Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

Objective and Scope

The objective of this policy is to protect secure and sensitive information and assets by preventing unauthorised physical access, loss or damage and other interference or harm to company premises and infrastructure.

The scope of this policy covers the physical environments as listed:

- Head Office - 2 North House, Bond Avenue, MK1 1SW – Used for Market Research Data Collection.

Physical security includes access to buildings, infrastructure, restricted areas within a building and information assets held at each location.

Roles, Responsibilities and Authorities

The *Operations Director* or competent delegate takes ownership of the selection, implementation and management lifecycle of the physical working environment - buildings and infrastructure.

Asset owners are assigned to persons or operational areas for lifecycle management purposes.

Responsibility for home offices is the management representative at each location.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
Health and Safety at Work Act 1974	https://www.hse.gov.uk/legislation/hswa.htm
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/
Market Research Society Code of Conduct	https://www.mrs.org.uk/pdf/MRS-Code-of-Conduct-2019.pdf
Market Research Society Fair Data Principles	https://www.fairdata.org.uk/10-principles/

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Operations	8.1			
Secure areas		11.1		
Physical security perimeter		11.1.1		7.1
Physical entry controls		11.1.2		7.2
Securing offices, roms etc		11.1.3		7.3
Protecting against external and enviro threats		11.1.4		7.5
Working in secure areas		11.1.5		7.6
Physical security monitoring		11.2		7.4
Equipment siting and protection		11.2.1		7.8
Supporting utilities		11.2.2		7.11
Cabling		11.2.3		7.12
Equipment maintenance		11.2.4		7.13
Removal of assets		11.2.5		7.10
Security of equipment and assets off premises		11.2.6		7.9
Secure disposal and reuse		11.2.7		7.14
Unattended user equipment		11.2.8		8.1
Clear desk clear screen		11.2.9		7.7

Related Information

- Information Security - CIA Lifecycle Protections
- Social Media Policy
- Physical (Equipment) Asset Management Policy
- Asset Register
- Register of persons holding keys to company offices/premises - Key Register per location
- Information Classification Policy
- New hardware setup checklist

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

- Working from home checklist
- Emergency response posters - fire / power failure / telco failure

Policy

Prevision Research shall ensure the physical working environment including buildings, infrastructure and contents (assets) providing information and information processing or storage facilities are established, maintained and protected from intrusion or harm in a secure and fit for purpose manner.

Locational threats shall be risk assessed to determine security needs considering:

- Risks associated with the intended business use e.g. sales (low risk), centre of IT resources (high risk),
- General geographic location (secure neighbourhood)
- Building suitability and current security (e.g. 24/7 security patrols)
- History of break ins or other damage
- Shared tenancy or stand alone building
- Weather related risks such as earthquake, flooding, known power supply failures
- Emergency services availability within the areas - fire services etc

Once the premises are deemed satisfactory as a business location, the following minimum standards and other listed protocols shall be met.

Minimum security standards for each **business** office/location

1. The front door of office locations is to be key locked at all times outside of normal business hours.
2. The entrances of designated offices (other than home offices) should be subject to video surveillance cameras where practical to do so.
3. Door keys of designated offices are only provided to staff members if there is a business need and only once they have signed an employment agreement that includes confidentiality and security obligations.
4. When termination of employment occurs, keys shall be returned to the designated line manager and the Key Register updated.
5. Lost keys shall be reported immediately to the Centre Manager. The need to reset locks shall be determined by the Centre Manager..

Minimum security standards for each **home office/remote** working location

1. Premises are to be locked when not in attendance and office internal location segregated from other persons when practical to do so.
2. IT equipment used at a home office is subject to the same password protection and other security measures as is equipment at any work location. Shut down equipment when not in use - clear desk clear screen protocols apply to home offices.
3. Complete the Working from Home Checklist and submit to the line manager for each remote location used as a permanent or semi permanent work location.

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

Secure areas: Physical security perimeter and entry controls

Where premises are wholly owned/occupied by the company, the perimeter is considered the boundary of the complete building and all entries apply to security controls.

