

Physical Security Policy

Document Title: Physical Security Policy

Document Owner: Jeff Williams

Approved By: Gary Conlan

Version: 1.0

Effective Date: June 2026

Review Date: June 2027

1. Purpose

The purpose of this Policy is to define the organisation's approach to protecting people, premises, physical assets, and information-bearing media against unauthorised access, theft, loss, damage, interference, or misuse.

This Policy establishes the minimum physical security requirements for offices, secure areas, equipment, records, and assets used by the organisation.

2. Scope

This Policy applies to:

- all employees, contractors, temporary staff, agency workers, consultants, and relevant third parties
- all offices, sites, rooms, storage areas, and facilities used by the organisation
- all physical assets, including laptops, desktops, mobile devices, servers, removable media, keys, passes, paper records, and other sensitive equipment or materials
- all secure storage, access monitoring, CCTV, alarm, and disposal arrangements operated by or on behalf of the organisation

3. Policy Statement

The organisation shall implement proportionate physical security controls to prevent unauthorised physical access to its premises, systems, records, and assets, and to reduce the risk of theft, loss, damage, tampering, or compromise.

Physical security controls shall include defined responsibilities, controlled access, monitoring, secure storage, asset management, and secure destruction and disposal arrangements.

4. Roles and Responsibilities

4.1 Senior Management

Senior Management shall:

- approve this Policy
- ensure adequate physical security arrangements are in place
- support investment in appropriate premises, monitoring, storage, and disposal controls
- review significant physical security risks, incidents, and improvement actions

4.2 Managers

Managers shall:

- ensure colleagues understand and comply with this Policy
- report physical security concerns, incidents, or control failures promptly
- ensure sensitive assets and records within their area are stored appropriately
- support asset checks, access reviews, and investigations where required

4.3 Facilities / Office Management

Facilities or Office Management shall:

- maintain physical access controls for offices and secure areas
- manage locks, keys, passes, alarms, CCTV, and access records where applicable
- coordinate repairs or escalation where physical security weaknesses are identified
- support secure disposal of physical records and assets where appropriate

4.4 IT / Asset Owners

IT and relevant Asset Owners shall:

- maintain asset inventories
- ensure sensitive devices and media are tracked, stored, transferred, and disposed of securely
- support secure wiping, destruction, or disposal of information-bearing assets
- investigate lost, stolen, or damaged devices

4.5 All Employees and Users

All employees and users shall:

- protect physical assets, keys, passes, and records in their care
- prevent unauthorised persons from entering restricted areas
- challenge or report unknown persons where appropriate and safe to do so
- report lost passes, keys, devices, records, or suspicious activity immediately
- keep desks, screens, devices, and sensitive records secure when unattended

5. Physical Access Control

Access to organisational premises and restricted areas shall be controlled according to business need.

The organisation shall ensure that:

- access to offices and secure areas is limited to authorised persons

- keys, passes, fobs, codes, or other access mechanisms are issued, controlled, and revoked
- access permissions are reviewed periodically and when staff join, move, or leave
- visitors, contractors, and delivery personnel are managed appropriately
- access to higher-risk areas is subject to stronger controls where needed

6. CCTV

Where CCTV is used, it shall be operated for legitimate security, safety, and asset-protection purposes.

The organisation shall ensure that:

- CCTV coverage is proportionate to the risk and business need
- signage is displayed where required
- access to CCTV footage is restricted to authorised persons only
- footage is retained, reviewed, and disclosed only in accordance with legal, regulatory, and business requirements
- CCTV systems are protected against unauthorised access, tampering, or misuse

7. Intruder Alarms and Security Monitoring

The organisation shall operate alarm or monitoring controls where appropriate to protect premises, secure areas, and critical assets.

This may include:

- intruder alarms
- monitored alarm systems
- door or window sensors
- motion detection
- after-hours alerting
- escalation arrangements for alarm activation

Alarm activations, faults, and overrides shall be recorded and investigated where necessary.

8. Records of Access

The organisation shall maintain records of access to premises or secure areas where appropriate to the level of risk.

Access records may include:

- issuance and return of keys, passes, fobs, or codes
- visitor logs

- sign-in and sign-out records
- door access logs
- contractor attendance records
- alarm and CCTV access logs

Access records shall be retained for an appropriate period and protected against unauthorised access or alteration.

