

Physical security perimeter

Smartwatch Ltd uses security perimeters to protect areas that contain sensitive or critical information and information processing facilities. Smartwatch Ltd site have physical security perimeters. The security perimeter is checked on an annual basis and recorded at internal audit. The Managing Director is responsible for maintaining that site's secure perimeter. Smartwatch Ltd central information processing facilities are within secure areas Server Cabinet. The director has a site map for each site or secure area.

Physical entry controls

Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. A risk assessment is used to determine the type of entry controls that might be required for secure areas and these are implemented by the site manager. Currently the Smartwatch is protected by an external door with access control (managed by building manager/provider). All internal doors are protected by a key lock (that is locked outside of business hours)

Securing offices, rooms and facilities

Smartwatch Ltd has designed and applied physical security for offices, rooms and facilities. Smartwatch Ltd conducts risk assessments of its offices that contain confidential or high risk information assets to identify the controls that might be necessary to secure them. These are implemented and checked at internal audit. There are no sites where confidential information processing facilities are shared with a third party organization, other than under the terms of a contract.

Protecting against external and environmental threats

Smartwatch Ltd has designed and applied physical protection against damage from natural disasters, malicious attack or accidents. Smartwatch Ltd has assessed the risk of external and environmental threats and has applied controls that are included or that are part of the Business Continuity Management framework.

Working in secure areas

Smartwatch Ltd has designed and applied procedures for working in secure areas and these are contained as below;

- Secure areas must be locked when not in use (i.e when no one is in the office. The owner must check the secure area at least once per day, even if no one is working in it.

- Access to secure areas/areas where confidential or restricted information is processed (including in conversation) or stored is restricted to authorized persons. Authorization is provided by the Managing Director via email or writing.
- Access to secure areas requires authentication and authorized persons are issued with security fobs or keys provided by the Director.
- The authentication system retains a record of accesses and these are reviewed regular to identify any unauthorized accesses.
- The owner of a secure area is responsible for ensuring that photographic, video, audio or other recording equipment and mobile phone cameras, are not taken into the secure area without authorization.
- Third party support personnel only have access to secure areas when required and this access is specifically requested, authorized and monitored. The manager for this is the building manager. A detailed request should be made on email and kept for reference.
- In general, the owner of a secure area and all those who are authorized to work within it, are required only to divulge details of the area and what is done in the area to other staff on a need-to-know basis.

Delivery and loading area policy.

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access.

Smartwatch Ltd controls for delivery and loading areas are detailed below;

- Smartwatch Ltd controls access to its premises by unauthorized persons by:
- Restricting access to delivery and loading areas by receiving deliveries only from the front door. No delivery staff or unauthorized (non Smartwatch personnel) are let into the office unless they are expected.
- All staff must ensure that that delivery personnel cannot gain access from the delivery and loading area to other parts of the site, by applying physical entry controls in the Smartwatch Policies.
- The external doors of the delivery area are closed when the internal doors are opened.
- Incoming material is assessed by the receiving staff member for threats (particularly physical threats) before it is moved from the delivery area to the point of use.
- Incoming information assets should be registered on arrival.

Visitor and guest Policy

- Entrance to the building is has an unmanned reception. All visitors, guests and delivery staff should only be allowed past this point if they are expected. A visitor or guest must never be left unattended in the Smartwatch office.

- When entering site, a visitor should be informed of any relevant fire and safety notices
- Visitors /Guests must never be left alone in the Smartwatch office or data processing areas
- When leaving the building the visitor should be escorted to the main door ensuring they exit the building
- No visitor or guest should ever be given the keys to the Smartwatch office.

Siting and protection of equipment

The requirements are:

- a) That equipment is sited so as to minimize unnecessary access to work areas.
- b) Information processing and storage equipment (including faxes, photocopiers and telephone equipment used for confidential information) is sited in secure areas [server/communications rooms/secured offices] so that it is not possible for confidential information to be seen by unauthorized people.
- c) Secure areas are subject to the same level of physical perimeter protection as secure sites.
- d) Controls are implemented to deal with theft, natural or man-made disaster and electrical supply interference (see D above)
- e) Smartwatch Limited does not allow smoking inside any of its sites.

Supporting utilities

All servers and communications equipment are in secure areas that have adequate power supplies. For each secure area, the maximum power requirements are calculated by reference to the manufacturer's recommendations for each device, plus the requirements for other items running off the same and the Managing Director has incoming power cables checked annually by an electrician (PAT Testing) to ensure that they supply adequate power. Offices and other (non-secure) areas that contain information processing equipment are similarly assessed to ensure that power supplies are adequate.

The Managing Director is responsible for ensuring that all supporting utilities and equipment is inspected on a frequency determined by manufacturer's.

Telecommunications

- a. Telecommunications equipment is connected to the provider by a single route.
- b. Agreements are in place for "emergency" provisions for Telecoms and Internet services. See disaster recovery plans for details.

Cabling security

The Managing Director has a site map that identifies all network cabling and all incoming power and telecommunications lines.

Equipment maintenance

The Managing Director is responsible for ensuring that all equipment on the site is maintained in line with manufacturers' recommended service intervals and specifications. The Managing Director maintains a schedule of all equipment, showing its due and actual service dates, and retains copies of the service reports, together with fault reports and details of preventive or corrective action. Only authorized and experienced maintenance personnel may carry out maintenance. Equipment that processes or stores confidential information is serviced only by technicians who have been screened in line with business requirements.

Unattended user equipment

Employees are required to ensure that equipment removed from its secure area is returned and secured when it is no longer in use. Employees identifying unattended equipment outside its secure area are required to return the equipment to the Asset Owner. Unattended user equipment within its secure area must be left in a secure state. For work stations, this requires logging out of any secure sessions and locking the device. All users must agree to terms and conditions set out by Smartwatch, IT and HR policies before logon. Computers are set to automatically lock with a password after 15 minutes of inactivity, users may not change this setting.

Removal of assets

Equipment, information or software may not be taken off-site without prior authorization as required by the acceptable use and access control policies.

Security of equipment and assets off-premises

Security is applied to off-site equipment and assets taking into account the different risks of working outside Smartwatch Ltd premises. Equipment, information or software may not be taken off-site without prior authorization as required by the acceptable use and access control policies.

Secure disposal or re-use of equipment

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Clear desk and clear screen policy

Smartwatch Ltd has adopted a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities, and the requirement for compliance with this policy is set out below;

- Users are required to ensure that no confidential or restricted information (in paper or removable storage media format) is left on their desk, in my environs, or left in or near reproduction equipment (photocopiers, fax machines, scanners) when they are not in attendance. Documents with customer details or confidential documents may only be left in office that are lockable in line with Smartwatch Limited security requirements.
- Users must ensure that no one is able to access their workstation when they are not in attendance and that they must have a password protected screensaver that operates within five minutes of no activity (or which they activate when the workstation is unattended).
- Users are required to terminate active computer sessions when they have finished and must log off (i.e. not simply turn off the computer screen) whenever they are finished working.
- It is prohibited to use personal storage media, MP3 players, digital cameras and mobile phones with (or without) photographic capability while at work or connect them to a Smartwatch computer.
- Users may only use Smartwatch Limited's reproductive equipment (photocopiers, fax machines, scanners) for proper organizational purposes and users must ensure that they will use facilities that are appropriate for the classification level of any information with which they are dealing.

Signed:

Position: Managing Director



Name: Neil Jones

Date: 31/07/2025