Australian Cricket

Cyber and Information Security Policy

Version 6.4 February 2025

CONTENTS

1. DOCUMENT DETAILS

Responsible	Accountable	Consulted	Informed
Head of Cyber Security	Head of Cyber Security	Australian Cricket Technology Leadership Head of Risk	Australian Cricket

Audience	Classification
Australian Cricket	Confidential
Approved By	**Endorsed By**
General Manager, Australian Cricket Technology	Australian Cricket Technology Steering Committee

Version	Comments	Created By	Approved By	Approval Date	Next Review Date
1.0	New document	Security Manager, SPMS Technology	Head of Technology		
4.0	Steering committee review	Security Manager, SPMS Technology	Head of Technology	September 30, 2017	August 2018
5.0	Annual review	Snr Mgr, Security & Operations	General Manager, Technology	March 29, 2019	Q1 2020
6.0	Annual review	Snr Mgr, Security & Operations	General Manager, Technology	September 2020	Q3 2021
6.1	Style and minor form updates	Head of Cyber Security	General Manager, AC Technology	September 2022	March 2023
6.2	Annual review	Head of Cyber Security	General Manager, AC Technology	January 2023	January 2024
6.3	Annual review	Head of Cyber Security	General Manager, AC Technology	March 2024	January 2025
6.4	Annual review	Head of Cyber Security	General Manager, AC Technology	February 2025	January 2026

2. PURPOSE

The Australian Cricket (AC) cyber security function is focused on achieving the right balance between the required levels of information protection, while taking into consideration the user experience, speed to market, and organisational culture.

The purpose of this policy is to:

a) establish and communicate the expectations for cyber and information security across AC;
b) ensure the security of sensitive information and assets under AC's custody or care; and
c) ensure the secure ongoing operation of all AC entities.

The policy is designed to support the following goals:

a) Support AC Personnel in performing their role.
b) Protect Australian cricket, its fans, participants, and people. This includes protecting the reputation of Australian cricket and its relationship with stakeholders.

AC's fans, participants, and people will be at the centre of all of our thinking, and we will prioritise them in any decision-making or policy setting within the cyber and information security context. Protecting this cohort and ensuring their safety and security is fundamental to growing cricket, and to uniting and inspiring everyone to love and play cricket.

3. STANDARDS

The Head of Cyber Security will maintain a series of standards that support the Cyber and Information Security Policy. These standards must include:

a) awareness and training;
b) backup and archiving;
c) business continuity;
d) change management;
e) configuration management and maintenance;
f) cryptography and key management;
g) cyber security assurance;
h) external suppliers;
i) identity and access management;
j) incident management;
k) information classification and handling;
l) log management and monitoring;
m) malicious code and software;
n) mobile device and remote working;
o) patch and vulnerability management;
p) physical security;
q) privacy;
r) secure application development; and
s) secure deletion and disposal.

The Head of Cyber Security may introduce additional standards with the approval of the General Manager – Australian Cricket Technology.

All standards must be reviewed annually and endorsed by the Australian Cricket Technology Steering Committee (or other responsible committee, council, or individual as specified within the standard).

While the Head of Cyber Security maintains the standards, responsibility and accountability is shared with other members of Australian Cricket leadership (as specified within each standard).

4. POLICY STATEMENTS

The Cyber and Information Security Policy is composed of the following policy statements:

<table>
<tr><th colspan="3">MEET AUSTRALIAN CRICKET'S LEGAL AND REGULATORY REQUIREMENTS</th></tr>
<tr><td colspan="3">Our objective is to ensure Australian Cricket complies with relevant laws and regulations governing information security.</td></tr>
<tr><td colspan="3">Because laws and regulations frequently change, and in most jurisdictions throughout the world, ignorance of the law is no defence, we must ensure our cyber and information security safeguards are maintained in accordance with those laws and regulations. Failure to do so may result in sanctions or penalties.</td></tr>
<tr><th>ROLE</th><th>RESPONSIBILITIES</th><th>SUPPORTING DOCUMENTS</th></tr>
<tr><td>Cyber Security</td><td>Consult with Legal on any legal or regulatory requirements which may impact the Cyber and Information Security Policy.

Ensure responsibilities for compliance with laws and regulations are assigned and understood.

Establish and maintain governance practices which establish, resource, and maintain cyber and information security practices.

Ensure that this policy and supporting cyber and information security standards is communicated to all personnel.

Monitor, manage, and report on compliance.

Consult with legal as required on changes to laws and regulations which may impact compliance.

Implement controls to meet compliance requirements.</td><td rowspan="3">Cyber and Information Security Policy (this document).

Australian Cricket Privacy Policy.

Australian Privacy Principles (as detailed in the Privacy Act).

Cyber Security Assurance Standard</td></tr>
<tr><td>Business unit representatives</td><td>Contribute to the design and implementation of controls to meet compliance requirements.</td></tr>
<tr><td>Everyone</td><td>Comply with Australian Cricket technology, cyber, and information security policies, standards, legal and regulatory requirements.

Report any non-compliance with technology, cyber, and information security policies to the relevant owner.</td></tr>
</table>

<table>
<tr><th colspan="3">PROTECT AUSTRALIAN CRICKET'S INFORMATION ASSETS</th></tr>
<tr><td colspan="3">Our objective is to ensure appropriate controls are in place to secure Australian Cricket information assets (based on the value of information to the business and our fans and participants).</td></tr>
<tr><td colspan="3">Because applying security safeguards equally to all information is expensive and time-consuming, security safeguards should be appropriate to the value or sensitivity of the information protected.</td></tr>
<tr><th>ROLE</th><th>RESPONSIBILITIES</th><th>SUPPORTING DOCUMENTS</th></tr>
<tr><td>Cyber Security</td><td>Define and implement security and data classification standards, targeted at information, regardless of location.
Implement controls to ensure information assets are managed in accordance with the Information Classification and Handling Standard.</td><td rowspan="4">Technology Usage Policy
Technology Asset Register
Information Classification and Handling Standard
Configuration and Maintenance Standard
Cryptography and Key Management Standard
Patch and Vulnerability Management Standard
Secure Application Development Standard
Backup and Archiving Standard
Malicious Code Standard
Secure Deletion and Disposal Standard
Physical Security Standard
Change Management Standard
External Suppliers Standard
Mobile Device and Remote Working Standard
Identity and Access Management Standard</td></tr>
<tr><td>Business unit representatives</td><td>Identify information assets used within the business area and assign ownership to a relevant business stakeholder (information owner).</td></tr>
<tr><td>Information owners</td><td>Classify information assets in accordance with the Information Classification and Handling Standard.</td></tr>
<tr><td>Everyone</td><td>Handle, evaluate and classify information produced commensurate to the sensitivity in accordance with the Information Classification Standard.
Adhere to approved operating methods, systems, and tools.</td></tr>
</table>

<table>
<tr><th colspan="3">MANAGE AUSTRALIAN CRICKET CYBER SECURITY RISKS</th></tr>
<tr><td colspan="3">Our objective is to understand the security risks to Australian Cricket information assets and business operations and take precautions commensurate with the risks to the business.</td></tr>
<tr><td colspan="3">Because underestimating cyber security risks can result in inadequate safeguards being put in place to protect our information assets, and overestimating our cyber security risks can result in over-spending on cyber security and productivity losses.</td></tr>
<tr><th>ROLE</th><th>RESPONSIBILITIES</th><th>SUPPORTING DOCUMENTS</th></tr>
<tr><td>CA Audit & Risk Committee and S/T counterparts

Technology Steering Committee

Risk</td><td>Define the cyber security risk appetite for the business per the Risk Management Framework.</td><td rowspan="4">Risk Management Framework

Technology Risk Profile

Technology Risk Register

Exemption Register

External Suppliers Standard

Cyber Security Insurance Policy

Cyber Security Assurance Standard</td></tr>
<tr><td>Cyber Security</td><td>Understand, evaluate and remediate any potential risks and vulnerabilities to our systems and services in accordance with our Risk Management Framework.

Implement and manage controls in line with the risk and in accordance with Australian Cricket security standards and guidelines.

Maintain a risk profile within the risk appetite.</td></tr>
<tr><td>Business unit representatives</td><td>Undertake security risk assessments for new projects, systems or services, and update existing risk assessments where there is a change to the operating environment of a system or service.

Contribute to risk identification and mitigation discussions.</td></tr>
<tr><td>Everyone</td><td>Participate in risk management processes and assessments.

