the use and processing of information.
- Maintaining a register of cyber security risks with related controls.
- Reviewing risks at regular intervals and due to significant security incidents, threats, or changes to business requirements.
- Implementing and strengthening controls to reduce risk.
- Evaluating the effectiveness of controls.

A cyber security incident is an event involving an actual or potential malicious actor that threatens the confidentiality, integrity, or availability of Company information assets (electronic or paper) or otherwise contravenes this policy. The source of a cyber security incident may be accidental, malicious, or significant exposure to a known threat.

The Global Head of Enterprise Technology, Risk and Cyber Security will manage cyber security incidents by applying quick, effective, and orderly responses that aim to comply with applicable legal requirements (see the Notifiable Data Breaches Policy and Procedure), minimise harm to impacted individuals, and minimise damage and risk. Management of incidents includes communication and collection and analysis of evidence from the incident. All incidents must be reported to the Senior Leadership Team and to the Compliance and Risk Management Committee.

Controls and other preventative measures are put in place to avoid cyber security incidents, either because of experience from previous incidents or as a countermeasure or deterrent to likely

incidents. These measures are documented and regularly reviewed to ensure their validity and reliability.

Cyber security vulnerability testing will be performed against systems, processes, and people to determine the Company's vulnerability to cyber threats. The results will measure and improve service quality and protection against cyber threats.

6. Responsibilities

Users

Staff are responsible for reporting potential cyber security incidents to IT and Infrastructure support, including those of an accidental nature such as a lost laptop or device.

Staff and contractors are responsible for:

- Participating in cyber security training where relevant to their work role; and
- Acting consistently and responsibly to protect the Company's information assets by –
    - Complying with procedures in place to protect information assets.
    - Incorporating safe cyber security practices into their work; and
    - Reporting risks to IT and Infrastructure.

IT and Infrastructure

The Global Head of Enterprise Technology, Risk and Cyber Security will assess the ongoing maturity of the Company's cyber security practices and review this policy in response to significant cyber security incidents and changes in cyber security strategy and applicable legislation.

The Global Head of Enterprise Technology, Risk and Cyber Security is accountable for the maintenance of cyber security metrics for reporting to the Compliance and Risk Management Committee on a half-yearly basis.

The metrics will cover the following cyber security management:

- current risk level.
- control effectiveness.
- the Company record of cyber security against best practice.

The IT and Infrastructure Team will drive compliance with this policy and procedure through:

- ongoing cyber security awareness activities.
- checks in key IT processes to ensure cyber security risk management activities are performed.
- technical enforcement.
- regular reporting of self-assessments by Company business units and departments on required cyber security controls implemented to protect information assets; and
- audits to assess compliance and effectiveness of technical controls.

IT and Infrastructure Team manage relevant cyber security risks and are accountable for compliance with relevant cyber security standards and operating procedures including:

- Assisting to identify and develop suitable cyber security frameworks, standards, and local operating procedures.
- Monitoring IT systems and services for potential cyber security risks and threats.
- Reviewing the effectiveness of cyber security controls.

Audit (internal and/or external) will provide independent oversight, review, and assurance on the effectiveness of cyber security controls to manage risk and meet compliance requirements.

7. Other Relevant Policies

- Acceptable Use Policy
- Notifiable Data Breach Policy