IT Security

1. Purpose

This policy establishes the framework for protecting CBIP's information systems, data, and digital assets from unauthorised access, loss, misuse, or damage in compliance with the NZ Privacy Act 2020 and ISO 17024 2012.

CBIP's security framework ensures confidentiality, integrity, and availability of information in alignment with New Zealand legal and regulatory obligations.

2. Scope

This policy includes office-based and remote access to CBIP system and applies to all:

- Candidate and member personal information including examination results, certification records, identity data
- Personal information of CBIP personnel including contractors, Board members, and other authorised users of CBIP's systems
- IT systems, devices, networks, and software used for CBIP business
- data created, stored, processed, or transmitted by CBIP
- third-party service providers handling CBIP data.

Also refer to CBIP's Privacy Policy.

3. Definitions

For the purposes of this policy:

Confidential Information

Any sensitive or private information relating to CBIP, its members, staff, or stakeholders.

Cybersecurity Incident

Any event that compromises data, systems, or network security (e.g. hacking, malware, data breach).

Information Systems

All hardware, software, networks, and cloud services used by CBIP.

Multi-Factor Authentication (MFA)

A security method requiring more than one form of verification.

Privacy Breach

A privacy breach includes unauthorized access or disclosure, accidental release of information, loss of person data (devices, emails, files), and inability to access data e.g. ransomware.

User

Any person authorised to access CBIP systems.

4. Responsibilities

4.1 Governance Board

The Board has overall accountability for information security governance. It is responsible for:

i. ensuring adequate resources to implement CBIP's IT security policy and procedures

ii. assessing and managing IT Security risks in accordance with CBIP's Risk Management Plan

iii. responding to all privacy breaches promptly

iv. determining whether a breach is notifiable under NZ law

v. notifying the Privacy Commissioner and affected individuals where required

vi. investigating and preventing recurrence of all security incidents.

4.2 Operations Manager

The Operations Manager is responsible for:

i. notifying the Board immediately of any security incident

ii. implementing security controls and liaison with CBIP's IT security provider(s)

iii. making CBIP personnel aware of their responsibilities regarding privacy and IT security

iv. ensuring that electronic information is destroyed in a way that ensures the data cannot be recovered, reconstructed, or accessed by unauthorised parties.

4.3 Users

All users must:

i. comply with this policy

ii. protect login credentials and devices

iii. report any suspected security incidents promptly.

4.4 IT Service Providers

IT service providers must:

i. maintain systems in accordance with security best practice

ii. monitor and respond to security threats as agreed in the service contract

iii. assist CBIP with the secure sanitation and destruction of electronic information when required.

5. Policy

5.1 CBIP is committed to maintaining a secure IT environment. The Board will ensure that any actual or suspected information security breach involving candidate or member data is promptly identified, reported, contained, investigated and resolved.

5.2 Appropriate notifications will be made to regulatory authorities, affected individuals and NZ's Privacy Commissioner in accordance with applicable legal and accreditation requirements. Under NZ law, a breach is notifiable if it causes or is likely to cause serious harm. Such notifications must only be made by CBIP's Board Chair or his/her nominee. Refer to CBIP's Privacy Policy.

5.3 Access Control

i. All users must have unique login credentials.

ii. MFA must be used where available.

5.4 Password Management

i. Strong passwords must be used and updated regularly.

ii. Passwords must not be shared.

iii. Approved password managers may be used.

5.5 Device Security

i. All devices must have approved security software installed.

ii. Operating systems and applications must be kept up to date.

iii. Lost or stolen devices must be reported immediately.

5.6 Data Protection

i. Confidential data must be stored securely.

ii. Data must be backed up regularly.

iii. Encryption must be used where appropriate.

5.7 Email and Internet Use

i. Users must be vigilant against phishing and scams.

ii. Suspicious emails must be reported.

iii. CBIP systems must not be used for unlawful activities.

5.8 Destruction of Electronic Information

i. Electronic information will be destroyed according to its classification level:

- Public – recycle bin, emptied at least monthly
- Internal – recycle bin, emptied at least monthly
- Confidential – clauses 5.8 ii and iii that follow.

ii. Electronic files must be securely erased using approved software tools that overwrite data to prevent recovery (as advised by IT service provider)

iii. Mobile phones and tablets must be factory rest and securely wiped before disposal or reassignment

5.9 Incident Management

i. All suspected cybersecurity incidents must be reported **within 1 hours of discovery**.

ii. Incidents will be investigated and managed in accordance with CBIP Incidents and Improvements policy.

6. Procedure

6.1 Any person: Immediately report suspected security breach to the Operations Manager (Privacy Officer) or Board Chair.

6.2 Operations Manager, as appropriate for the breach and in liaison with CBIP's IT Service provider(s):

i. isolate affected system(s)

ii. disable compromised accounts

iii. retrieve or secure disclosed information where possible

iv. prevent further access

v. notify the Board Chair

vi. record the incident.

6.3 Board Chair or Board Nominee:

i. Notify affected individuals in writing

ii. Include:

- What happened
- What information was involved
- Steps taken to resolve and prevent recurrence
- What they should do
- Contact details

7. Record Management

The following record must be maintained for compliance purposes:

Record	Filed	Retention
Security Incident Reports	CMS: One Drive	3 years
System backup logs	Mini Mac Hard drive	Weekly
IT Service Provider Agreement	CMS: One Drive	Length of service provision
Risk Assessment and Management Plan	CMS: One Drive	Indefinite. Updated annually

8. Quality Standard

ISO/IEC 17024, 2nd edition, clauses:

- 7.3 Confidentiality
- 7.4 Security

9. Revision History

This is a new document.