Report cyber security risks perceived or otherwise, and relevant controls.</td></tr>
</table>

<table>
<tr><th colspan="3">ENSURE APPROPRIATE ACCESS TO INFORMATION AND RESOURCES</th></tr>
<tr><td colspan="3">Our objective is to ensure only appropriate access to Australian Cricket information assets and resources is given to parties who need access.</td></tr>
<tr><td colspan="3">Because controlling access to information through the principle of least privilege is the most effective method to reduce our cyber security risk. Failure to control sensitive information increases our risk of unauthorised disclosure, fraud, misuse of information, which can result in adverse financial results or media attention.</td></tr>
<tr><th>ROLE</th><th>RESPONSIBILITIES</th><th>SUPPORTING DOCUMENTS</th></tr>
<tr><td>Cyber Security</td><td>Develop and maintain data loss prevention and rights management framework, including monitoring and auditing.</td><td rowspan="4">Technology Usage Policy
Identity and Access Management Standard
Information Classification and Handling Standard
Physical Security Standard
Cryptography and Key Management Standard
Configuration and Maintenance Standard
External Suppliers Standard</td></tr>
<tr><td>Business unit representatives</td><td>Only authorise access to information assets where there is a business requirement for access.
Regularly review access to information assets on a quarterly basis and remove those without a business need.
Ensure the access authorised minimises the risk of fraud or misuse.</td></tr>
<tr><td>Information owners</td><td>Only provision access that has been authorised.
Only provision access to information assets and resources using a uniquely identifiable method.
Only provide access that supports segregation of duties, according to roles and responsibilities.</td></tr>
<tr><td>Everyone</td><td>Obtain authorisation for access to information and resources from the information owner or formal delegate, and your line manager.</td></tr>
</table>

MANAGE CYBER AND INFORMATION SECURITY INCIDENTS		
Our objective is to ensure that Australian Cricket has the capability to detect and respond to security incidents to reduce the risk of harm to Australian Cricket's fans, participants, and people, to prevent disruption to cricket activities and any consequent reputational damage.		
Because cyber and information security threats always change, and security controls will never secure Australian Cricket against all threats.		
ROLE	**RESPONSIBILITIES**	**SUPPORTING DOCUMENTS**
Cyber Security	Develop and maintain an incident management framework to ensure methodical resolution of incidents. Implement security monitoring capabilities on all environments and systems hosting sensitive information. Resolve security incidents effectively, with the support of the technology team. Report and manage the risks to the business. Ensure that relevant business areas are kept aware of their responsibilities during a cyber incident. Ensure that relevant business areas have the necessary training and education to effectively respond to a security incident.	Incident Management Standard Incident Response Plans Log Management and Monitoring Standard Awareness and Training Standard
Business unit representatives	Provide support to incident management teams. Escalate incidents to cyber security. Take part in incident management planning and practice.	
Everyone	Report suspected incidents of suspicious activity as soon as possible. Support and cooperate with cyber security investigations. Undertake cyber security awareness and training.	

PROVIDE CYBER ASSURANCE TO OUR STAKEHOLDERS		
Our objective is to validate that implemented cyber security measures are functioning effectively and as expected and be able to report to relevant internal and external stakeholders.		
Because Australian Cricket is responsible for providing proof to auditors, regulators, and third parties that information assets are protected. Failure to provide sufficient assurance of that protection can result in the loss of confidence in the business.		
ROLE	**RESPONSIBILITIES**	**SUPPORTING DOCUMENTS**
Cyber Security	Obtain independent assessments and testing of cyber and information security controls, and ensure remediation activities are undertaken where those controls are unsatisfactory. Ensure that our policies and standards are reviewed regularly (at least annually) to ensure they reflect our current environment and needs.	Cyber Security Assurance Standard
Business unit representatives	Take responsibility for cyber security within your business unit. Gather and maintain evidence that cyber security measures have been implemented within your business unit in accordance with the Australian Cricket cyber and information security standards. Assess and report on compliance with relevant cyber and information security controls for all systems under your care at least annually.	
Everyone	Be involved in the assurance process and assist in the evaluation of controls.	

