Cyber/Information Security Policy and Procedure

1. Purpose

1.1. The purpose of this Policy and Procedure is to set out the information security policies that apply to the Australian Performing Arts Conservatory (APAC) to protect the confidentiality, integrity, and availability of data.

1.2. This Policy and Procedure establishes APAC's cyber security risk management and responsibilities, and it applies to all APAC, and any entity or person associated with APAC authorised for the use of Digital Services including, but not limited to the internet and email.

1.3. This Policy and Procedure aims to protect APAC's information from unauthorised access, loss, or damage, intentional or otherwise while ensuring seamless access to academic resources by students.

2. Scope

This Policy and Procedure is broad and applies to all stakeholders at APAC that hold or process APAC information, including:

- Current, prospective and former students;
- Staff;
- Third parties (e.g., consultants, contractors, education agents, partners and suppliers);
- Visitors.

3. Chief Executives Statement of Commitment

APAC is committed to the protection of all data within APAC's various systems. APAC recognise that we have a responsibility to protect all the data we hold or process, whether it belongs to APAC, our employees, students, partners or suppliers. By protecting this data, we can ensure that we maintain our reputation as a trusted employer and education provider, enabling us to grow as a business and deliver exceptional education to our students.

It is the responsibility of all our staff, to understand and acknowledge our security management processes and to comply with all information security and privacy policies and the procedures that underpin them.

We commit to ensure that our security management systems and processes are efficient, effective and continuously improving to protect our data assets while avoiding the reputational, legal and financial harm that would result from a data breach.

4. Principles and Key Requirement

4.1. Policy Statement

4.1.1. APAC recognises the importance of cybersecurity. It is committed to ensuring all Institute activities involving Information Technology are appropriately defended against cybersecurity threats.

4.1.2. APAC is committed to the appropriate use of Information Technology and Services to support its learning, teaching, research, administrative, and service functions. The Acceptable Use of Information Technology Policy defines acceptable behavior expected of APAC users using APAC IT Facilities and Services.

4.1.3. Management of cyber security risk requires a concerted effort across all APAC and APAC recognises that successful implementation of cybersecurity relies on having a well-informed user community combined with effective management procedures.

4.1.4. This overarching policy is supported by this recognition, and it provides principles for APAC's continuous enhancement in terms of operational practice, action plans, technology controls and education programs around the concern of cybersecurity.

4.1.5. APAC's approach to cyber security is informed by the Australian Cyber Security Centre Information Security Manual and Guidelines ACSC Homepage | Cyber.gov.au.

4.2. Information Security Objectives

4.2.1. To ensure the confidentiality, integrity, and availability of APAC information including all personal data as defined by the GDPR based on good risk management, legal regulatory and contractual obligations, and business needs.

4.2.2. To provide the resources required to develop, implement, and continually improve the information security management system.

4.2.3. To manage third-party suppliers who process, store, or transmit information to reduce and manage information security risks.

4.2.4. To implement a culture of information security and data protection through effective training and awareness.

4.3. Information Security Policy Framework

The key platforms of the framework are information management, cyber security risk management and cyber security incident management, as explained below.

4.3.1. The specification of cyber security controls is incorporated into relevant IT standards or as separate cyber security standards.

4.3.2. APAC will have sufficient IT and cyber security standards to facilitate the effective implementation of cyber security controls across all IT infrastructure, systems, and applications.

4.3.3. Standards will be developed in consultation with key stakeholders to support business requirements, provide adequate cyber security risk mitigation, and align with the cyber security strategy.

4.3.4. The Cyber Security Standard Exception Procedure is available for instances where the standard is not suitable, otherwise, the standard must be followed.

4.3.5. Standards will be updated as required to reflect changes in security controls.

4.4. Cyber Security Risk Management

Cyber security controls seek to reduce cyber security risk by either reducing the likelihood or impact of an incident or both.

APAC will continue to identify and treat cyber security risks by implementing and following preventive measures:

4.4.1. Internet, website, and email filtering;

4.4.2. Enterprise Endpoint Detection and Response;

4.4.3. Change request control and ITIL framework;

4.4.4. Password strength and multi-factor authentication;

4.4.5. Endpoint and system management and monitoring;

4.4.6. Security controls in application and patch management;

4.4.7. Restricted administrative privilege;

4.4.8. Regular backups;

4.4.9. Maintaining a register of key information assets;

4.4.10. Establishing a framework for performing cyber security risk assessments aligned with APAC's Enterprise Risk Management Framework;

4.4.11. Incorporating cyber security risk identification and assessment into processes impacting the use and processing of APAC information;

4.4.12. Maintaining a register of cyber security risks with related controls;

4.4.13. Review risks at regular intervals and because of significant security incidents, threats, or changes to business requirements;

4.4.14. Implementing and strengthening controls to reduce risk;

4.4.15. Evaluating the effectiveness of controls;

4.4.16. Make staff and contractors aware of the security requirements of APAC IT resources and services and take precautions to safeguard their access to systems against any unauthorised use.

4.5. Cyber Security Incident Management

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

The APAC Cyber Security Incident Response Plan details how incidents are managed and aim to comply with applicable legal requirements, minimise harm to impacted individuals, and minimise damage and risk to APAC.

Incidents should be reported immediately to the IT Team.

4.6. Information Security Roles and Responsibilities

Information security is the responsibility of everyone to understand and adhere to the policies, follow processes and report suspected or actual breaches.

4.7. Responsibilities of All Users

Users are responsible for:

4.7.1 Cyber Security Events or breaches of security controls must be reported to the IT Team immediately, even if only suspected.

4.7.2 Use of all remote desktop software presents a significant threat to the security of APAC's Digital Services. As such, the CEO and Head of IT must first authorise and approve any software solution that provides remote access, to ensure the confidentiality, integrity, and availability of APAC's Digital Services and Data.

4.7.3 When using or accessing APAC Digital Services remotely or from a personal device, be aware of the inherent risks to the privacy of confidential and sensitive information kept in those services and ensure the personal device used to access APAC's Digital Services is up-to-date and virus free and will not circumvent or compromise the security controls the institution places around its Digital Services.

4.7.4 Keep passwords confidential and do not disclose them to others.

4.7.5 Change their password as soon as possible if they suspect, or come to know, that their password has been compromised.

4.7.6 Distribute, transmit, move, or delete information assets only if there is a valid business or academic need to do so.

4.7.7 Not remove APAC information assets or equipment from APAC facilities without prior authorisation. An authorisation is deemed to have been granted to use APAC-issued portable devices (such as laptops, mobiles, and tablets), to conduct daily business activities from remote locations.

4.7.8 Distribute, transmit, move, or delete information assets in accordance with APAC information handling standards and relevant contractual regulations and legal regulations.

4.7.9 Users must not store information assets classified as 'confidential' or 'restricted' on the facilities of external providers, unless the use of the facility has been approved by the applicable asset owner and the CEO, Head of IT.

4.8. Responsibilities of APAC

APAC is responsible for:

4.8.1 To establish the Digital Information Security Policy, defining, and supporting a strong security culture.

4.8.2 Through the Finance, Audit and Risk Management Committee (FARM) ensuring the APAC has effective cyber security and foreign interference controls in place to protect the Company.

4.8.3 The review of digital material which can pose a risk to the APAC is undertaken by appropriate Marketing and Communications authorised personnel.

4.8.4 Providing appropriate training and awareness campaigns created to educate Authorised Users about Cyber Security Events and issues, as well as foreign interference awareness, to improve the effectiveness of the reporting and response processes.

4.9. Responsibilities of the APAC Management Team

APAC Management Team is responsible for:

4.9.1 Authorising the appropriate group(s) within IT to perform specific procedures for ensuring APAC's Cyber Security, including those identified within this policy.

4.9.2 All Cyber Security Events reported to IT are evaluated to determine if a response is required. If a response is required, the Event becomes a Cyber Security Incident and will be managed by the appropriate response team in accordance with the steps outlined in the Cyber Security Incident Management Procedure. This will ensure a consistent and effective approach to the management of Cyber Security Incidents, including communications, and that the collection and analysis of evidence from the Cyber Security Incident occurs without compromising its integrity.

