Cyber Security Policy and Procedure

CONTENTS

1 Purpose

This document sets out Polytechnic Institute Australia's (PIA) policy on cyber security and provides the foundation for cyber security management within the organisation.

2 Scope

This Policy applies to:

- All authorised users of PIA's IT facilities and services; and
- PIA's information in any medium or form such as electronic or printed paper.

3 Policy statement

It is the aim of PIA to be more resilient to cyber-attacks and better able to protect its interests in the digital environment. It is committed to ensuring all activities involving information technology are appropriately defended against cyber security threats.

Effective cyber security requires an organisational approach to ensure each responsible entity has the procedures, tools and support required to undertake its business effectively while managing the risk of adverse security incidents and events.

This Policy supports the Board of Directors and its committees in demonstrating that cyber security risks and measures are being identified and managed in a way that is appropriate for the organisation in trying to meet its business objectives.

4 Policy principles

- All PIA's IT facilities and services will be protected by effective management of cyber security risks.
- Use of IT facilities and services must comply with PIA's policies and relevant legislation.
- PIA will have sufficient IT to facilitate the effective implementation of cyber security controls across all IT infrastructure, systems and applications.

- All access to PIA's IT facilities and services must be authorised, restricted on the basis of need, and periodically verified.
- The effectiveness of the PIA's management of cyber security risks will be regularly assessed and improved.
- The cyber security response and recovery plans, via the Business Continuity Plan, will be maintained, tested, and periodically improved.

5. Responsibilities

COO/ IT Manager has the following responsibilities:

- ensuring all authorised users comply with the policies and procedures around 'acceptable use' of the organisation's IT facilities and services;
- ensuring effectiveness of cyber security measures through monitoring programs;
- ensuring effectiveness of disaster recovery plans through a program of testing;
- approving complementary operational procedures to support this policy;
- approving the isolation or disconnection of any equipment or IT facility from the network which poses a severe and unacceptable risk; and
- reporting to appropriate governance bodies including the Quality Assurance and Risk Committee on risks pertaining to cyber security.

Quality Assurance and Risk Committee has the following responsibilities:

- monitoring cyber security risks and controls by reviewing the outcomes of cyber risk management processes and monitoring emerging risks; and
- reporting to the Board of Directors on risks pertaining to cyber security capability and controls.

Users of IT Facilities and services have the following responsibilities:

- using IT facilities and services according to IT policies at all times;
- being aware of the security requirements of the IT facilities and services they use, and take every precaution to safeguard their access to these systems against unauthorised use;
- immediately reporting any known or suspected security incidents and breaches to the COO/IT Manager; and
- not communicating the cyber security risks, controls, events and incidents outside the institution except where required or authorised to do so by law or PIA's policy or procedures.

5 Definitions

Acceptable Use – means those behaviours and actions, in connection with the use of the organisation's IT facilities and services, which are permitted under the Information Technology Usage Policy and Procedures.

Authorised User – any authorised person using any of the IT facilities and services.

Cyber security – the practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification or destruction.

Cyber Security Policy and Procedure

Cyber risk – refers to any risk of financial loss, disruption or damage to the reputation of an organisation resulting from the failure of its information technology systems.

Cyber threat –is deemed any malicious act that attempts to gain access to a computer network without authorisation or permission from the owners.

IT facilities and services – Information Technology facilities operated by or on behalf of the organisation. This includes services and systems and associated computing hardware and software used for the communication, processing and storage of information.

6 Related legislation and documents

Data Breach Response Procedure
Information Technology Usage Policy and Procedures
Privacy and Personal Information Policy and Procedure
Records Management, Security, Retention and Disposal Policy and Procedure
Risk Management Policy
Risk Management Framework
Staff Code of Conduct
Student Code of Conduct and Disciplinary Procedures

7 Feedback

PIA staff and students may provide feedback about this document by emailing policy@pia.edu.au.

8 Approval and review details

Approval and Review	Details
Approval Authority	Board of Directors
Administrator	COO / IT Manager