APIC
ASIA PACIFIC INTERNATIONAL COLLEGE

CYBER SECURITY POLICY

Document ID	Cyber Security Policy
Related Documents	Data Collection Policy Information Technology Security Procedures Privacy Policy Risk Management Policy Student Code of Conduct Staff Code of Conduct Workplace Surveillance Policy Risk Management Plan ICT Disaster Recovery Plan ICT Management Plan
Date	12 September 2017
Date of Next Review	12 September 2019
Authorised by	Director of Accreditation, Compliance and Quality Assurance
Approved by	Governing Board, 20 October 2017
Version	2.0
Responsible Officer	ICT Manager
References and Legislation	Privacy Act 1988

Contents

1. Purpose

This general Cyber Security Policy has been prepared to outline APIC's internal policy and procedures for the protection of data and specific cyber threats as identified herein. In addition to its internal use, this policy may be provided to APIC's employees, students, business partners, contractors, and vendors to provide assurance of APIC's commitment to information technology security and data protection.

APIC understands that in providing its services it may, from time to time, store or transmit data belonging to its students, partners, clients, vendors, or their customers. APIC is willing and able to work with its business partners to ensure high standards of data protection are met, in line with APIC's partners' data protection commitments.

a) This document sets out the APIC policy on cyber security. APIC recognises that its practices involve large volumes of data that is stored and communicated electronically, both of APIC internally and of its students, and the security of this information and protection from external threats is a key priority.

b) The purpose of the policy is to ensure there are measures and practices in place directed at protecting IT facilities and services, and stored data, from unauthorised access, use, disclosure, disruption, modification, hacking, phreaking, phishing, reverse engineering and destruction.

c) APIC aims to ensure its IT facilities, services and stored data have adequate controls and protections that are relative to the perceived cyber security risks, so that the integrity and confidentiality of data is maintained at all times.

d) APIC is committed to ensuring APIC's activities that use IT facilities, services and data are properly defended against the perceived cyber security threats. This necessarily requires effective management procedures and informed staff and students.

e) This policy sets out:

- requirements for physical access to and control of APIC Devices and Servers;
- security standards applicable to APIC Workstation and Servers;
- network security standards;
- roles and responsibilities of APIC Staff;
- data protection policy;
- dealing with specific threats; and
- Security incident response procedure.

f) All staff and, to the extent required, students, across APIC's offices should be made aware of this policy, their responsibilities and obligations. All staff are obliged to comply with this policy, as well as observe their obligations under relevant legislation (including privacy law)

2. Scope

This policy applies to all APIC students, staff members and contractors who use APIC IT resources during business hours or outside business hours in relation to their employment or engagement with or on behalf of APIC. APIC employees and contractors are required to comply with this policy (and other instruction issued by APIC from time to time)

Breach of this policy may be dealt with using APIC's disciplinary procedures, and in serious cases may be treated as misconduct and result in a summary dismissal and/ or termination of the provision of services.

3. Definitions

Item	Definition
Access Hours	The time period during which APIC Staff are present at APIC premises, and shall reflect the ordinary business hours of APIC.
Confidentiality Agreement	a Windows, Office or similar user account created for use on or with any APIC System.
APIC Asset	Any device, server, workstation, computer, tablet, laptop, system, router, hub, switch, bridge, network filter, or other component used by APIC, its employees, agents, or contractors, or otherwise connected to APIC network infrastructure.
APIC Server	A computer, owned or operated by APIC, which stores, processes, hosts, provides, or controls access to data.
APIC Staff	Any employee of APIC, or any contractor engaged to provide services to or on behalf of APIC.
Student	Any person who is enrolled in any course or program offer at, or in conjunction with, APIC.
APIC System	Any computer (including workstation, server, or mobile device), application, used, hosted, developed, owned, or provided by APIC.
APIC Workstation	A desktop computer, laptop computer, tablet, or mobile device owned by APIC or used with an APIC System.
Confidential Information	Information which is not generally publicly available, and unauthorised disclosure of this information may cause damage (either financial or reputational) to APIC, its students, Staff or agents, clients, or related parties. Confidential information includes any information that is protected under Australian legislation (for example, the *Privacy Act 1988*), or information which may be the subject of a Confidentiality Agreement between APIC and another party. This information requires a high level of protection against unauthorised access and disclosure, modification, use, and destruction.
Core Infrastructure	Servers and network devices including routers, switches, hubs, wireless access points, modems, network filters, network taps, and cables.
LMS	Learning Management System