4.9.3 Logs are reviewed to identify and manage Cyber Security Incidents and/or breaches in the security of Digital Services, as well as create and manage records and documents associated with Cyber Security Incidents for further analysis. In the event of a breach in APAC's Information Security, IT will utilise the IT Data Breach Incident Report Procedure to triage the event and notify appropriate parties within APAC if personal data is involved, as defined in the Privacy Policy and Privacy Management Plan.

4.9.4 Controls and other preventative measures are put in place to avoid Cyber Security Incidents, either because of experience from previous Cyber Security Incidents or as a countermeasure or deterrent to likely Cyber Security Incidents. These measures are documented and regularly reviewed to ensure their validity and reliability.

4.9.5 Nominated members of IT actively participate in higher education sector and government cyber security exercises, as appropriate.

4.9.6 If a Cyber Security Incident is identified as originating from a state-based foreign actor, escalation within and external to the APAC is considered appropriate in the interests of national security.

4.10. Responsibilities of the CEO and Head of IT

The CEO and Head of IT are responsible for:

4.10.1 Actively supporting information security through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

4.10.2 Ensuring that all information security roles and responsibilities are clearly allocated.

4.10.3 Ensuring that the Information Security Policy and all supporting processes are effectively implemented in their areas of responsibility.

4.10.4 Conducting risk assessments to identify and define the positions that require applicants to pass personal background checks as part of the recruitment process; and

4.10.5 Communicating to staff members leaving the APAC their ongoing responsibilities to the APAC (which include ongoing confidentiality requirements in relation to APAC's information assets).

4.11. Responsibilities of Asset and Service Owners

Asset and Service Owners are responsible for:

4.11.1 Ensuring that all visitors and contractors are given temporary authorisation for appropriate system access, which will expire on the visitor or contractor's expected departure date or contract end date.

4.11.2 Security Controls being implemented and maintained according to the relevant APAC security standards.

4.11.3 The confidentiality, integrity and availability of information assets and information systems is protected by appropriate controls that are determined through a risk-based approach.

4.12. Responsibilities of External Providers

External providers must not commence handling or processing any information assets for the University until it has entered an appropriate contract with the APAC that includes relevant information security controls with which the provider must comply.

Without limiting external providers' other obligations set out in this policy, external providers must implement, operate, and maintain the appropriate information security controls as specified in their contracts with APAC.

The Head of IT will monitor and review external provider services and manage any changes to external provider contracts considering information assets and information systems.

External providers must ensure that they only connect devices to APAC network using approved secure access methods.

4.13. Monitoring

Compliance with the policies and procedures of the information security management system is monitored via the APAC Management Team, together with independent reviews by both Internal and External Audit on a periodic basis.

4.14. Legal and Regulatory Obligations

The organisation takes its legal and regulatory obligations seriously and these requirements are documented.

4.15. Training and Awareness

Policies are made readily and easily available to all employees and third-party users. A training and communication plan is in place to communicate the policies, processes, and concepts of information security. Training needs are identified, and relevant training requirements are documented.

4.16. Continual Improvement of the Management System

The information security management system is continually improved and documented to ensure that there is a continual improvement process in place.

5. Policy Compliance

5.1. Compliance Measurement

The APAC management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved and documented by the IT team in advance and reported to the APAC Management Team.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.4. Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

6. Related Legislation

- Higher Education Standards Framework (Threshold Standards) 2021
- Education Services for Overseas Students Act 2000 (ESOS Act)

Version Control and Document Owner

Policy Category	Operational	**Approval Date**	25 January 2023
Document Owner	Chief Executive Officer	**Approval Authority**	The Board of Directors
Audience	Staff	**Review Date**	January 2026

Revision History				
Version	**Author**	**Change Summary**	**Date Approved**	**Date Effective**
1.0	DVE Business Solutions Pty Ltd	New document.	9 December 2022	
1.1	APAC	Review and update of policy and procedure.	25 January 2023	
1.2	DVE Business Solutions Pty Ltd	Added education agents to scope. Approved by Document Owner.	24 May 2023	24 May 2023
1.3	APAC	Change from QRMC to FARM Committee		22 May 2024