



Cyber Security Policy

1.0 Overview

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, **ANDREW YULE & COMPANY LIMITED** has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

2.0 Purpose

The purpose of this policy is to

- (a) protect **ANDREW YULE & COMPANY LIMITED**, data and infrastructure,
- (b) outline the protocols and guidelines that govern cyber security measures,
- (c) define the rules for company and personal use, and
- (d) list the company's disciplinary process for policy violations.

3.0 SCOPE

This policy applies to all of **ANDREW YULE & COMPANY LIMITED** employees, remote workers, permanent, and part-time employees, contractors, suppliers, trainees and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

4.0 POLICY

ANDREW YULE & COMPANY LIMITED has outlined security measures that may help mitigate cyber security risks.

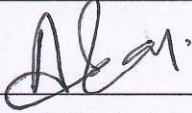


(a) Confidential Data

ANDREW YULE & COMPANY LIMITED defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

(b) Data security

It is the responsibility of all employees of AYCL.

Prepared & Issued By	Reviewed By	Approved By	Pages
			
Document Controller	CISO	Dy. General Manager (P&A)	2 of 6
Issue No./Date: 01/10.09.2021 Rev. No./Date : 00/10.09.2021 Document No. AYCL-ISMS-CSP-01-00)			



Cyber Security Policy




(c) Device Security:

To ensure the security of all company-issued devices and information, **ANDREW YULE & COMPANY LIMITED**, employees are required to:

- Keep all company-issued devices password-protected. This includes Laptops, desktops, and mobile devices.
- Secure all relevant devices before leaving their desk.
- Obtain authorization from the IT System Head and/or Asset Manager before removing devices from company premises.
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.
- Don't install any software on company issued computers without prior approval from IT Dept.
- Only open websites that you know.
- Never randomly click a link as it may direct you to a malicious website or trick you to download an infected file or program.
- When using USB flash drives, thumb drives or any other removable drives, make sure you scan them using your security software. Best practice is to ask IT dept. to scan if you're not too sure.
- Report any suspicious computer activity to IT Dept. right away.
- Educate yourself on the protection systems that are installed on your computer and to check if it is up to date or any alerts.
- Never leave your computer unattended.
- As a best practice always lock your computer session before leaving your computer unattended.
- Follow Clean and clear desk policy,

ANDREW YULE & COMPANY LIMITED recognizes that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.

Prepared & Issued By	Reviewed By	Approved By	Pages
			
Document Controller	CISO	Dy. General Manager (P&A)	3 of 6
Issue No./Date: 01/10.09.2021 Rev. No./Date : 00/10.09.2021 Document No. AYCL-ISMS-CSP-01-00)			



Cyber Security Policy

- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

(d) Email / Internet Security.

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, **ANDREW YULE & COMPANY LIMITED** requires all employees to:



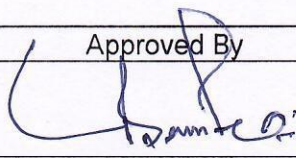
- Verify the legitimacy of each email, including the email address and sender name.
- Do not open emails from unknown senders.
- Avoid opening suspicious emails, internet sites, attachments, and clicking on links on Internet.
- Look for any significant grammatical errors.
- Avoid click bait titles and links.
- Contact the IT department regarding any suspicious emails.

Employees must follow laid down Information Security Protocols by AYCL. This is vital as ignoring these protocols can introduce security risk to company and personal data.

(e) Transferring Data.

Andrew Yule & Co. Ltd recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over **ANDREW YULE & COMPANY LIMITED** networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to **ANDREW YULE & COMPANY LIMITED** data protection law and confidentiality agreement.
- Immediately alert the IT department regarding any breaches, malicious software, and/or scams.

Prepared & Issued By	Reviewed By	Approved By	Pages
			
Document Controller	CISO	Dy. General Manager (P&A)	4 of 6
Issue No./Date: 01/10.09.2021 Rev. No./Date : 00/10.09.2021 Document No. AYCL-ISMS-CSP-01-00)			



Cyber Security Policy

5.0 Policy Governance

The following table identifies who within **ANDREW YULE & COMPANY LIMITED** is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.




Responsible	Dy. General Manager (P&A)
Accountable	CISO
Consulted	Process Owners
Informed	Employees of ANDREW YULE & COMPANY LIMITED

Dy. General Manager (P&A) of **ANDREW YULE & COMPANY LIMITED** is responsible for ensuring that all staff and managers are aware of security policies and that they are observed.

CISO need to be aware and have a responsibility to ensure staff has sufficient, relevant knowledge concerning the security of information and systems.

Designated Process owners and owners of systems, who have responsibility for the management of **ANDREW YULE & COMPANY LIMITED** systems and inherent information, need to ensure that staff have been made aware of their responsibilities toward security.

Designated owners of systems and information need to ensure they uphold the security policies and procedures.

Prepared & Issued By	Reviewed By	Approved By	Pages
			
Document Controller	CISO	Dy. General Manager (P&A)	5 of 6
Issue No./Date: 01/10.09.2021 Rev. No./Date : 00/10.09.2021 Document No. AYCL-ISMS-CSP-01-00)			



Cyber Security Policy

6.0 Responsibility

Dy. General Manager (P&A)	Approves the Policy document.
CISO	CISO and Project Manager's are responsible for implementing and monitoring this policy.
Internal Security Audit Team	Responsible for reporting findings based on observations related to the implementation of the policy
Employees of ANDREW YULE & COMPANY LIMITED	All employees of ANDREW YULE & COMPANY LIMITED shall be guided by the information category in their security related handling of company's information and are required to follow the policy. The employees dealing with Third Party entities are required to instruct Third Party persons to follow the policy while working in ANDREW YULE & COMPANY LIMITED premises.

7.0 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to **ANDREW YULE & COMPANY LIMITED** assets, or an event which is in breach of the **ANDREW YULE & COMPANY LIMITED** security procedures and policies.

The **ANDREW YULE & COMPANY LIMITED** will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place.

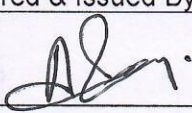

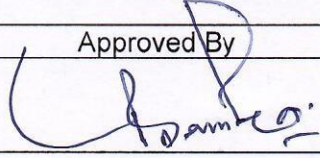
If any user is found to have breached this policy, they may be subject to **ANDREW YULE & COMPANY LIMITED** disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

All employees have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Company's Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access the Information Systems of the **ANDREW YULE & COMPANY LIMITED**.

8.0 Review and Revision

This policy will be reviewed as and when required or at least once in a year.

Policy review will be undertaken jointly by **CISO** and **Dy. General Manager (P&A)** of **ANDREW YULE & COMPANY LIMITED**.

Prepared & Issued By	Reviewed By	Approved By	Pages
			
Document Controller	CISO	Dy. General Manager (P&A)	6 of 6
Issue No./Date: 01/10.09.2021 Rev. No./Date : 00/10.09.2021 Document No. AYCL-ISMS-CSP-01-00)			