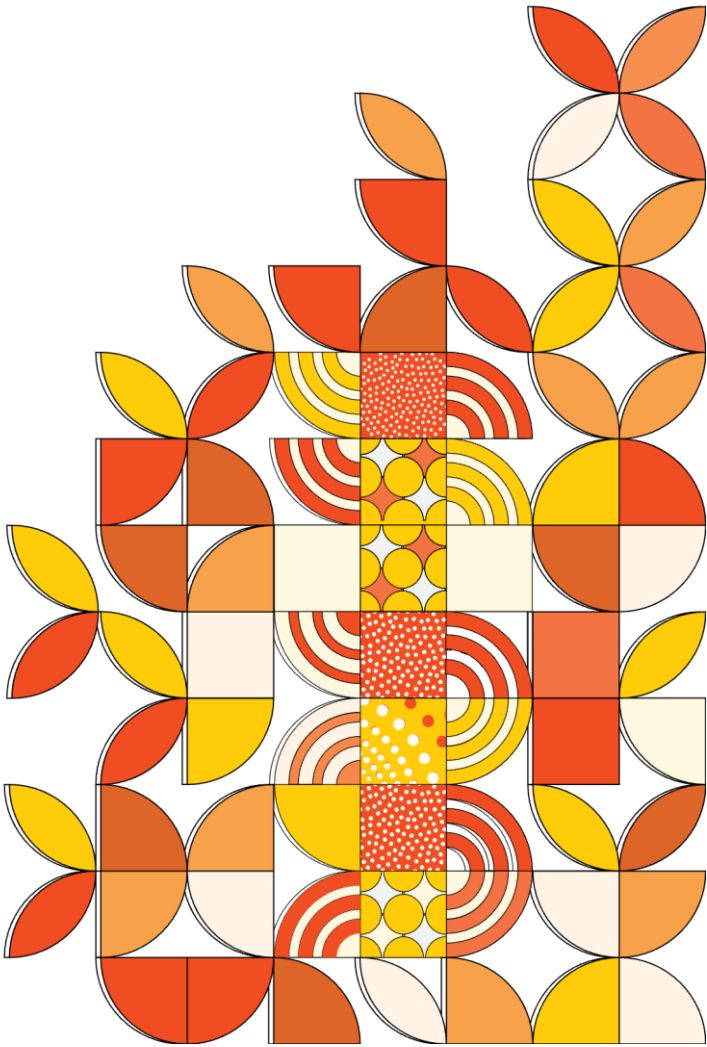
Legal entity: INSTITUTE OF HEALTH & MANAGEMENT PTY LTD.
Category: Institute of Higher Education
CRICOS Provider: 03407G| Provider ID: PRV14040
ABN: 19 155 760 437 | ACN: 155 760 437

# Cyber Safety and Security Procedure



www.ihm.edu.au
enquiry@ihm.edu.au

EDUCATION for EMPLOYMENT:
Bridging the gap globally

# SECTION 1

## Purpose

1. The purpose of this procedure is to provide a systematic approach to implementing the Cyber Safety and Security Policy at the Institute of Health & Management (IHM).
2. This includes guidelines for password management, email security, social media use, handling sensitive data, and incident response.

## Scope

3. This procedure applies to all staff, students, and stakeholders, including members of governance committees involved in the teaching, implementation, and support of IHM-accredited courses and non-award offerings.

## Definitions

4. Definitions for key terms are presented in the Glossary of Terms.

## Suite documents

5. This Policy is linked to the following:
   a) Cyber Safety and Security Policy
   b) See also Associated Information listed in the 'Related Internal Documents' in Section 3 below.

# SECTION 2

## Procedure

6. **Password Management: Setting Password Requirements**
   6.1 Passwords protecting private or confidential data must be updated at least once every three months.
   6.2 Use complex passwords combining uppercase and lowercase letters, numbers, and special characters.
   6.3 Avoid common names and easily predictable elements.
   6.4 Implement Multi-Factor Authentication (MFA) and authentication apps like MS Authenticator.

7. **Email Security: Enhancing Email Security**
   7.1 Use firewalls to monitor and control email traffic and filter malicious content.
   7.2 Regularly update firewalls and configurations to defend against threats.

8. **Detecting Unauthorised Access**

   8.1 Monitor for signs like incorrect passwords, unusually sent emails, unexpected password resets, unauthorised device logins, and notifications from Have I Been Pwned.