Item	Definition
Partner	A third party to whom APIC delivers its services or with whom APIC works to deliver services.
Phishing/Phreaking	The action of hacking into telecommunications systems.
Restricted Information	Information which is not generally publicly available, and unauthorised disclosure of this information may cause damage (either financial or reputational) to APIC, its students, Staff or agents, clients, or related parties. This information must be protected against unauthorised access and disclosure, modification, use, and destruction, however, the sensitivity of Restricted Information is lower than that of Confidential Information.
Security Incident Response	The prescribed procedure for dealing with any actual, suspected or threatened data security threat or incident.
Secured System	Microsoft Office 365 and other line-of-business applications that store, transmit, or otherwise use APIC Data.
SMS	Student Management System.
Student Data	Data pertaining to any of APIC's students.
Unrestricted Information	Information which may be publicly available, or which may be disclosed without risk of damage to APIC, its Staff, clients, or related parties.
User	A person who uses an APIC System.
Visitor	A person attending the APIC premises who is not an APIC Staff member.

4. Principles

The use of APIC's IT facilities and services must comply with the policies set down by APIC and any applicable legislation in respect of privacy, copyright and intellectual property, employment and workplace health and safety. This document is to be read in conjunction with the APIC Privacy Policy (including as incorporated into the Data Protection Policy).

The operations and management of APIC's IT facilities and services will ensure that:

- Security critical data, services, programs and infrastructure are identified and managed in proportion to the level of perceived risk, with regular control procedures in place if required;
- A cyber security monitoring program is in place and updated daily, and which includes analysis of cyber risk events, audits, and other relevant tests; and
- A recovery plan is in place and regularly tested for any security critical applications and IT infrastructure in case an adverse cyber security event occurs.

5. Staff training

All APIC Staff:

- are to be provided with a copy of this policy, and training on this policy which can be found in the on-line College policy library;
- are able to ask questions and provide feedback about the policy;
- are to be informed about changes to this policy, and are able to access the full policy when it is updated; and
- should request help or clarification from their line manager or any member of the data security team.

6. Key Persons and Responsibilities

The ICT Manager has the following responsibilities:

- Implementing and enforcing the APIC Cyber Security Policy and framework with the Data Security Team;
- Develop and implement any operational policies and procedures required to ensure the effective application of this policy;
- Developing, testing and implementing cyber security management and monitoring programs;
- Developing, testing and implementing the adverse cyber security event recovery plan;
- Taking immediate action on any perceived cyber security risks, including disconnection of key networks and equipment; and
- Reporting to the President on the implementation of this policy and any incidents or breaches.

The ICT Team Leader has the following responsibilities:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is properly functioning.
- Evaluating any third-party services the company is considering using to store or process data to ensure it complies with or is capable of complying with, this agreement.

The International Recruitment Manager is responsible for

- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries;
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principals and this policy.

These persons, collectively, are referred to as the Data Security Team.

7. Physical Access and Control

7.1 On-Site Access

Access to APIC's office premises and on-site APIC assets must be restricted to APIC staff, students and authorised personnel. All APIC staff accessing APIC's systems must possess a key or code to the relevant locked room (insofar as this applies) and password issued in accordance with this policy for access to all devises.

Access to APIC's core infrastructure must be restricted to only personnel who require access during their employment. Access privileges must be assessed by the Data Security Team and reviewed at least once every 12 months.

Visitors to APIC's business premises must, upon arrival, provide identification to APIC reception, and complete and sign a log-book. Whilst on-premises, visitors must be accompanied at all times by an APIC staff member.

Unless necessary and approved by the Data Security Team, access to APIC premises outside the hours of 08:00 and 17:00 Monday to Friday and to core infrastructure is restricted to only authorised personnel. Access controls must be tested every 12 months or as directed by the Data Security Team.

Access to APIC software and assets is removed at the time of an employee's separation from APIC whilst completing the termination checklist before final payment to the employees

7.2 Equipment Installation

Core infrastructure must only be installed by persons suitably authorised or registered to perform installation of the relevant equipment. Where compliance with industry standards and certification is required for the installation such equipment, persons engaged to perform equipment installation must hold a current and appropriate qualification.

