1. **Scope**

All designated secure areas on any of *{OrganisationName}*’s premises are subject to controlled access and usage.

1. **Responsibilities**

Every secure area has an *[owner]* and the *[owner]* is responsible for ensuring that prescribed controls are maintained and as otherwise specified below.

The *{PremisesManager}* is responsible for authorising access to secure areas.

All *{Employees/Staff}*, contractors and third parties have certain responsibilities as defined below.

1. **Physical security perimeter**
   1. *{OrganisationName}* uses security perimeters to protect areas that contain sensitive or critical information and information processing facilities.
   2. [All] *{OrganisationName}*’s sites have physical security perimeters.
   3. The [Site Manager] of each *{OrganisationName}* site is responsible for maintaining that site’s secure perimeter.
   4. *{OrganisationName}*’s central information processing facilities are within secure areas [server room/communications room], each of which have Owners (see [ISMS-C DOC 8](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_8.docm)) that are themselves within a site’s secure perimeter.
   5. The {InfoSecManager} has a site map for each site or secure area, together with a current security checklist that identifies the current state of conformity to the requirements in that checklist.
2. **Physical entry controls and working in secure areas**
   1. Secure areas must be locked at all times. The lock specification is *[insert details]*. The *[owner]* must check the secure area at least once per day, even if no one is working in it.
   2. Access to secure areas/areas where confidential or restricted information is processed (including in conversation) or stored is restricted to authorised persons. Authorisation is provided by *[insert details of how this is done and by whom]*.
   3. Access to secure areas requires authentication and authorised persons are issued with *[provide details of access cards, etc. and related security procedures, PINs, etc.]*.
   4. All *{Employees/Staff}*, contractors and third parties are required to wear an identification badge *[insert details of how issued, what it contains]* and are required to notify security *[if they encounter unescorted visitors]* and anyone not wearing required identification.
   5. Third-party support personnel only have access to secure areas when required and this access is specifically requested, authorised and monitored *[insert details of who should authorise access and how it should be recorded – it will depend on the risk assessment, because the appropriate control could be a log book or it could be a more sophisticated process that requires the third party engineer to be specifically validated prior to access]*.
3. **Securing offices, rooms and facilities**
   1. *{OrganisationName}* has designed and applied physical security for offices, rooms and facilities.
   2. *{OrganisationName}* c onducts risk assessments in line with [ISMS DOC 6](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Section_4-10/ISMS_DOC_6.docm) of individual offices, rooms and facilities that contain confidential or high-risk information assets to identify the controls that might be necessary to secure them. There are no sites where confidential information processing facilities are shared with a third-party organisation, other than under the terms of a contract.
4. **Protecting against external and environmental threats**
   1. *{OrganisationName}* has designed and applied physical protection against damage from natural disasters, malicious attack or accidents.
   2. *{OrganisationName}* has assessed the risk of external and environmental threats and has applied controls that are included in this document or that are part of the Business Continuity Management framework (see [ISMS-C DOC 17](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_17.docm)).

1. **Delivery and loading areas**
   1. {OrganisationName} controls access to its premises by unauthorised persons by:
      1. Restricting access to delivery and loading areas at *[all its sites]* from outside the building either to personnel identified and authorised in line with Clause 4 above or to personnel identified and authorised as employed by the third party delivering to or collecting from the site.
      2. Ensuring that delivery personnel cannot gain access from the delivery and loading area to other parts of the site, by applying physical entry controls as described elsewhere in this document.
      3. Incoming information assets should be registered on arrival *[this step must tie in with your goods inwards process and notify your asset inventory controller of the arrival of a new asset so that it can be logged]*.
      4. Keeping incoming and outgoing shipments physically separate.

1. **Equipment siting and protection**
   1. The requirements are:
      1. That equipment is sited so as to minimise *[public / unnecessary]* access to work areas.
      2. 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 unauthorised people.
      3. Secure areas are subject to the same level of physical perimeter protection as secure sites.
      4. Equipment that requires special protection *[categories]* is isolated *[in a secure area]*.
      5. Controls are implemented to deal with theft, natural or man-made disaster, environmental pollution *[insert details]*, dust *[insert details of controls]*, vibration *[insert details of controls]*, chemical effects *[insert details of controls]*, electrical supply interference *[insert details of controls]*, communications interference *[insert details of controls]*, electromagnetic radiation *[insert details of controls]*.
      6. Secure areas are monitored for temperature and humidity *[insert details of equipment used]*, acceptable limits for both have been set *[where are they]* and *[who?]* receives an immediate alert *[how?]* once they are breached.
2. **Supporting utilities**
   1. [This will vary considerably between organisations and industries. Describe the controls you apply to supporting utilities that are essential for the operation of *{OrganisationName}*’s processes. This is likely to include power (do you use a UPS? Are there backup generators?), Internet and telecommunications, water, sewage, heating and ventilation, emergency power control switches, etc.]
3. **Cabling security**
   1. The *{PremisesManager}* has a site map that identifies all network cabling and all incoming power and telecommunications lines; those lines that are not underground are protected *[how?]*.
   2. Network cabling is protected from unauthorised access *[provide details]* and power and network cables are segregated *[how]* and clearly marked for ease of maintenance *[how is color coding/marking linked to equipment so that it is clear which cable goes where?]*.

1. **Equipment maintenance**
   1. The *{PremisesManager}* is responsible for ensuring that all equipment on the site is maintained in line with manufacturers’ recommended service intervals and specifications. The *{PremisesManager}* 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.

1. **Removal of assets**
   1. Equipment, information or software may not be taken off-site without prior authorisation as required by [ISMS-C DOC 11](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_11.docm).

1. **Security of equipment and assets off-premises**
   1. Security is applied to off-site equipment and assets taking into account the different risks of working outside *{OrganisationName}*’s premises.
   2. Users of mobile equipment are required, as part of their User Agreements (see [ISMS-C DOC 9](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_9.docm)), to provide appropriate physical security for equipment when off-site and to ensure that manufacturer’s instructions for protecting equipment are followed.
   3. The {FinanceDirector} is responsible for ensuring that *{OrganisationName}*’s insurance specifically provides cover against loss of or damage to mobile devices off-site.
2. **Secure disposal or re-use of equipment**
   1. 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.
3. **Unattended user equipment**
   1. Employees are required to ensure that equipment removed from its secure area is returned and secured when it is no longer in use.
   2. Employees identifying unattended equipment outside its secure area are required to return the equipment to the *[Asset Owner]*.
      1. *[Include details of other equipment that requires securing, or provide a link to the appropriate work instructions.]*
4. **Clear desk and clear screen policy**
   1. *{OrganisationName}* has adopted a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities, as described in the Individual User Agreement (see [ISMS-C DOC 9](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_9.docm)).

***Document Owner and Approval***

The *{InfoSecManager}* is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to *[all/specified]* members of staff on the *[corporate intranet]* and is published *[ ]*.

This work instruction was approved by the *{ChiefInfoSecOfficer}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |