1. **Organisational Scope**

All information processing equipment owned or used by Retirement Capital is subject to secure siting and protection requirements.

1. **Responsibilities**
   1. The Director (CISO) is responsible for the siting and protection of information equipment.
   2. The Director (CISO) is responsible for ensuring that equipment is protected from possible power supplies and other power-related disruptions.
   3. The Director (CISO) is responsible for cabling security.
   4. The Director (CISO) is Director (CISO) is responsible for the secure siting of all telecommunications facilities.
   5. The Operations Director is responsible for defining and resourcing business continuity needs.
   6. The Managing Director is responsible for insurance.
   7. Where necessary, other responsibilities are identified in the course of this procedure.
   8. Access to secure areas is controlled in line with [ISMS-C DOC 11.1.2](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A11\ISMS-C_DOC_11.1.2.docm).
2. **Siting and protection of equipment** [ISO27002 Clause 11.2.1]

The requirements are:

1. That equipment is sited so as to minimise 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 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 (e.g.: server) is isolated in a secure cabinet.
5. Controls are implemented to deal with theft (see control section 11.1 of the [Manual](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\InfoSecManual.docm)), natural or man-made disaster (see control section 11.1.4 of the Manual), environmental pollution, dust, vibration, chemical effects, electrical supply interference (UiPS) communications interference (faraday cage enclosure), electromagnetic radiation (faraday cage enclosure).
6. Retirement Capital does not allow smoking inside any of its sites, nor does it allow eating or drinking inside secure areas.
7. Secure areas are monitored for temperature and humidity insert details of equipment used, acceptable limits for both have been set (according to manufacturer instructions).
8. Lightning protection is applied to all buildings occupied by Retirement Capital and lightning protection filters are fitted to all incoming power and communications lines.
9. **Supporting utilities** [ISO27002 Clause 11.2.2]
   1. 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 supply (heating, cooling, lighting, fire suppression, alarms, what else?) plus an element for buffer and the Premises Manager has incoming power cables checked by the landlord 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.
10. The Premises Manager is responsible for ensuring that heating and ventilation engineers provide a formal report on the heating, cooling/air conditioning and ventilation requirements of each secure area, and water supply for equipment that requires water, and each site that contains information processing equipment and for reporting on the adequacy or otherwise of current installations.
11. Sewage is to be assessed for adequacy by the landlord.
12. The Premises Manager is responsible for ensuring that all supporting utilities and equipment is inspected (also see [ISMS-C DOC 11.1.11](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A11\ISMS-C_DOC_11.1.11.docm) and [ISMS-C DOC 11.1.2](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A11\ISMS-C_DOC_11.1.2.docm)) on a frequency determined by manufacturer’s recommendations and previous inspections and that inspection certificates are retained in line with control section 18.1.3 of the Manual.
    1. A UPS is installed in each secure area. The specifications of the UPS are adequate for 30-minute uninterrupted supply.
    2. Emergency power down switches are installed near/to the right of emergency exits from all secure areas.
    3. Telecommunications:
    4. Voice services meet the local jurisdictional requirements for supporting emergency communications as the phone locations are registered with the provider.
13. **Cabling security** [ISO27002 Clause 11.2.3]
    1. The Director (CISO) has a site map that identifies all network cabling and all incoming power and telecommunications lines; those lines that are not underground are protected; this is contracted to the managed office supplier.
    2. Network cabling is protected from unauthorised access and power and network cables are segregated and clearly marked for ease of maintenance, managed by the managed office supplier.
    3. Connections to secure areas/specific critical equipment are further protected by:
14. Armored conduit and locked boxes/rooms at inspection and termination points.
15. Secure routing of transmission media.
16. Using fibre optic cabling.
17. Electromagnetic shielding for cables.
18. Technical sweeps and physical inspections by the managed office supplier to ensure that no unauthorised devices are attached to cables.
19. Controlled access to patch panels and cable.
20. Color coded patch cables, together with a documented patch list held by the managed office supplier.

THE CHESSINGTON OFFICES ARE MANAGED BY THE BUILDING SERVICES COMPANY WHO ARE RESPONSIBLE FOR THE ABOVE. ALL COMMUNICATIONS ARE ENCRYPTED.

1. **Equipment maintenance** [ISO27002 Clause 11.2.4]
   1. The Director (CISO) is responsible for ensuring that all equipment on the site is maintained in line with manufacturers’ recommended service intervals and specifications. The Director (CISO) 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 (also see ISMS-C DOC 11.1.11).
   2. Only authorised and experienced maintenance personnel carry out maintenance.
   3. Equipment that processes or stores confidential information is serviced only by technicians who have been screened in line with the requirements of control 7.1.1 of the Manual/is cleaned of confidential information prior to servicing.
   4. Retirement Capital’s insurance policy with Hiscox has no requirements in respect of equipment maintenance.
2. **Unattended user equipment** [ISO27002 Clause 11.2.8]  
   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 company.
   3. Unattended user equipment within its secure area must be left in a secure state.
      1. For workstations, this requires logging out of any secure sessions and locking the device.

***Document Owner and Approval***

The Director (CISO) 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 members of staff on the corporate intranet.

This procedure was approved by the Director (CISO) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |