POLICY – TEMPLATE

Acceptable Use Policy

Document Control

Version Control

Date	Version	Details	Author

Approval

Delegation required for approval: XXXX

Name: XXXX Position: XXXX

Signature: Date: XXXXX

N.B. ASSOCIATIONS SHOULD USE THIS TEMPLATE AS GUIDANCE TO SHAPE THE POLICY, WHICH IS MEANINGFUL AND FIT FOR PURPOSE, FOR THEM.

THIS IS NOT INTENDED TO BE A ONE SIZE FITS ALL TEMPLATE.

Definitions

Term	Definition
Personnel	Employees, including players, Board, committee members and administrators including officers, team support staff and coaches engaged by XXX as independent contractors and volunteers
Information Assets	A body of information defined and managed by XXX so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles. I.e., cloud service customer data, software, information, physical assets.
Personal Use	Using XXXX equipment, systems or IT Infrastructure to use for personal business/administration.

1. Purpose and Background

Information security is fundamental to XXXX. As an advocate for robust security and risk management, as well as a custodian of valuable Information Assets, the secure management of Information Assets is essential to maintain legal and regulatory compliance, commercial reputation, and competitive advantage.

This includes protecting XXXX Assets from a breach of confidentiality, integrity, or availability by implementing a range of people, process, and technical controls.

2. Policy Statement

POLICY – TEMPLATE

Acceptable Use Policy

The Acceptable Use Policy defines acceptable use behaviour, rules and guidance for Users utilising XXXX Information Assets and Information Systems.

This Policy is in place to protect personnel, partners, customers, and the organisation, as inappropriate use exposes XXXX to risks including data loss, virus attacks, compromise of systems and services, and legal issues.

3. Scope and Applicability

This Policy applies to all forms of Information Assets and Information Systems that are either owned, managed, or supported by XXXX.

This Policy applies to all XXXX personnel, contractors, consultants, partners, third parties and vendors (Users) who have access to XXXX Information Assets and Information Systems within or outside company premises.

A summary of responsibilities associated with this Policy and the acceptable use of XXXX Information Assets and Information Systems is provided in Table 1 below.

Table 1. Summary of Responsibilities

Role	Responsibilities
XXXX Board of Directors	• Make policies which are necessary or desirable for the control, administration, management and protection of XXXX affairs; and • May amend, repeal and replace those policies
President	• Provides authority to authorised staff members to monitor and audit the use of Information Assets and Systems. • Monitors and reports on User compliance with this Policy
All XXXX personnel	• Ensures acceptable and efficient use of Information Assets and Systems • Reports security incidents and any identified weaknesses as soon as practicable

Approval and Acknowledgment

- Users will acknowledge this Policy to only use Information Assets and Information Systems for official XXXX business approved training, and limited personal use.
- Users acknowledge that the access to, and the use of, Information Assets and Information Systems will be monitored and/or recorded for lawful purposes.

4. Policy

4.1 Acceptable Use

- Users will take all reasonable care when downloading, accessing, or executing files, accessing websites or links from the internet and by other means (e.g., email, text message, social media, web browsing)
- Users will protect Information Assets and Information Systems from unauthorised access by adhering to information classification and handling requirements (Confidential, Restricted, Public).

- Users will store XXXX Information Assets on XXXX approved storage commensurate with the information security classification.
- Users viewing confidential information must ensure that it cannot be viewed or copied by unauthorised persons.
- Users are responsible for the proper and safe keeping of Information Systems assigned to them.
- All Information Assets and Information Systems must be returned promptly after its intended use is over or the employment contract has been terminated.
- Users must immediately notify the XXXX if they suspect their account credentials have been compromised in any way.
- Users acknowledge that the data they create on XXXX Information Systems remain the property of XXXX. XXXX cannot guarantee the confidentiality of User's personal information stored on any Information System belonging to XXXX.
- Users must always protect the intellectual property rights of XXXX, by classifying the information appropriately.
- Users must comply with the XXXX Privacy Policy.

4.2 Account Credentials

XXXX utilises a combination of account credentials (e.g., passwords and passphrases) and multi-factor authentication to protect Information Asset access. The following requirements are applicable to the use of all User account credentials:

- Users will protect their account credentials by not sharing them with any other person (including colleagues or family), or storing them in insecure methods (e.g., handwritten notes, excel spreadsheets)
- All account credentials and multi-factor tokens are to be treated as Confidential Information Assets
- Account credentials must not be inserted into email messages, ticket management or other forms of electronic communication.
- Do not use the "Remember Password" feature of applications (for example, web browsers)

Any User suspecting that their account credentials may have been compromised must report the incident as per Reporting Incidents below and change those impacted account credentials.

4.3 Unacceptable Use

When using XXXX Information Assets and Information Systems, User's should not:

- Connect devices to unencrypted or public networks (e.g., free Wi-Fi in airports or planes, coffee shops, libraries, etc.), unless business critical and use best endeavours to reduce any risks.
- Email, publish, or reveal to others in any format XXXX account credentials.
- Distribute non-public XXXX information to the internet or other unauthorised external locations.
- Wilfully waste Information Assets and Information Systems, including downloading large files (e.g., movies, games), operating personal online businesses or sending emails in bulk (e.g., spam)
- Violate the intellectual property rights of others.
- Copy copyrighted material or install any copyrighted software for which XXXX or the User do not have an active license.
- Knowingly introduce malware onto any network, server, or host
- Transmit payment card information such as credit card numbers, debit card numbers and associated expiration dates via email or any other insecure method.

- Perform any form of harassment via email, telephone, or any other XXXX technology platform (chat services, etc.) whether through language, frequency, content, or size of messages.
- Trafficking in confidential customer or client information
- Deliberately damage Information Assets and Information Systems
- Unless authorised:
    - Attempt to subvert any security measures, including storage or use of tools on Information Systems
    - Execute any form of network monitoring which may intercept data not intended for that User.
    - Post publicly on websites, blogs, and social media from a XXXX email address, or purport to represent XXXX.
- Use any program, script, or command, or send messages of any kind, with the intent to interfere with, or disable a user's access.
- Breach, or interfere with the investigation of a breach of:
    - XXXX policies
    - State, Commonwealth, or International Laws.

4.4 Clear Desk and Clear Screen

Users will adhere to the following:

- Information Assets and Information Systems will be left logged off or protected with a screen locking mechanism controlled by a password when left unattended.
- Users will ensure any hard copy Information Assets are appropriately secured (locked in a filing cabinet, secured at home) before leaving the desk unattended.
- Information Assets and Information Systems should never be left unattended while travelling or in public places (including leaving devices visible in unattended vehicles)
- A passphrase protected screen saver will be automatically enabled after 15 minutes of inactivity, requiring the User to unlock the computer with their account credentials.
    - As best practice, XXXX personnel are advised to lock their screen upon leaving the desk/workspace unattended (**Press Windows logo key + L**)

4.5 Social Media

XXXX Social Media Policy should be referenced in regard to Acceptable Use.

4.6 Personal Devices

XXXX permits the use of personal devices ('Bring Your Own Device or 'BYOD') where applicable.

The Mobile Device Policy should be followed, and all use should align with XXXX Acceptable Use Policy.

4.7 Reporting Incidents

- Users must report the following to the XXXX as soon as practicable:
    - Suspected or actual security incidents
    - Security weaknesses in people, processes, and/or systems
    - Security risks
    - Security issues
- If an XXXX owned device or personal device containing XXXX data is lost or stolen, the User must report the incident immediately to the XXXX.
- If an XXXX owned device or personal device containing XXXX data is lost or stolen while off-site, the User may be required to file a police report with the appropriate local Police and obtain a reference number.

4.8 Training and Awareness

Periodic awareness training on information security shall be conducted to facilitate User understanding and compliance with policies, procedures, and standards.

4.9 Monitoring and Privacy

XXXX reserves the right to audit all use of Information Assets and Information Systems periodically to ensure compliance with this Policy and protection of Information Assets. XXXX has implemented various security controls which capture logs, user behaviour, and analytics information based on User interaction with XXXX Information Assets and Information Systems. Logs and alerts from such systems shall be retained as per XXXX backup and data retention plans.

5. Breach of Policy

XXXX will suspend a User's access to Information Assets and Information Systems where there are reasonable grounds to suspect that a User has breached the guidelines within this Policy.

Misuse of Information Assets and Information Systems will be dealt with in accordance with the XXXX Code of Conduct & Integrity, including but not limited to, termination of employment.

Breaches of this policy are to be reported to the relevant member of XXXX

6. Related Policy Documents

- Social Media Policy
- Access Control and Password Policy
- Privacy Policy

7. Review

This policy must be reviewed annually, or earlier if required.