# Information Security Policy

## 1. PURPOSE

To define the information security framework and principles to protect information from unauthorised use or accidental modification, data loss or public release.

## 2. SCOPE

This policy applies to:

- All users of Holmesglen Information Assets and systems.
- Third parties who have access to Holmesglen's Information Assets or systems where their contract of engagement provides explicit access to Information Assets or systems.
- All Institute Information Assets and information systems regardless of location.
- Asset owners concerning the assets that they own.

## 3. POLICY STATEMENT

Holmesglen collects and maintains a vast amount of information (data) as part of its operational activity. Holmesglen recognises its duty to protect and manage the risks associated with Information Assets and information systems.

Holmesglen recognises the following four core principles of Information Security:

- **Confidentiality** – To protect against the unauthorised disclosure of information and to ensure that information is only accessible to those with authorised access.
- **Integrity** – To protect against information errors or unauthorised loss or modification of information and safeguarding the accuracy and completeness of information.
- **Availability** – To ensure that the business systems will be available to support operational activity. Authorised users have access to information when required.
- **Accountability** – To ensure that appropriate controls are in place so that users have access to accurate, relevant and timely information and Holmesglen complies with all legal and contractual obligations.

Further, Holmesglen requires all users to comply with this Information Security Policy and related procedures. Any Information Security breach is investigated and may be subject to disciplinary action.

## 4. PRINCIPLES

4.1 Appropriate controls are incorporated into human resource management to minimise the risk of loss or misuse of Information Assets, including but not limited to:

(i) Implement induction and ongoing training, to ensure all employees are aware of and acknowledge Holmesglen's Information Security Policy.

(ii) Document and assign security roles and responsibilities where employees perform specific Information Security related roles, and ensure that security clearance requirements are addressed, in recruitment, selection and in job descriptions; and

(iii) Implement procedures for the separation of employees from Holmesglen to ensure that network access and access to Information Assets are disabled.

4.2. Information Asset Responsibility:

(i) Holmesglen ensures its Information Assets are:

- documented in an Information Asset Register,
- classified and assigned to Information Asset Owners,
- assigned a business impact level value and an appropriate classification, and

- protected from internal and external threats.

(ii) Information Assets holding personally identifiable or public sector data must have an associated System Security Plan or Security Risk Assessment.

(iii) The creation, storage and processing of information only occurs on approved ICT assets.

(iv) Four mission-critical Information Assets and their respective owners are identified as below:

| Information Asset | Information Asset Owner |
|---|---|
| Corporate Governance, Quality, Risk and Strategy Data | Chief Executive |
| Financial Data, Assets and Audit Data | Chief Financial Officer |
| Human Resource Data | Associate Director Human Resources Operations |
| Curriculum, Academic Data, Educational Resources & Research Data | Executive Director Education and Applied Research |
| Other Student Data, Marketing and Communication Data | Executive Director Engagement and Support. |
| Industry and Community Engagement information, International Student Programs | Executive Director People, Global Relations and Industry Engagement |
| Capital Works, ICT, Facilities, campus safety and contractor management data | Executive Director Corporate and Commercial Services |

*Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the Information Asset Owner.*

4.3. Information Asset Owners ensure each asset owned is classified in accordance with the Information Classification Scheme in the table below.

| Classification | Definition |
|---|---|
| **PROTECTED** | Information Assets that contain important and sensitive information, that if compromised could cause significant harm or life threatening injury to an individual or damage to the organisation and the government. |
| **OFFICIAL: Sensitive** | Information Assets that contain sensitive materials, when disclosed have the potential to harm, lead to discrimination, mistreatment, humiliation or undermining an individual's dignity or safety. Can cause damage to Holmesglen reputation, operations capability and service delivery. |
| **OFFICIAL** | Information Assets necessary for Holmesglen business and intended only for use by employees and approved non-employees such as contractors, vendors, or learners. |

| | |
|---|---|
| **Unofficial** | Information Assets that do not need a protective marking and may be approved for unlimited public release. |

4.4. Holmesglen has procedures in place for the use of portable or mobile devices, removable media, personal storage devices and the use of cloud services, taking into consideration the adopted Information Classification Scheme.

4.5. Access Control

(i) Users are authenticated when accessing Information Assets classified as **Official** and above. Asset owners determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated Information Security risks.

(ii) Physical access controls are deployed for information assets classified as **Official: Sensitive** and above.

(iii) The principle of Least Privilege will be the basis of all access control rules.

(iv) Users are made aware of their responsibilities concerning safeguarding their authentication information. For example, sharing of passwords, writing passwords down on paper – would constitute a breach of this policy.

Holmesglen does not implement non-individual authentication information, such as generic IDs unless authorised by the Chief Information Officer.

4.6. Physical Security of Equipment

(i) Holmesglen ensures that critical infrastructure (such as server rooms, communications closets and other TSD secure areas) are protected via physical barriers such as keyed or electronic access control.

(ii) Technology equipment, where possible, has a Holmesglen Asset Tag (E number) affixed before being deployed. Physical restraints (such as Kensington Locks) are used where appropriate. Portable or mobile devices (netbooks, laptops and tablets) are, where possible, permanently marked or engraved, clearly indicating Holmesglen ownership, before being deployed.

4.7. Standard Operating Environment (SOE)

(i) Holmesglen develops, maintains and deploys a base SOE image that incorporates hardening techniques and controls including, but not limited to:

- disabling services not required by Holmesglen,
- removing administrative rights from users,
- disabling the ability for users to install software, and
- disabling the ability for users to turn off or defeat virus and malware protection.

Application deployment via an application launcher is incorporated in the base SOE. Specific applications critical to the Institute are launched upon approval from the Information Asset Owner.

(ii) Holmesglen develops, maintains and deploys a base server SOE image which incorporates hardening techniques commensurate with the asset classification and the security risk. System Administrators log in to servers using a different set of credentials than their day-to-day login credentials.

4.8. Mission-critical applications must have both a development and production environment; with controls in the development environment to limit the amount of access to select users only. Development and change procedures must be followed to move software or changes into production environments.

4.9. Holmesglen implements a clear desk and clear screen policy to reduce the risks of unauthorised access, loss of and damage to information during and outside normal working hours. Safes or other forms of secure storage are also utilised to protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

4.10. Holmesglen employs a number of methods to detect and mitigate risks from cyber threats. Upon detection of a cyber-threat, all exposed information assets are protected from repeated attempts or threats.

4.11. Holmesglen applies the Australian Government's policy position and will not make ransom payments to cybercriminals. Holmesglen takes proactive steps to understand the threat environment and ensures its standard operating procedures and controls to prepare, prevent, respond and recover from a ransomware attack are aligned to government advice and its legislative and regulatory obligations.

4.12. All devices connecting to the Holmesglen network must have appropriate virus and malware protection. Institute owned devices have virus and malware protection installed as part of the Standard Operating Environment. Institute owned mobile devices have virus and malware protection capable of being updated without the need to connect to the Holmesglen network.

4.13. Adequate Intrusion Protection safeguards are in place and are capable of physically or logically separating public access from protected networks and information assets. The Holmesglen wireless network is logically separated from the corporate wired network at all times.

4.14. Vulnerability management process is implemented to deploy patches to Information Systems and other devices. Patch deployment only occur after recommendation by the vendor. Prior to the patch being deployed in the live system, extensive testing (User Acceptance Testing) occurs in the test environment. Fall back contingency processes are also identified.

4.15. Standard operating procedures and controls are documented and implemented to ensure that all Information Assets are managed securely and consistently, in accordance with the level of required security, including:

- Operational change management procedures and release procedures are implemented to ensure changes to Information Assets or Information Systems are approved and managed;
- System capacity is regularly monitored to ensure risks of system overload or failure which could lead to a security breach are avoided;
- Comprehensive systems maintenance processes and procedures including operator and audit/fault logs, backup procedures and archiving are implemented;
- Each employee must use the authorised and supplied communications methods, including electronic mail and SMS messaging while undertaking Holmesglen business; and
- Access to electronic mail and SMS messaging is via the use of user credentials and when accessed from the Internet, transported under a Secure Hypertext Transport Protocol (HTTPS).

4.16. Holmesglen is committed to maintaining the confidentiality, integrity and availability of information assets. Therefore, all changes to information systems, software, or infrastructure must adhere to the established change management process. This process encompasses thorough planning, assessment of potential security impacts, testing, approval, implementation, notification of any planned disruptions or outages and documentation of changes. The change management process is designed to mitigate risks associated with changes and ensure that security controls remain effective.

Information asset owners utilising third parties for the delivery of information technology services are required to adopt and follow the change management processes offered by the third-party vendor.

4.17. Holmesglen identifies and mandates Information Security controls to address supplier access to Holmesglen's information. These controls identify processes and procedures that Holmesglen requires the supplier to implement.

4.18. Holmesglen manages and responds to Information Security incidents effectively by establishing and maintaining an Information Security incident and response register and recording all incidents; and ensuring:

- All Information Security incidents are reported and escalated (where applicable) through appropriate management channels and authorities;
- Information Security incidents are investigated and if it is found that a deliberate Security violation or breach has occurred, apply formal disciplinary processes; and
- Responsibilities and procedures for the timely reporting of security events and incidents are communicated to all Holmesglen users.

4.19. Holmesglen ensures that all media likely to contain information classified as **Official** or higher is sanitised before reuse or physically destroyed.

4.20. Emerging Technologies and AI

Holmesglen recognises the increasing role of emerging technologies, including Artificial Intelligence (AI), in the information security landscape. In accordance with the Office of the Victorian Information Commissioner (OVIC) guidelines, the following principles and practices are established:

- **Transparency and Accountability:** Holmesglen commits to transparency in the use of AI technologies, ensuring that stakeholders are informed about the purposes, capabilities, and limitations of AI systems employed within the organization. Additionally, accountability mechanisms are implemented to monitor and assess the ethical implications of AI applications.
- **Fairness and Non-Discrimination:** AI algorithms and systems utilised by Holmesglen adhere to principles of fairness and non-discrimination. Outputs generated by AI must not be used to formulate decisions, undertake assessments, or used for other administrative actions that may have consequences for individuals.
- **Data Privacy and Protection:** Compliance with the Privacy and Data Protection Act 2014 (Vic) prohibits the use of personal information with generative artificial intelligence platforms. Breach of this act will be treated as an information security incident and reported immediately to OVIC.
- **Security and Resilience:** AI-enabled systems are designed and operated with security and resilience in mind. Holmesglen implements measures to mitigate cybersecurity risks associated with AI, including vulnerability management, threat detection, and incident response capabilities.
- **User Empowerment and Education:** Holmesglen empowers users with knowledge and skills necessary to interact with AI technologies safely and responsibly. Training programs and awareness initiatives are conducted to educate stakeholders about AI-related risks, best practices, and ethical considerations.

## 5. ACCOUNTABILITIES

| Action | Accountability |
|---|---|
| ▪ Be aware of, understand and comply with this Policy.<br>▪ Notify any breaches (or suspected breaches) of Information Security to the TSD Helpdesk. | All users |
| ▪ Provide input into the risk management process for Information Security.<br>▪ Provide input into the development and content of guidelines and procedures where appropriate. | Chief Information Officer |

| Action | Accountability |
|---|---|
| ▪ Responsible for establishing data governance policies and practices related to privacy, information security and AI data usage.<br>▪ Provide oversight and guidance on AI projects, ensuring that data ethic and compliance consideration are addressed throughout the AI lifecycle. | Privacy and Data Protection Committee |
| ▪ Ensure Holmesglen's Information Security is compliant with relevant legal, auditory, regulatory and contractual obligations. | Executive Director Corporate and Commercial Services |
| ▪ Determine appropriate classifications of information.<br>▪ Determine appropriate logical and physical access controls.<br>▪ Develop and maintain a System Security Plan or Risk Profile Assessment.<br>▪ Ensure business continuity plans are in place for systems. | Information Asset Owners |
| ▪ Provide and manage the technical infrastructure to provide security protection.<br>▪ Maintain the Information Security related policies and procedures.<br>▪ Undertake an annual review of Information Security training requirements for TSD employee.<br>▪ Ensure Information Security personnel resourcing is aligned with the Holmesglen's requirements.<br>▪ Undertake investigations around security violations and breaches.<br>▪ Report security violations and breaches to the Executive Team and authorities.<br>▪ Provide input into the risk management process for Information Security.<br>▪ Provide input into the development and content of guidelines and procedures where appropriate.<br>▪ Provide oversight of technology related to initiatives involving implementation and management of AI systems. | Chief Information Officer |
| ▪ Ensure Information Security incidents and breaches that occur in their area are reported.<br>▪ Maintain local Business Continuity Plans to operate in the event of a disaster or Information Security incident. | Managers |
| ▪ Maintain standards and architecture for security technologies.<br>▪ Ensure security controls are applied in accordance with the information classification associated to it by the Information Asset Owner, including applying appropriate IT security access controls, SOE hardening and ensuring backup and recovery procedures are in place.<br>▪ Provide research, guidance, advice and recommendations on Information Security.<br>▪ Assist with internal and external audits and conducting risk management assessments. | Infrastructure Manager (TSD) |
| ▪ Implement the Information Security Policy and related codes of practice on information systems. | Information System Administrators |