7.3 Asset Security

Removable assets (e.g. laptops, tablets, etc) must be secured using appropriate cable locking mechanisms when unattended or not in use and login passwords kept secure at all times.

Such removable assets will only be provided to certain individuals as approved by the Data Security Team and only after they have been trained in this policy and signed a receipt to the effect it has been read.

Staff will be responsible for protecting any device on which data is stored, including any laptop computer and/ or mobile telephone which has been issued to them in accordance with this policy and which may be used externally, including but not limited to keeping same in specifically designated cases or covers, not leaving same unattended at any time, and keeping them in safes/ secure holding places when not in use, including while travelling.

Core components of the APIC infrastructure, including servers, wireless access points, switches & copper/fibre lines, must be isolated from the general staff and protected with physical security mechanisms (e.g. locks, doors etc). Access to the core components is provided only when required, and only to personnel approved by the Data Security Team.

APIC Assets must be protected from tampering and/or misuse. Maintenance of APIC assets must only be performed by personnel as approved by the Data Security Team. All maintenance tasks must be logged in an equipment maintenance register maintained by Data Security Team.

7.4 Monitoring & Surveillance

APIC premises must be monitored using:

- a motion-detecting alarm system, outside of access hours; and
- closed circuit television monitoring of core infrastructure.

Access controls, including key cards/PIN codes must be inspected for misuse/tampering at least once every 12 months.

Access logs may be provided for the purpose of investigating security incidents.

Access logs must be kept for a minimum of 12 months, and video surveillance footage kept for a minimum of one month and may be internally reviewed or provided to an affected partner or investigative service provider, or police, for the purpose of investigating security incidents.

7.5 Financial Systems / Card Security

Any system or device that captures or stores financial information, including credit or debit card numbers, PIN codes and expiry dates, must be physically protected from physical access by unauthorised personnel.

8. Network/Systems Access

8.1 Access Control

APIC uses specific and tested software for the issuance of unique passwords and log-ins to restrict access to secured systems.

Users must access APIC systems, workstations, or servers using an authorised account. Accounts must be created by the Data Security Team, including by the use of approved software. Account privileges must be restricted only to functions required for the performance of the account holder’s role, and in consideration of the classification of information to which access is required by the account holder.

The role and permissions granted to each user of a secured systems must be reviewed at least once every 12 months by the Data Security Team to ensure that user is granted the minimum-required permissions to perform his or her function.

Access to SMS, LMS and file servers are restricted by “roles” whereby only certain functions/files are available based on the staff’s role within the group. Such “roles” and the associated access to be provided are subject to annual review.

8.2 External Access

APIC Staff and students may be permitted to access APIC Systems remotely. Remote access to APIC Systems must be performed:

- using a secure connection with a minimum 128-bit Advanced Encryption Standard (AES) or similar security standard as approved by Data Security Team from time to time; and
- using APIC Account credentials.

A vulnerability scan will be conducted on the externally-accessible systems at least once every 12 months. To facilitate scanning, a maintenance period will be enforced. During this maintenance period, no external access will be available.

Students accessing the SMS will require a unique user name and password in order to do so.

The ability to access the SMS will be restricted to current students only, once a person ceases to be a student of APIC, their account, log-ins and passwords will immediately be made invalid and access denied

9. Social Engineering Fraud

In order to prevent social engineering fraud, all student databases will be classified as confidential and access to same will be restricted only to personnel who require such access for the performance of their role.

The Data Security Team will undertake an annual review of the storage of all databases and access permissions.

In relation to any request, whether internal or from a third party, that would ordinary require a release of any such information, APIC will enter into a system of authenticity, whereby all such requests, when received in writing, will be verified via phone or similar prior to the release of information. Such information will not be transmitted via email in accordance with this Policy.

All staff will be trained on what social engineering fraud is, and be directed to treat any actual or suspected act of same as a high-risk security incident in accordance with this policy.

10. Phishing & Phreaking

In order to prevent Social Engineering Fraud, all Student databases will be classified as Confidential and access to same will be restricted only to personnel who require such access for the performance of their role.

The Data Security Team will undertake an annual review of the storage of all databases and access permissions.

The Data Security Team will investigate any ongoing unsuccessful attempt to log-in by any User of the APIC Systems, and will treat any suspicious or frequent failed attempts as a High Risk Security Incident in accordance with this policy.

Access to databases containing private or confidential information will be restricted only to specific personnel as approved by the Data Security Team.