MANAGE THIRD PARTY CYBER RISKS		
Our objective is to ensure our partners can be trusted to protect Australian Cricket information assets under their care by managing our external stakeholders to reduce the risk of compromise of sensitive information.		
Because Australian Cricket information assets entrusted to third parties are still under the responsibility of Australian Cricket to secure against a breach.		
ROLE	**RESPONSIBILITIES**	**SUPPORTING DOCUMENTS**
Cyber Security Procurement Legal Risk	Develop and maintain a process for assessing the risk of third parties who have access to Australian Cricket Information. Evaluate and assure the compliance of third parties with relevant security standards and their ability to secure the information entrusted to them.	Suppler Information Security Risk Assessment Questionnaire Vendor Management Framework (Procurement) External Suppliers Standard Cyber Security Assurance Standard
Business unit representatives	Take accountability for the cyber security of external stakeholders. Ensure that all agreements with third parties include cyber security provisions, the right to audit, and a requirement to report cyber security incidents to Australian Cricket.	
Everyone	Be involved in the assurance process, and assist in the evaluation of controls. Ensure agreements are in place with third parties to secure information before sharing information with them.	

5. ROLE DEFINITIONS

Cyber Security
The Cyber Security team supports the entire business by developing strategies, controls, and monitoring compliance to ensure that systems and networks are appropriately secured to ensure they are:

a) available to authorised fans, participants, volunteers, and personnel;
b) protected from unauthorised access; and
c) protected from unauthorised modification or tampering.

Business unit representative
Business unit representatives (typically the head of the relevant business area or their delegate) support cyber security in defining access rights to the systems and processes under their purview. They are also tasked with taking responsibility for ensuring cyber security controls (as defined in this policy and the Information Security Management Framework) are implemented within their business area and for monitoring compliance on an ongoing basis.

Information owner
The person who creates or initiates the creation of a specific piece of information. In practical terms, often the information owner will be the head of the relevant business area in which the information originated.

Everyone
Refers to AC Personnel. All AC Personnel have a responsibility to familiarise themselves with the policies and procedures that comprise the Cyber and Information Security Policy and Information Security Management Framework and ensure they comply with any cyber security requirements relevant to their role.

6. CYBER SECURITY EXEMPTIONS

While the Australian Cricket Cyber and Information Security Policy (and its associated Standards and Procedures) apply to all AC Personnel as well as third parties with access to Australian Cricket systems or information, there may be instances in which compliance with specific security requirements is not possible.

In these circumstances, the following steps must be followed:

Lodgement of exemption request
The relevant business unit representative is to identity activities that do not meet documented security requirements and request an exemption from the relevant requirement(s) by lodging a Cyber Security Exemption Request.

The Cyber Security Exemption Request must be lodged with the cyber security team and needs to:

a) identify the specific cyber security requirements that cannot be complied with;
b) the reasons for non-compliance; and
c) any mitigations that may be able to be implemented to compensate for the non-compliance.

Review of exemption request
Once the Cyber Security Exemption Request is received, the Head of Cyber Security will review it to consider whether granting the exemption:

a) may pose unacceptable cyber security risk;
b) may otherwise unduly impact the ability of Australian Cricket to achieve its business objectives; and
c) whether it is practical and possible to implement any mitigating actions in order to reduce the level of risk associated with the exemption (should it be approved).

The Head of Cyber Security must assign a low, medium, or high risk rating depending on the level of severity associated with the exemption and include a recommendation as to the duration the exemption should last for prior to being reviewed.

Approval of Exemption Request
The Head of Cyber Security must forward any Cyber Security Exemption Requests carrying a risk of high to the General Manager of Australian Cricket Technology and the executive owner of the impacted system for approval.

If approved, the approval must also include the duration for which the exemption remains valid.

Documentation of risks for approved requests in risk register
If the Cyber Security Exemption Request is approved, the risk is documented in the Technology Risk Register. The Register will be regularly reported to the CA Audit & Risk Committee and applicable AC Entity equivalents.

Review of approved exemptions
Approved exemptions must be reviewed annually by the Head of Cyber Security to ensure that the granting of the exemption remains appropriate. If this is not the case, the Head of Cyber Security should notify the relevant business unit representative.

7. CISMS MAPPING

The table below maps the External Supplier Security Standard with the security domains of ISO27001:2022 Security Standard and National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 - Security and Privacy Controls for Information Systems And Organizations.

ISO27001:2022	**Information Security Policy**
5.1 Policies for information security 6.2 Information security objectives and planning to achieve them 7.3 Awareness	Protect Our Assets Manage Third Party Risks Manage Security Risks Ensure Appropriate Access to Information and Resources
NIST SP 800-53	
PL-1,2, Planning (3.12)	