In the case of a shared building, the perimeter of the building is determined as that which is occupied by the company and the immediate boundaries within the control of the organisation. The direct entries to the designated company office/infrastructure are considered those critical to company security.

Regardless of whether a building is a stand alone or shared premises, where information processing occurs on premises, as a minimum the following secure protocols shall be in place:

- Limit physical access to working areas during working hours on a needs basis e.g. front reception desk manned or buzzer access
- Recording of visitors to site by day/time/who/why/contact details
- Information processing equipment segregated from general activities and securely attached with security cables or equivalent control
- Exit fire doors alarmed and/or monitored with security cameras or other intruder detection mechanisms

Secure areas: Offices, rooms and facilities

Where there is a need for rooms or areas to be highly secure due to the nature of information being processed or stored:

- Confidential information on computer screens should not be visible to other than the operator
- Data tracking of work via an electronic audit trail of accessed confidential files/data should be maintained according to the security status of the individual and nature of work
- Lockable offices or secure cabinets made available for high and above risk classified information - electronic or hard copy format.

Visitor access

- Visitors are requested to show evidence of the purpose of their visit (who they intend to see) and provide ID.
- A log of the visit recorded
- The visitor will be escorted by the person requesting their attendance or a nominated person.

Protecting against physical and environmental threats

The organisation shall risk assess the likely emergency situations facing each physical location and working environment. As a result of the risk assessment, the company shall have in place emergency plans for certain emergency and disruptive scenarios.

A poster shall be clearly displayed in entrances and primary working areas indicating what to do in an emergency. Examples include building or fire / flood/ earthquake / power failure / telco failure.

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

Working in secure areas

Protocols shall be in place for those working in IS secure areas. This shall be included in induction into the particular building and shall include as appropriate:

- Working these areas involve secure information therefore individuals are required to have signed a NDA
- Working in a secure area should involve supervision to ensure only 'need to know' work protocols are practiced
- Stand in or replacement staff must have the same or greater security clearance than the person they are replacing
- Third parties such as vendors or contractors must be security vetted before entry and supervised at all times
- The use of security cameras is limited to prevent secure information being viewed via a camera

Physical security monitoring

Surveillance monitoring of high risk areas either as guarding or electronic surveillance, alarm systems or video monitoring is used when a risk assessment determines a need.

The following systems are in place:

- Fire alarm – covers the entire building maintained by the landlord.
- CCTV – Locations TBC (currently being installed)
- Security Alarm – covers the prevision office, maintained by Prevision.

Deliveries

Incoming and outgoing deliveries require a risk assessment to determine information security risks, if any, and initiate risk controls. This applies to circumstances where high risk classified information and a strong presence of computer and general IT equipment is being handled.

Only nominated personnel with security clearance (appropriate to the risk classification) can authorise any inwards/outgoing goods movement including couriers. Tracking of activities shall include:

- Request and approvals for goods in/out and inspection before leaving against the request and on receipt against receipts/shipping dockets
- Use of approved suppliers only
- Signatures and a log of entries tracking all activities shall be retained
- Security cameras activated at all times

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

Equipment: Siting and utilities protection - refer Asset Register

Equipment critical to data and information services (refer Asset Register) reliability shall be:

- Placed in a secured area subject to protection from theft.
- Placed away from general workplace behaviours such as food and drink consumption.
- Positioned away from risks associated with weather effects (open window).
- Protected from unintended power source interruption such as unplugging power points.
- Installed using power surge protectors attached to devices at the wall or the building including lightning protection. These are subject to periodic inspection and maintenance. Records are kept.
- Where equipment could be subject to theft, secure cables shall be installed on removable or portable devices. These are subject to periodic inspection and maintenance. Records are kept.

Supporting utilities reliability shall be managed to ensure reliability and continuity of service:

- Utility service providers shall be selected and monitored for performance reliability.
- A backup power supply providing interim power for a period should be provided where practical including emergency lighting.

Equipment maintenance

Equipment is maintained according to manufacturer's instructions to ensure availability, integrity and confidentiality of information. Records of maintenance and repairs are recorded against each device via the Asset Register.