9. Asset Management

The organisation shall maintain an inventory of relevant physical assets.

Asset records shall include, where applicable:

- asset description
- unique identifier or serial number
- owner or custodian
- assigned user
- location
- classification or sensitivity where relevant
- status, including in use, in storage, under repair, returned, lost, stolen, or disposed

Assets shall be physically protected in accordance with their value, sensitivity, and criticality.

10. Secure Areas and Storage of Sensitive Assets

The organisation shall identify and protect secure areas used for the storage or processing of sensitive assets, records, or information.

Secure storage controls shall include, where appropriate:

- locked rooms, cabinets, or containers
- limited and authorised access only
- separate storage for high-value or sensitive assets
- environmental protection where needed
- additional protection for backup media, paper files, removable media, and information-bearing devices
- restricted storage of keys, access passes, and security materials

Sensitive assets shall not be left unattended in unsecured locations.

11. Clear Desk and Clear Screen

Users shall apply clear desk and clear screen practices to reduce the risk of unauthorised access to sensitive information.

This includes:

- locking screens when unattended
- securing laptops and mobile devices when not in use
- placing paper records in locked drawers or cabinets where appropriate
- removing sensitive material from desks, meeting rooms, printers, and shared areas
- avoiding visible display of confidential information to unauthorised persons

12. Visitors and Third Parties

Visitors and third parties shall be managed to prevent unauthorised access to sensitive areas, records, or assets.

The organisation shall ensure that:

- visitors are signed in where required
- visitor identity is confirmed where appropriate
- visitors are escorted in restricted areas unless explicitly authorised otherwise
- visitor access is limited to relevant areas only
- temporary access methods are controlled and recovered

13. Security Incidents and Loss of Assets

Any physical security incident shall be reported immediately.

This includes:

- lost or stolen keys, passes, or devices
- forced entry or attempted entry
- missing records or assets
- vandalism or tampering
- suspicious persons or behaviour
- alarm faults or unauthorised alarm overrides
- damage to secure cabinets, doors, locks, or barriers

All such incidents shall be logged, investigated, and escalated as appropriate.

14. Secure Destruction and Disposal of Assets

Assets, records, and media shall be disposed of securely when no longer required.

The organisation shall ensure that:

- paper records containing sensitive or confidential information are cross-shredded or disposed of using an approved confidential waste service

- information-bearing devices and media are securely wiped, destroyed, or degaussed as appropriate before disposal, reuse, or return
- disposal of high-risk assets is documented
- disposal methods are proportionate to the asset type and sensitivity of the information
- disposal by third parties is subject to appropriate control and evidence where needed

No asset containing organisational or client information shall be disposed of through general waste without appropriate sanitisation or destruction.

15. Removal of Assets from Site

Assets shall not be removed from site without authorisation where such approval is required.

Where assets are taken off site:

- the movement shall be authorised and recorded where appropriate
- the user shall remain responsible for the asset's protection
- the asset shall be kept secure during transport, travel, and storage
- loss, theft, or damage shall be reported immediately

16. Review and Testing of Physical Security Controls

Physical security arrangements shall be reviewed periodically and when significant change occurs.

Reviews may include:

- inspection of locks, cabinets, alarms, and barriers
- verification of access lists and visitor logs
- checks of asset registers
- testing of alarm response
- review of CCTV coverage and retention settings
- review of secure storage arrangements
- review of disposal records

Weaknesses identified through review, incident, or audit shall be addressed promptly.

17. Breaches of Policy

Failure to comply with this Policy may result in:

- removal of access rights
- retraining
- disciplinary action

- contractual action
- legal or regulatory escalation where appropriate

Deliberate or reckless disregard of physical security requirements shall be treated as a serious matter.

18. Exceptions

Any exception to this Policy shall be:

- documented
- risk assessed
- approved by the appropriate authority
- time-bound where possible
- reviewed periodically

19. Review

This Policy shall be reviewed at least annually, or sooner where:

- premises or security arrangements change
- significant incidents occur
- audits or inspections identify weaknesses
- legal, contractual, or regulatory requirements change