| Action | Accountability |
|---|---|
| - Monitor and report the security of the information systems under their technical control. | |

## 6. DEFINITIONS

| Term | Meaning |
|---|---|
| Artificial Intelligence | Platform that uses natural human-like language to respond to a prompt from a user to generate new content. The platform generates outputs based on patterns it has learned, and responds accordingly with its informed guesses and prediction of preferred or acceptable word order. |
| Clear Desk Policy | Requires all users to clear their desks of all “Internal” and “Confidential” information when they leave their work area. |
| Clear Screen Policy | Requires all users to lock their computer screen when leaving their work area for a period of time. |
| Cloud Services | Internet-based services – such as Dropbox or other Software As A Service (SAAS) – external to Holmesglen. |
| Information Asset | An identifiable collection of data including, but not limited to: paper documents, databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans and archived information. |
| Information Security | The practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. |
| Information System | A system composed of people and computers that processes or interprets information. |
| Least Privilege | Allocating minimal user privileges on computers, based on users' job roles and necessities. |
| Manager | The person who is responsible for the operations of a faculty, department, centre, unit or another functional area within Holmesglen. |
| Personal Media Devices | Includes, but is not limited to, removable media, portable hard drives and portable SSD storage. |
| Removable Media | Includes, but is not limited to, USB flash drives/keys, SD Cards, CDs/DVDs and personal media devices. |
| Mobile Devices | Includes, but is not limited to, smartphones and tablets, laptops and netbooks. |
| Third party vendor | Includes the engagement of service providers to provide information technology services including support services for information assets (and systems) held on premise and Software as a Service (SaaS). |
| Users | All employees or learners, or any other persons who uses Holmesglen’s facilities, including a contractor and any employee or agent of a contractor. |

## 7. CONTEXT AND/OR REFERENCED DOCUMENTS

**Internal**

Access Control Policy

Conduct Rule

Employment Policy

Holmesglen Code of Conduct

ICT Acceptable Use Policy

TSD: Standard Operating Procedures

**External**

AS ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security controls

Privacy and Data Protection Act 2014 (Vic)

Copyright Act 1968 (Cth)

Health Records Act 2001 (Vic)

Public Records Act 1973 (Vic)

Electronic Transactions Act 2000 (Vic)

Victorian Protective Data Security Framework V2.0

## 8. REVIEW

8.1 This policy must be reviewed no later than three years from the date of approval.

8.2 The policy will remain in force until such time as it has been reviewed and re-approved or rescinded. The policy may be withdrawn or amended as part of continuous improvement prior to the scheduled review date.

## 9. VERSION HISTORY

| Version Number | Date | Summary of changes |
|---|---|---|
| 101 | Mar 2016 | New policy. |
| 102 | November 2017 | Minor changes to reflect PDPA requirements and position title changes. |
| 1 | August 2018 | Translated from the former policy in accordance with the Rule for Governance Framework. |
| 2 | July 2021 | Minor changes to information classification in accordance with the VPDSF V2. |
| 3 | June 2022 | Addition of ransomware non-payment principle. |
| 4 | April 2024 | Inclusion of Emerging Technologies & AI and minor update to Information Asset Owner table. |