All such databases or software containing private information of students or staff, including contact details, will be classified as confidential information, and kept secure.

The Data Security Team will be responsible for ongoing maintenance and review of all permissions granted to access any third party social media accounts or software accounts. Such access/ permissions and administrator appointments will be restricted only to those personnel for whom such access is required to perform their role.

The Data Security Team will regularly monitor all social media accounts for any unusual or suspicious conduct, and ensure in the event of same:

- The relevant social media or third-party software provider is notified immediately in the event of an actual or threatened data security breach; and
- The relevant incident is treated as a security incident in accordance with this policy.

In relation to any request, whether internal or from a third party, that would ordinarily require a release of any personal of confidential information, APIC will enter into a system of authenticity, whereby all such requests, when received in writing, will be verified via phone or similar prior to the release of information.

APIC will never request personal or financial information be provided by way of email from any third party, including its partners and students.

In the event any member of the Data Security Team is forwarded or otherwise provided an email, social media post or other communication (in whatever form) that appears to be an incidence of phishing, then:

- The Data Security Team will immediately verify with the CEO or other such personal as appropriate in the circumstance that the relevant communication is not and was not sent with the authority of APIC;
- The Data Security Team will cause to be issued a memorandum or email or alert (through whatever means) as soon as reasonably practicable to such persons as appear to be at threat as a result of such incidence confirming the nature of the threat, and requesting any further such communications be forwarded to a nominated member of the Data Security Team;
- Such communication will be treated as a 'high risk security incidence' in accordance with this policy; and
- If deemed appropriate, and an act of fraud has or appears to have taken place, the Data Security Team will report the incident to the police or other relevant body.

All staff will be trained on what phishing and phreaking is, and be directed to treat any actual or suspected act of same as a high-risk security incident in accordance with this policy.

11. Financial Transactions

All financial information of all parties will be treated as confidential information in accordance with this Policy.

Any transaction for a sum in excess of $2,000 will be co-authorised by a relevant member of staff, and a log kept of all such authorisations, before being processed.

The Data Security Team will ensure all financial information of APIC, its students, staff and partners will be treated as Confidential Information at all times, and access to same will only be provided to such staff as is reasonably necessary for them to perform their role.

The Data Security Team will out in place a system of review of all APIC bank records and transaction logs so as to monitor same for proper use.

Any actual or threatened leak of financial information of any party shall be treated as a High Risk Security Incident in accordance with this policy.

In the event of suspected or actual or threatened unauthorised access to the financial accounts of APIC or any of its students, staff and/ or partners, APIC will notify the relevant financial institution and/ or account holder and put in place such account freezes or similar as is necessary to protect the funds and Confidential Information.

12. Links to Other Sites

The Services (including SMS) may contain links to other websites. The fact that APIC may link to a website or present a banner ad or other type of advertisement is not an endorsement, authorisation or representation that we are affiliated with that third party, nor is it an endorsement of their privacy or information security policies or practices. APIC does not exercise control over third party websites. These other websites may place their own cookies or other files on APIC computers, collect data or solicit personal information from you. Other websites and services follow different rules regarding the use or disclosure of the personal information staff submit to them. APIC encourages all staff and students to read the privacy policies or statements of the other websites that they visit.

13. Third Party Software

The Data Security Team will ensure, in relation to any third-party software used on the APIC system or devices are free from viruses, only made accessible to such persons as are reasonably required to access the system to perform their role, that all security or other updates are undertaken by the Data Security Team and that measures are put in place to ensure any end-user of any item of software complies with that software providers terms and conditions.

14. Password and Username Issuance

Each User will receive a username and password, which password must be changed by each user every 45 days. It is the user’s responsibility to keep its account details confidential, including username and password. The user is liable for all activity on its account. The user agrees that it will not disclose its password to any third party and that it will take sole responsibility for any activities or actions under its account, whether or not it has authorised such activities or actions. The user will change its password regularly.

14.1 Passwords

All passwords used on APIC systems must follow the guidelines as outlined in the below table:

System/account type	Information Access Level	Requirements
Network Access	Unrestricted	No minimum requirements.
	Restricted	Complex password with a minimum of 8 characters.
	Confidential	Complex password with a minimum of 8 characters, and restricted.
Servers	All	Complex password with a minimum of 8 characters.
Privileged Accounts	All	Complex password with a minimum of 8 characters, and restricted.

