HybrIT Services

Physical and Environmental Security Policy

Internal Document

Prepared by: Ian Mills

Strictly private and confidential. The content within this document may not be divulged to any third party without the prior written consent of a Director of HybrIT Services.

ISO Document Control

Document Name:	Physical and Environmental Security Policy
Document Reference:	ISMS DOC 11.1.1 - 11.2.9
Version Date:	08/04/2024
Status:	Published
Document Author:	Ian Mills
Document Owner:	Ashley Marshall

Version Control

Date	Revision	Distribution	Overview
18/01/2023	0.1		Draft
18/02/2023	1.0	Internal	Policy Published
08/11/2023	1.1	Internal	Added Clarity re locking devices away at night
12/01/2024	1.2	Internal	Added Pulsant DC updates
08/04/2024	1.3	Internal	Updated to new document template

Contributors

Name	Role	Telephone	E-mail
Dave Landreth	CISO		Dave.landreth@hybrit.co.uk
Ian Mills	COO		Ian.Mills@hybrit.co.uk

Distribution List

Name	Role	Company/Department
Group Wide	All Staff	HybrIT Services

Table of Contents

1 Purpose

This procedure is applicable to all areas within the scope of the ISO 27001 standard as defined in the standard.

2 Secure Areas

The control objective is as follows:

- To prevent unauthorised access, damage and interference to the organisation's information and information processing facilities.

2.1 HybrIT Sites

The sites are:

- HybrIT Weedon – Building 3
- HybrIT Weedon – Building 4
- PLMK – Pulsant Milton Keynes
  - St Neots House, Rockingham Drive, Linford Wood, MK14 6LY
- LDex1 – iomart
  - The Oxgate Centre, Staples Corner, London, NW2 7JA

By use of Risk Assessment, HybrIT has identified product and services that need to be located in high-availability and secure environments, and these are located at external data centres and physical security is managed outside of this ISMS.

2.2 Physical Security Perimeter

HybrIT uses security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

HybrIT's sites at Weedon have physical access controls. The Perimeter is covered by 24x7 CCTV monitoring covering main entrances and working areas. Cameras are positioned so as not to have visibility of screens or secure data.

Access to the cameras is restricted to authorised personnel only.

The LDEX and PLMK locations are professionally managed data centres where only scheduled and approved visits can occur. Data centres are secured by a comprehensive series of physical barriers, pass access, human security guards and video cameras.

2.3 Physical entry controls

Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

All doors to HybrIT work areas are protected by secure access passes as are access to LDEX and PLMK data centres.

Visitors must sign in electronically before a limited access pass is allocated and sign-out as leaving the premises.

PLMK and LDEX Server racks are either locked by key or combination. Keys are stored securely with security or in key safes as appropriate. Access to Servers in Weedon are controlled by secure restricted badge access.

2.4 Securing Offices, Rooms, and Facilities

HybrIT has designed and applied physical security for offices, rooms, and facilities.

All HybrIT offices, rooms and data are contained with secure facilities. Key facilities are located behind multiple layers of security to restrict access by the public.

HybrIT has an intruder alarm within secured areas which is maintained and tested.

2.5 Protecting Against External and Environmental Threats

HybrIT has designed and applied physical protection against damage from natural disasters, malicious attack, or accidents.

HybrIT has assessed the risk of external and environmental threats and has applied controls that are included our business continuity plan.

- Not in a flood zone (high ground).
- Building designed to withstand explosion (Weedon).
- Fire alarms across facilities.

HybrIT has a fire alarm system across the Weedon Office which is maintained and tested and in all other sites as controlled by Pulsant governance and processes.

2.6 Working in Secure Areas

Staff, visitors, and third-party support personnel only have access to secure areas as and when required.

Visitors and 3rd party support personal are accompanied where appropriate unless they or their organisation on their behalf has signed as appropriate non-disclosure agreement. The host is responsible for ensuring that visitors and third-party contractors are aware of the security requirements and comply with these. These rules are explained and signed on entry to the offices.

2.7 Delivery and Loading Areas

HybrIT has a small delivery area and storeroom where parcels and deliveries may be received.

- Storage areas are restricted to approved staff.
- Loading area is sperate from the main office with multiple secure access doors.
- Only expected deliveries are accepted or deliveries from known suppliers.
- Incoming good are rejected were signs of tampering or damage are detected.

PLMK and LDEX Data Centre delivery and loading areas are subject to strict access controls, covered by cameras and human security. Entries are all protected against non-authorised accesses.

3 Equipment

The control objective is as follows:

- To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.

3.1 Equipment Siting and Protection

All equipment is sited to minimise breach of security from external and environmental threats. Computer screens and other documents are positioned/angled to minimise opportunities for viewing by unauthorised persons.

- Smoking is prohibited anywhere within the confines of the building or data centres. Consumption of liquids or food with Data Centres is prohibited. Locations and facilities are provided for eating and drinking.
- Monitoring of temperature and humidity of DC's and offices is undertaken. Back-up air-conditioning unit are available on site in case of outage.
- Surge and UPS protection is in place for DC's.
- Racks are secured with inbuilt key and / or combination locks or physical access controls.

3.1.1 Responsibilities

- The Owners of information assets are responsible for the siting and protection of information equipment.
- The CISO is responsible for ensuring that equipment is protected from possible power supplies and other power-related disruptions, cabling security, secure siting of all telecommunications facilities.
- The COO is responsible for maintenance of equipment, insurance and for defining and resourcing business continuity needs.

3.2 Supporting Utilities

All business-critical systems are in data centres which are designed to have highly available supporting utilities and key applications are cloud-based.

Power to the office buildings is provided by supplies that enter the building from below ground and from two separate sources for added resilience.

Monitoring of temperature and humidity of DC's and offices is undertaken, back-up air- conditioning units are available on site in case of outage.

Surge and UPS protection is in place for DC's.

Telephony connections are via diverse network connections and can be managed and support from cloud services.

3.3 Cabling Security

Data cables enter the building below ground and are routed via protective trunking and power cables enter from underground.

Internal cabling is set into conduit along ceilings and floors to minimise interference, with power cabling being similarly protected. Power cables are separated from network cables to minimise interference.

Data Centres have resilient Power sources and internal to the data centres, power is distributed to the racks in an 1+1 redundancy power model.

3.4 Equipment Maintenance

Weedon:

- Air conditioning in the server room is maintained under agreement.
- Intruder alarm and fire detection systems are maintained - records of such maintenance available.
- All repair and maintenance is conducted by suitable qualified and authorised personnel or subcontractors.
- All faults are logged within the Services Desk ticketing system.

Pulsant provided data centres:

- All power, air conditioning and physical location are supported and maintained as part of the commercial arrangement.

3.5 Removal of Assets

All equipment allowed off-site is authorised by management. Certain equipment (e.g. laptops or mobile phones) are provided as part of a staff member's position and in this case such authorisation is granted automatically as part of the job holder's duties.

Any other equipment taken off site requires a Line Manager to approve such removal. This approval may be granted verbally.

3.6 Security of Equipment and Assets Off-Premises

The following procedures should be followed for equipment and assets taken off premises:

- Equipment (including media) taken off site must not be left unattended in a public place (e.g. airport, railway station etc.).
- Laptops/Notebook computers should be carried as hand luggage and disguised if possible during travel.
- Any relevant advice from manufacturers should be taken into account such as susceptibility and protection against strong magnetic fields.
- Home workers are subject to a risk assessment to identify any relevant risks and the necessary controls. Home workers should comply with the clear desk and clear screen policies, ensure access is controlled as if in the office and have appropriate security measures (e.g. lockable files, secure shredding facilities) as well as secure communications via VPN or similar with the office.
- The company insurance policy provides adequate cover for equipment taken off site except for items that are self-insured where relevant.

3.7 Secure Disposal or Re-Use of Equipment

The following procedures should be followed for the secure disposal or re-use of equipment:

- Once wiped, equipment may be disposed of by sale or as a gift at the discretion of a director.
- Equipment on lease must be wiped before being returned.
- Devices containing restricted information are securely and permanently wiped prior to disposal or re-use. If necessary, the device(s) are put beyond practical use.

- Devices containing confidential information (Confidential or Restricted) that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.
- Portable or removable storage media of any description are destroyed prior to disposal.

3.8 Unattended User Equipment, Clear Desk, and Clear Screen

The following procedures should be followed for unattended user equipment, clear desk and clear screen:

- Where appropriate, paper and computer media are stored in suitable locked cabinets when not in use.
- Confidential or restricted business information, including papers etc., are locked away when not required.
- Active computer sessions should be logged off when work is finished and at the end of each day.
- All information, especially confidential or restricted information, when printed, is cleared from printers immediately.
- Equipment should be protected by a password, screen saver, or equivalent controls when not in use. This should operate within five minutes of no activity, or which is activated when the workstation is unattended.
- Staff must lock their screen when leaving their device.
- When leaving their desks for any length of time (e.g. at the end of the working day) staff should clear away documents.
- Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet at the end of the day and NOT be left unattended overnight. This excludes the build room which is secured with restricted door and building access and is considered a secure location.