9. **Responding to Email Compromises**

   9.1 **Internal Reporting**: Report incidents to the Head of Digital Transformation, Reporting Manager, and IT Support email (itsupport@hci.edu.au).

   9.2 **External Reporting**: Contact financial institutions and report to the Australian Cyber Security Centre (ACSC) through Report Cyber. Keep track of the Report Reference Number and any actions taken.

10. **Protecting Against Fraud and Security Breaches**

   10.1 **Multi-Factor Authentication**

   a) Enable MFA for all accounts.

   b) IHM recommends Microsoft Authenticator to be the default authentication method.

   10.2 **Domain Protection**

   a) Regularly renew domain names to prevent scammers from acquiring them.

   b) Consider registering similar domain names to prevent spoofing.

   10.3 **Email Authentication**

   a) Implement email authentication measures to prevent email spoofing.

   b) Refer to ACSC's How to Combat Fake Emails.

   10.4 **Privacy Protection**

   a) Limit online sharing of personal information to reduce the risk of targeted cyber-attacks.

   b) Follow guidelines from the Office of the Australian Information Commissioner (OAIC).

   10.5 **Training and Awareness**

   a) Conduct regular cybersecurity training to help staff recognise and avoid phishing and scam attempts.

11. **Handling Sensitive Data: Data Management**

   11.1 Discuss sensitive information only when necessary and ensure physical files are stored securely.

   11.2 Properly label and destroy sensitive data when no longer needed.

12. **Handling Technology: Device Management**

   12.1 Store devices securely when not in use.

   12.2 Report theft or loss of devices immediately.

12.3 Regularly update devices with system upgrades and security patches.

12.4 Use antivirus software and check removable media before use.

13. **Social Media and Internet Use: Usage Standards**

13.1 Share only appropriate information on social media.

13.2 Use work email accounts responsibly.

13.3 Follow guidelines for internet and social media usage while at work.

14. **Incident Response Plan**

14.1 **Preparation**

a) Prepare staff and systems to handle cyber incidents through policies and training.

b) Identify critical assets and potential risks.

14.2 **Detection**

a) Monitor for unusual activities like inaccessible accounts, missing data, or unexpected system behaviour.

b) Report incidents to the Head of Digital Transformation or IT Support (itsupport@hci.edu.au) immediately via email with all supporting information.

14.3 **Response**

a) Isolate affected systems to prevent further damage.

b) Eliminate threats and restore systems.

c) Notify contacts and relevant third parties of the incident.

14.4 **Review**

a) Review and improve procedures based on lessons learned from incidents.

15. **Regular Updates and Reviews: Maintaining Up-To-Date Procedures and Policies**

15.1 The Digital Transformation Department will regularly review and update the cybersecurity policy and procedure.

# SECTION 4

## Associated Information

| | |
|---|---|
| **Related Internal Documents** | Bullying and Harassment Policy<br>Bullying and Harassment Procedure<br>Cyber Safety and Security Policy<br>Marketing of Courses to Overseas and Offshore Students Policy<br>Marketing of Courses to Overseas and Offshore Students Procedure<br>Privacy Policy<br>Privacy Procedure<br>Social Media Policy<br>Social Media Procedure |
| **Related Legislation, Standards, and Codes** | Victoria's Cyber Strategy \| vic.gov.au (www.vic.gov.au)<br>Information Security Manual (ISM) \| Cyber.gov.au<br>Victorian Information Privacy Act (2000)<br>Federal Privacy Act (1988), |
| **Date Approved** | 02.08.2024 |
| **Date of Effect** | 03.08.2024 |
| **Date of Next Review** | 30.07.2027 |
| **Approval Authority** | Audit and Risk Committee<br>Endorsed by Board of Directors |
| **Responsibility for implementation** | Digital Transformation Department |
| **Document Custodian** | Head, Digital Transformation Department |
| **IHM Doc ID** | IHM-CSSP-2.0 |

## Change History

| **Version Control** | | |
|---|---|---|
| **Change Summary** | Date | Short description of change, incl version number, changes, who considered, approved etc |
| Version 1.1 | 22/02/2013 | Ratification by Board of Governors |
| Version 1.2 | 23/11/2013 | Version 1.2 approved by Board of Governors |
| Version 2.0 | 2/08/2024 | • Policy and Procedure are separated into two documents<br>• The definitions relocated to the glossary of terms<br>• Template updated<br>• Major update on password management, email security, protecting against fraud and security breaches, handling sensitive data, handling technology, social media and internet use, incident response plan |