Users must not disclose their passwords to any other person for any purpose.

15. Antivirus & Anti-Malware

All APIC workstations and services must use antivirus and anti-malware software as directed by the Data Security Team. Antivirus and anti-malware software is centrally managed, and must be kept up-to-date, with updates checked daily.

Only APIC personnel with administrator access are permitted to alter, disable, or remove anti-virus or anti-malware software upon approval by the Data Security Team.

16. Data Backup & Recovery

Data stored on APIC servers and workstations is required to be backed up in accordance with the following schedule:

Device	Backup Schedule	Storage period
Servers	Nightly	1 week
	Nightly	30 Days

16.1 Data Loss Prevention

Data loss prevention is a key aim of this policy. Key elements of APIC's data loss prevention strategy include:

- encryption, of data stored on or in transit to or from APIC workstations, servers;
- maintenance of up-to-date software, including antivirus software;
- control of access to APIC's network/systems;
- data backup and recovery;
- security vulnerability testing, monitoring, and reporting; and
- maintenance of event logs.

17. Security Incident Response Procedure

17.1 What is a Security Incident?

A security incident is an event resulting in:

- violation of this policy;
- unauthorised access, disclosure, disruption, modification, destruction, or theft of data stored on or transmitted to or from a APIC System, including the LMS and SMS; or
- an increased risk of unauthorised access, disclosure, disruption, modification, destruction, or theft of data stored on or transmitted to or from a APIC System.

Examples of security incidents include:

- 'hacking' by a third party of a APIC system;
- theft of an APIC asset;
- phishing;
- phreaking;
- unauthorised access to an APIC premise; and

- inadvertent or unintended disclosure or erasure of data.

17.2 Reporting & Documentation

It is the responsibility of all APIC staff to immediately report all security incidents upon a becoming aware that a Security Incident has occurred.

Security Incidents must be recorded with:

- an Initial Incident Report, provided to the Data Security Team by the APIC staff member or team who identified the incident;
- a severity assessment, performed by the Data Security Team;
- a resolution plan, prepared by the Data Security Team/other APIC staff or teams as applicable;
- an incident report, prepared by the Data Security Team which outlines what occurred, how it was resolved, and the steps taken to prevent further similar incidents.

17.3 Notification to Affected Parties

APIC recognises that in the event of a security incident, student data, including data provided by APIC Partners may be accessed without authorisation. All affected parties including APIC partners must be notified in accordance with the security incident response procedure.

Affected APIC partners may request involvement in investigation into any security incident to which they have been affected, subject to approval by the Executive Management Team.

17.4 Security Incident Classification

Security incidents must be classified and addressed in accordance with the below table:

Severity	Description	Containment Time	Target Resolution Time
High	Unauthorised access, disclosure, disruption, modification, destruction, or theft of restricted or confidential information has occurred. Any actual or suspected incidence of phishing and/ or phreaking.	Within 6 hours	12 Hours
Medium	Unauthorised access, disclosure, disruption, modification, destruction, or theft of restricted or confidential information may have occurred. Unauthorised access, disclosure, disruption, modification, destruction, or theft of Unrestricted information has occurred.	Within 12 hours	48 Hours
Low	Unauthorised access, disclosure, disruption, modification, destruction, or theft of unrestricted information may have occurred.	Within 48 hours	1 week
Non-Incident Event	No security breach has occurred.	N/A	1 week

18. Users of APIC IT

Each staff member and student of APIC is an authorised user of its IT services and facilities, and is responsible for:

- The use of the IT in accordance with this, and any related, policy at all times;
- Immediately report any known or suspected cyber security incident or threat, including any breach or potential breach, to the Group Manager, Technology and Innovation and the Data Security Team;
- Ensuring they are aware of the security requirements of the IT they use and take appropriate action to protect their access of these systems against unauthorised users;
- Signing out of all their user accounts when they will not be in use for an extended period time, including the SMS and LMS;
- Not use emails for the transmission of restricted or confidential data;
- Clear the downloads folder on the computer they are using at regular intervals; and
- Clear all contents from USB drives when they are finished using them, and return the USB to a secure place.

19. Document Change Control

Version	Change Description	Date	Author
1.0	New policy development	12 September 2017	Cesar Muradas
2.0	Small changes to improve clarity	30 November 2017	Corinne Green