Physical Security Policy

1. PURPOSE

The purpose of this policy is to provide a framework for the development of consistent and reasonably practical physical security controls that ensure safety and security of Holmesglen employees, learners, visitors, information assets and the Institute's facilities.

2. SCOPE

Applies to:

- All users of Holmesglen's facilities.
- All users of Holmesglen's physical assets.
- All users of Holmesglen's information systems and information assets.
- All guests and visitors accessing the Institute restricted security zones.
- Third parties and contractors who are under a contract agreement have access to Holmesglen's facilities, physical assets, information assets or information systems.

3. POLICY STATEMENT

Holmesglen is committed to providing a safe and secure environment for its employees, learners, contractors, and visitors. Holmesglen designs and implements physical measures intended to deter, prevent and detect unauthorised access, theft, or damage to its physical assets.

Holmesglen requires all users of its physical assets to comply with this policy and related procedures. Any attempted or actual security breach is investigated and may result in disciplinary action.

4. PRINCIPLES

General principles

4.1 Holmesglen's facilities provide an appropriate level of protection for the Institute's physical resources and assets.

4.2 Holmesglen appoints an asset owner across all stages of the asset management lifecycle in accordance with the Asset Management Rule and Asset Management Plan including accountabilities for asset access, use and security. Asset owners may identify asset custodians with responsibilities for securing and protecting the physical asset on behalf of the owner including physical locations or assets within a department, unit or faculty.

4.3 Physical security measures aim to minimise the risk of harm to people and damage or compromise to physical assets.

4.4 Holmesglen applies security measures proportionate to the security risk identified through the business impact assessment process.

4.5 Security of Holmesglen's physical assets is assured through effective controls aimed at:

a) controlling, deterring, detecting, and delaying unauthorised access and use

b) responding to and recovering from security incidents

c) maintaining security systems

d) providing security training and awareness as relevant to all members of the Holmesglen community.

Facilities planning and incident prevention

4.6 Holmesglen ensures that the facilities housing its resources and assets provide adequate security based on the facility's function and a security risk assessment.

4.7 Holmesglen identifies protective security requirements at the earliest point in the planning, selection, design or refurbishment/modification of physical facilities and documents these in security plans.

4.8 Incident prevention measures are considered as part of the safety planning and risk management processes, which may include:

a) Planning suitable building access

b) Installing physical barriers, alarms, surveillance and lighting systems

c) Monitoring information security

d) Maintaining a security presence including patrols by trained security employees

e) Ensuring users of facilities are appropriately inducted and receive communications and training regarding safety and security awareness, accountabilities and prevention strategies

f) Implementing testing, review and evaluation processes including trial evacuations and simulated emergency response testing

g) Developing and implementing associated policies and procedures relating to asset management, occupational health and safety, conduct and discipline, and remote working to ensure the safety and security of Holmesglen's physical assets.

Security zones

4.9 Security zones are identified to scale physical security measures based on security risk assessments.

4.10 Holmesglen implements three security zones with increasing restrictions and access control as the zone progresses. The physical security measures for each zone are designed to protect people, physical assets and information assets from compromise, damage or harm. Refer to Appendix 1.

Campus security

4.11 Holmesglen operates several security systems to keep Institute premises and the surrounding environment safe and secure for employees, learners, contractors and visitors.

4.12 Holmesglen uses CCTV systems on its premises (including outside and inside buildings) covering vulnerable areas, public access points and adjacent streets. The CCTV system and all its recordings are owned and operated by Holmesglen.

4.13 Holmesglen uses CCTV only for the purposes of protecting life and property and detecting and preventing criminal activity. The captured images are recorded and retained for evidence purposes.

4.14 All images from CCTV system are handled in accordance with the *Privacy and Data Protection Act 2014*, the *Surveillance Devices Act 1999* and Holmesglen's Privacy Policy. Individuals who have been monitored by a CCTV system have a right of access to their recorded images.

4.15 Covert cameras may be used in limited circumstances where their use is necessary to detect criminal activity and/or assist in apprehending offenders for a specified period. Recordings from covert CCTV cameras will be handled in compliance with the *Privacy and Data Protection Act 2014* and Holmesglen's Privacy Policy.

4.16 Security guards at Holmesglen provide a physical presence and rapid response to security incidents. Guards are appropriately licensed and have a police clearance.

4.17 Holmesglen operates several perimeter intrusion detection systems and panic alarms which are monitored 24/7. Security responds immediately to the activation of these alarms.

4.18 Regular patrols are made of buildings and the campus environment to provide visible deterrence to security breaches. Covert operations may also be conducted to investigate security incidents, gather evidence and detect or prevent criminal activity.

Access control

4.19 Holmesglen applies the least privilege access required to perform duties associated with an individual's role and positively identifies all individuals prior to granting access.

4.20 Holmesglen implements measures that allow authorised personnel, vehicles and equipment to pass through protective barriers, while preventing unauthorised access. These measures include:

a) Security boom gates located at the entry and exit points

b) Use of bollards for perimeter protection

c) Fences and walls to define the perimeter

d) Security offices monitoring and controlling entry and exit points using intercoms and CCTV

e) Mechanical locking devices operated by keys or codes

f) Electronic access control systems

g) Psychological and symbolic barriers such as signage, lighting, colour coding or landscaping.

4.21 All employees and learners are issued with a Holmesglen identification card, which functions as an identity card, library membership card, print release card, and access control card. Cards remain the property of Holmesglen. Card holders must:

a) Always carry their card while on campus

b) Present their card to security employees on request

c) Safeguard their card from unauthorised use and not loan it to another person

d) Report a lost or stolen card.

4.22 Employee ID cards are provisioned with basic access including the employee's work office, general classrooms, and computer laboratories for teaching staff. Employees and learners who require additional access must obtain formal approval.

Public events

4.23 Holmesglen ensures that public events held on Holmesglen premises are approved prior to the event and that a security risk assessment informs security requirements for the event.

4.24 Hire of Holmesglen facilities by external parties for public events is coordinated by the Purchasing, Licensing and Leasing department in accordance with relevant policies and procedures.

4.25 Holmesglen ensures that enhanced security measures are in place relevant to the nature, size and scale of the event.

4.26 Members of the public are permitted to be on the Institute premises for the duration of the public event they are attending. For ticketed events access is granted only to those with a valid event ticket.

Security incidents

4.27 Holmesglen maintains its readiness to handle emergencies and critical incidents on all its premises.

4.28 The Critical Incident Management Plan, Emergency Services and Management Procedure and associated documents provide a framework for emergency and incident management and document the accountabilities for managing physical security incidents.

4.29 All employees, learners, contractors and visitors are required to comply with all reasonable requests from Security Services including participating in investigations where relevant.

Training and awareness

4.30 Training and awareness programs are designed to equip employees, learners, contractors, and relevant stakeholders with the knowledge and skills needed to protect people, physical assets and information assets from physical threats.

4.31 All asset users are informed of Holmesglen's security measures and emergency procedures and are required to comply with all applicable policies and procedures.

4.32 Holmesglen delivers physical security programs tailored to roles and risks levels including:

a) General security awareness training for all employees, learners and contractors covering the importance of physical security, access control, recognition and reporting of suspicious behaviour, secure handling and storage of physical assets, emergency response procedures and guidelines for securing the workplace and when working remotely.

b) Role specific training for all managers and security, facilities and frontline employees covering advance training in use and management of surveillance systems, incident response, conflict de-escalation, patrol procedures, securing physical infrastructure, managing contractors, oversight of team compliance, incident escalation, business continuity.

c) Emergency procedure training for Emergency Wardens, First Aiders, Mental Health First Aiders covering fire evacuation, lockdowns, bomb threats responses, use of communication tools and participation in regular drills.

Reporting and records management

4.33 Security data and incidents are analysed and reported to relevant Holmesglen committees on regular basis to identify systemic issues, emerging risks and opportunities for improvement.

4.34 Records relating to physical asset security are handled in accordance with Holmesglen's Privacy Policy and Records Management Policy and all applicable legislative and regulatory requirements.

5. ACCOUNTABILITIES

Action	Accountability
▪ Report security threats, incidents, breaches or suspicious activities immediately to Security Services. This includes physical damage to infrastructure, disturbance and/or witnessing a behaviour of concern, possession of weapons or prohibited substances, receiving a bomb threats, identifying a suspect parcel, fire emergency, gas leak, hazardous or dangerous chemical spill. ▪ Take reasonable measures to protect personal property and Institute assets including equipment used in work and learning from unauthorised access, theft or damage. ▪ Safeguard access cards and keys and report lost or stolen items to Security (employees and contractors) or an Information Office (learners). ▪ Display a visitor/contractor pass as relevant and return it to the point of issue at the end of the visit.	All users of physical assets including employees, learners, contractors and visitors
▪ Follow procedures as relevant relating to asset handling, relocation and disposal, and contractor and visitor management.	All employees

Action	Accountability
▪ Secure individual offices when not occupied. ▪ Ensure that Institute equipment, including ICT assets, directly your control is kept safe and secure. ▪ Seek advice from Security Services to safeguard high value assets.	
▪ Ensure this policy is complies with the Institute's legal, regulatory and contractual obligations for physical asset security. ▪ Oversee implementation of this policy.	Executive Director Corporate and Commercial Services
▪ Monitor and respond to high-risk cyber and physical security incidents and breaches. ▪ Provide strategic directions and allocate resources. ▪ Champion a culture of security across the Institute.	Executive Directors
▪ Develop, implement and maintain physical security plans. ▪ Conduct regular risk assessments of physical security. ▪ Manage physical security controls including access systems, CCTV, and alarms. ▪ Coordinate with external bodies (e.g. police, emergency services, regulators). ▪ Lead investigations of security incidents and breaches. ▪ Monitor and control access to buildings and secure zones. ▪ Conduct patrols and respond to incidents. ▪ Secure all external entry and exit points outside of the Institute's operational hours. ▪ Issue identification cards to employees. ▪ Check identification, issues visitors pass, and escort guests as needed. ▪ Induct and issue access cards to maintenance contractors as authorised by the asset owner. ▪ Authorise access for individuals who are not directly engaged or covered by the terms of a contract or agreement. ▪ Escalate any suspicious activity or security breaches including any breaches (or suspected breaches) of physical access controls. ▪ Revoke, suspend or modify user access to physical assets where authorised.	Manager Security
▪ Align physical security with cyber security policies and procedures. ▪ Ensure physical access controls are in place for access to ICT communications rooms and data centres. ▪ Approve contractor access to ICT communications rooms and ensure verification via photo ID check. ▪ Manage access logs and integrate physical and digital security systems. ▪ Provide input into the development of physical asset security procedures, guidelines and related documentation where appropriate.	Chief Information Officer

Action	Accountability
▪ Approve requests to relocate or dispose of ICT assets and action accordingly. ▪ Provide and manage the technical infrastructure to support physical access control. ▪ Revoke, suspend or modify user access to information systems, information assets and ICT physical assets where authorised.	
▪ Maintain and secure physical infrastructure. ▪ Ensure physical barriers, locks and environmental controls are functioning as designed. ▪ Support implementation of security zoning and controlled areas. ▪ Collaborate with security personnel to manage security upgrades and maintenance. ▪ Implement physical controls to protect access to facilities and information assets. ▪ Coordinate with Security Services to manage maintenance contractor access to physical facilities.	Manager Facilities
▪ Issue identification cards to learners.	Registrar
▪ Integrate security responsibilities into employment contracts and inductions. ▪ Conduct identity verification processes prior to onboarding and provision of access to information assets. ▪ Manage employee access through onboarding and offboarding process. ▪ Implement employee disciplinary process for policy breaches.	Associate Director People
▪ Ensure employees, learners and contractors are inducted and briefed on security expectations. ▪ Ensure user identity details are entered and updated in the relevant access system on commencement, cessation and/or variation to employment or contractual arrangements. ▪ Approve access requests for additional access to facilities required by employees or learners. ▪ Ensure visitors are informed and comply with Holmesglen security policies and are aware of emergency procedures. ▪ Check and record the identity of a visitor entering Zone 3 premises and always escort the visitor.	Managers
▪ Consult with Brand, Marketing and Communications events managers to identify potential security risks for public events. ▪ Complete a security risk assessment in consultation with Security Services where relevant. ▪ Obtain prior approval from the Manager Purchasing, Leasing and Licensing to contract a third-party provider to organise a public event on Holmesglen premises.	Public event organisers

6. DEFINITIONS

Term	Meaning
Access control	The method/system that permits approved access to information, buildings and areas including, but not limited to, electronic code-pads, card readers, duress buttons, mechanical barriers, mechanical or electronic locks and keys, digital credentials, Bluetooth or radiofrequency-based access technology, and the use of identification cards, signs, definitions and instructions that are used to define spaces.
Access system	The system that facilitates approval for authorised users to use physical and information assets or enter restricted locations. Includes: ▪ Staff Access System (SAS). ▪ Student Management System (SMS)
Asset owner	The position or role that is accountable for the asset and has the authority to make decisions across the asset management lifecycle.
Asset custodian	The position or role responsible for defining and enforcing rules for the physical asset on behalf of the asset owner. It also could be a person responsible for physical locations or assets within their department, unit or faculty.
Least privilege	Allocating minimal user privileges to physical assets based on users' role and responsibilities.
Manager	The person who is responsible for the operations of a faculty, department, centre, unit or another functional area within Holmesglen.
Physical access control	An access control applied to a physical location – for example locks or a proximity swipe device.
Physical assets	Comprise land, buildings, infrastructure, plant and equipment, cultural collections such as artworks and library resources, natural resources and information and communication technology (ICT) assets.
Public event	Any event or activity conducted on Holmesglen premises attended by more than 30 members of the public.
Security zones	Campus and building spaces with specific physical security controls determined by risk assessment and business impact level of assets held.
Third-party arrangements	Includes arrangements for the provision of: ▪ a service to Holmesglen under a written agreement ▪ education, training and assessment services on Holmesglen's behalf under a third-party agreement: ▪ labour-hire workers ▪ recruitment services for domestic and /or overseas learners under a written agreement ▪ contractor or consultancy services defined by the Contractor or Consultant Engagement Procedure ▪ services on Holmesglen's behalf to facilitate data exchange with government agencies and regulatory bodies.
Users	Any person who is granted access to Holmesglen's information assets, information systems and/or physical assets including a person

Term	Meaning
	engaged under a third-party arrangement and any employee or agent within the third-party arrangement.

7. CONTEXT AND/OR REFERENCED DOCUMENTS

Internal

Access Control Policy

Asset Management Rule

Asset Management Plan

Code of Conduct

Contractor or Consultant Engagement Procedure

Critical Incident Management Plan

Emergency Services and Management Procedure

Employment Policy

Information Security Policy

Privacy Policy

Records Management Policy

Risk Management Rule

Risk Management Plan

External

Attorney-General’s Department Protective Security Policy Framework

Privacy and Data Protection Act 2014

Surveillance Devices Act 1999

Victorian Protective Data Security Framework

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
1	June 2025	New policy

APPENDIX 1: HOLMESGLEN SECURITY ZONES

Control element	Zone 1	Zone 2	Zone 3
Access and security clearance requirements	Public access area No security clearance required.	Offices and workshop areas Restricted public access. Unrestricted access for authorised personnel. Current Holmesglen employment screening process and Holmesglen condition of employment met including Working With Children Check: • All Institute employees including casual employees • Contractors • Volunteers	Restricted areas Only authorised personnel. Visitors access only for a need-to-know and with close escort. Requires National Police Check: • All employees in a position with financial delegation • All employees in a position with responsibility for cash and financial transactions • Other employees determined by Directors, Associate Executive Directors and Deans with authorisation from asset owners. Access to ICT communications rooms and data centres are restricted to employees who manage and maintain servers and communication equipment. Contractors or visitors accessing these facilities must obtain TSD approval and be verified with photo ID check.
Perimeter door and hardware	In accordance with Holmesglen risk assessment	In accordance with Holmesglen risk assessment. Electronic Access Control System (EACS) Use of approved locks	Use identity card and sectionalised Electronic Access Control System. Use of approved locks. Authorised and auditable key distribution.
Out of hours security alarm systems	In accordance with Holmesglen risk assessment	In accordance with Holmesglen risk assessment	Hard wired security alarm systems. 24/7 monitoring of alarms
Monitoring and response	All alarms systems monitored and responded. Response capability appropriate to the threat risk.	All alarms systems monitored and responded	All alarms systems monitored and responded.
Information asset use and storage	Information assets classified as OFFICIAL with a business impact level of 1.	Information assets classified up to OFFICIAL: Sensitive or with a business impact level of 2. Information asset classified	Information assets classified up to and including PROTECTED, or with business impact value of 2 and above.

Control element	Zone 1	Zone 2	Zone 3
		as PROTECTED can be used and stored if unavoidable.	
Detection devices	In accordance with Holmesglen risk assessment	Hard wired industry approved systems installed by qualified installer, regularly serviced by authorised provider.	Hard wired industry approved systems installed by qualified installer, regularly serviced by authorised provider.
Contractor clearance and induction	Detailed auditable contractor control and access instruction. Use of contractor passes	Detailed auditable contractor control and access instruction. Use of contractor passes.	Detailed auditable contractor control and access instruction. Use of contractor passes and escort. Secure method of contact for immediate communication Dedicated system for contractor induction and issuance of contractor access.
Visitor control	In accordance with Holmesglen risk assessment	In accordance with Holmesglen risk assessment. Recommended to record visitors, issue passes and escort in some areas	Detailed auditable visitor control and access instruction. Use of visitor passes and escort. Secure method of contact for immediate communication
Access control system	In accordance with Holmesglen risk assessment	In accordance with Holmesglen risk assessment Recommend use of identity access card in office environments.	Use identity card and sectionalised access control systems. Use Electronic Assess Control Systems (EACS) Verify the identity of all personnel, including contractors.
Technical surveillance	In accordance with Holmesglen risk assessment	In accordance with Holmesglen risk assessment	In accordance with Holmesglen risk assessment