Supporting utilities: Cabling security and equipment maintenance

- Telecommunications cabling by an external provider to the building shall be planned with the provider to ensure protection from unauthorised or unintended interference or environmental effects.
- Internal cabling within the building includes protective conduit and other guarding as appropriate to information security risks and available building infrastructure. This is subject to periodic inspection and maintenance.
- Equipment shall be operated and maintained according to manufacturer's specifications. Maintenance records are kept and equipment assigned to individuals - refer Asset Register.
- Electrical equipment shall be subject to regular electrical test and tag routine for reliability and safety. Records are kept.

Other essential services are maintained according to contract and in the case of an emergency due to loss of supply, refer to the emergency response plan 'Fire, Flood and Civil Unrest ERP'.

Equipment: Asset removal, secure disposal and reuse

Refer 'Physical (Equipment) Asset Management Policy': Asset lifecycle, acceptable use, return and destruction.

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements traceable through the Asset Register.

As a minimum, the owner of the asset as defined in the Asset Register shall have classification and user status appropriate to the use of the physical asset and access to any information held within the asset. This includes removal and transportation of the asset according to business need.

Other persons or groups may use an asset on a frequent or infrequent basis, however the overall responsibility for asset management rests with the asset owner as delegated in the Asset Register.

On termination of employment, the employee (asset owner) shall return assets to the Operations Director or IT Team member for cleansing of data, secure data transfer and/or asset destruction.

Should an individual wish to purchase the asset from the company or asset re-used by the organisation, the Operations Director shall approve the sale or re-use from an information security perspective. The asset shall then be wiped of all data or alternatively the data transferred to another secure device, and then returned to manufacturers specification and tested to confirm clear status before confirming the property is fit for sale or re-use.

Mobile asset (endpoint device) security when off premises

Any mobile asset moved or operated off site including BYOD devices that store or process information are an information security risk. As such they are required, regardless of ownership, to have in place protection measures to ensure devices are not stolen, lost, damaged or subject to unauthorised use. Each device must have a tracking mechanism installed and be listed on the Asset Register as part of data security protocols.

Information stored on mobile assets (endpoint device)

Information stored on, processed by or accessible via an endpoint drive shall be protected by:

- Device security
- Restriction on software installation
- Controlled software updates and patches in a timely manner
- Limitations of use via public networks
- Encryption if approved by the Operations Director
- Remote disabling and lock out capability

Unattended user equipment

Unauthorised use of equipment may occur when equipment is unattended. To protect from misuse, the following security measures are in place:

- Lockout / timeout measures when the screen session becomes inactive.
- User closes sessions or logs off when finished or the device is to be left unattended.
- Password protection in place on devices.

Information Security within the Physical Working Environment (Buildings & Infrastructure) Policy

Clear desk / clear screen protocols

The following clear desk / clear screen protocols apply regardless of whether the device is in the office or remote.

- Paper (hard copy) information is removed from view when left unattended. High risk classified information shall be moved to a lockable container - drawer or alternative locked area.
- Paper (hard copy) high classified information never re-used and can only be recycled if shredded.
- Use of photocopiers, scanners or cameras cannot be used without authorisation for highly classified information. When authorised, the copy shall be treated as a controlled document.
- Electronic information displayed on computer or other technology screens are subject to clear screen technology - timeout after 5 minutes.

For use of USB, CD's refer to 'Storage Media Policy'.

Security of assets off premises

Any device used outside designated business premises which stores or processes information (e.g. mobile device), including devices owned by the company or devices owned privately and used on behalf of the company (BYOD) needs protection. The use of these devices shall be authorised.

For devices used off site refer to 'Mobile Devices Policy' and 'Remote and Teleworking Policy'.

Storage media

The storage of removable media is managed through the following core principles:

- Authorisation from Operations Director is required for the use or removal of stored media of high risk classified information
- Devices must be secured in a safe environment to prevent loss from theft or damage due to environmental factors
- Devices holding secure business data including personal identifiable information must be registered, content encryptable and then only used as approved by the Operations Director.

For further information refer to 'Media Handling Policy'.

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N