DIGITALPOWER UK LTD

Physical Security Policy

Table of Contents

Physical Security Policy

1. Purpose

The Physical Security Policy is applicable to Digital Power UK Ltd. This policy recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its interested parties.

The Physical Security Policy forms a key control to ensure that the confidentiality, integrity and availability of our information assets, are protected effectively and that we can meet our obligations to the interested parties and is applicable for all assets within the scope of information data management

2. Scope

The Physical Security Policy applies to the following sites:

Location	Full Address
Digital Power UK Ltd	
Any other sites by Digital Power UK Ltd	

3. Policy Statement

Secure areas are necessary in order to protect the information assets located within the physical domains used by Digital Power UK Ltd with the aim of preserving Confidentiality, Integrity or Availability. All Digital Power UK Ltd sites which are used to create, process, transmit and store data, including operational management of these assets must be physically secure.

Physical security must adopt a layered approach which begins at the perimeter of buildings working inwards towards the location of information assets within physical sites.

To inform the selection of physical security controls all sites shall undertake a risk assessment to support the selection of controls identifying the adequacy and completeness of controls implemented and identifying residual[1] risk as appropriate.

Each site shall assess the adequacy of its physical security controls against the areas identified in this policy as a minimum requirement.

3.1 A.11.1 Secure Areas

Secure areas comprise controls that protect against unauthorised access, damage and interference to Shared Services premises, equipment and information, for example data centres. Digital Power UK Ltd should ensure that the sites covered under this policy are appropriately secure, with the objective of protected infrastructure facilities and the control of access to them.

The importance placed on the physical security of an area should reflect the Information Classification of the data stored there. Therefore, the physical security of any secondary site is subject to the same

[1] Residual risk is that part of risk which is left after controls have been applied and is deemed acceptable to the risk owner with consideration made to the Organisations risk appetite policy

criteria as the corresponding primary site.

Asset owners shall determine appropriate access control rules, access rights and restrictions for user roles specific to their assets. The level of rigour applied with security controls shall be to limit access and manage access reflective to the associated information security risks and security classifications assigned to each asset as given in Asset Control Matrix.

The Security manager will enforce the Access Control Policy and ensure each Asset Owner adheres to the relevant requirements provided by it.

3.2 A.11.1.1 Physical Security Perimeter

Physical barriers should be in place to ensure Physical Protection. The following controls must be covered to ensure a secure perimeter:

- A clearly defined perimeter, defined by fences, walls, gates and external doors which are strong enough to resist most breaches and protect against unauthorised access
- Physical access to the building is controlled, e.g. by a reception area
- Intruder detection systems and monitoring

3.3 A.11.1.2 Physical Entry Controls

Protected areas should have entry controls to ensure that only authorised personnel can gain access. The following controls must be covered to ensure that only authorised personnel can gain access:

- Regular review of access rights, particularly to secure areas
- Visitors are escorted at all times
- There is a record of date and time of visitor entry/departure
- Visitors are restricted to specific, authorised purposes
- All Digital Power UK Ltd Staff should challenge unknown visitors to site to ascertain their purpose of being there

3.4 A.11.1.3 Securing Offices, Rooms and Facilities

Secure areas should be protected from human threats. For these purposes the following controls should be in place:

- Secure areas should be located away from public access areas
- Rooms containing servers and confidential assets should not be signposted to provide minimum indication of their purpose
- Windows and doors should be locked, particularly at any time premises are left unattended
- Backup media is located away from the main site
- Windows should be tinted on ground level offices
- Access control mechanisms are fitted to all accessible doors

3.5 A.11.1.4 Environmental Protection

Secure areas and areas containing equipment should be protected from environmental hazards. The following controls should be in place to reduce environmental risks:

- Buildings should be physically strong, and capable of withstanding non-exceptional weathering. Any weaknesses should be reported and sought to rectify immediately.
- Primary and secondary data centre should be in physically separate locations so in case of destruction the relevant system components should failover from its primary data centre to its secondary

3.6 A.11.1.5 Working in Secure Areas

Access to secure areas should be assigned following sufficient screening as detailed in HR Screening Policy. Access should be assigned according to the Access Control Policy.

Those who have been granted access should be responsible for the following:

Those granted access should:	Those granted access should not:
Understand the specific instructions for all secure areas to which they are granted access	Keep secure doors open for longer than necessary
Challenge and/or report anyone suspicious, or any suspicious activity within the building.	Allow anyone without access to work in the area alone unless by arrangement
Escort visitors at all times	Lend anyone their access card
Inspect deliveries as soon as possible	Expose their access card to possible theft or loss
Check doors and windows when they are leaving the room vacant for any amount of time	Tell anyone or write down the door codes
Inform security/reception of any visitors you are expecting	Leave restricted or confidential information unattended in clear view

Table 1: Expected Behaviour of Employees Granted Access to Secure Areas

3.7 A.11.1.6 Delivery and Loading Areas

Deliveries should be secured by the building premises and are not available outside of working hours. Deliveries are always monitored.

3.8 A.11.2 Equipment Security

Equipment, including equipment used off-site must be protected in order to minimise the risk of unauthorised access to data, avoid loss or damage, and to ensure infrastructure remains available. This protection covers equipment siting and disposal.

3.9 A.11.2.1 Equipment Siting and Protection

The following controls should be in place to reduce the risks from human and environmental hazards to equipment.

- Precautions are taken to reduce the risk of others seeing sensitive information, for example tinted windows
- Personnel shall not eat, drink or smoke within vital areas such as server rooms
- Paper based information should be assigned an owner and a classification as given in [ICP] and stored according to that classification
- If possible, assets, or storage containing assets, which contain classified data should be physically attached to the building
- Precautions should be taken to limit the risks from environmental hazards such as heat, fire, smoke, dust, water and vibration

3.10 A.11.2.2 Supporting Utilities

Supporting utilities should be used to provide appropriate environmental protection to equipment. The following controls should be used:

- Power conforms to the equipment manufacturer's specifications
- Backup power supply to servers

3.11 A.11.2.3 Secure Cabling

Cabling should be kept secure from environmental and man-made risks to reduce interference and reduce the ease of hackers gaining access to the network. The following controls should be used:

- Power cables should be separated from network cables
- Network cables should be protected by conduit and where possible avoid routes through public areas
- The code for labelling of cables should be classified as confidential

3.12 A.11.2.4 Equipment Maintenance

Digital Power UK Ltd should correctly maintain equipment to ensure their continued availability and integrity. The following controls should be used:

- Equipment maintenance is compliant with the manufacturer's recommendations
- All repairs and services are only performed by authorised and accredited maintenance personnel
- Records are made of all remedial work carried out
- Compliance is ensured with all insurance policy requirements

3.13 A.11.2.5 Removal of Assets

Controls are placed on any media (external hard drives, USB Memory Sticks, Laptops etc.) which are to be removed from storage or from the site. The following controls are in place:

- The media should be labelled externally with its asset number
- A record should be made of when and to whom the media has been issued
- A User's line manager must approve the asset being removed from storage for use
- Offsite removal of equipment must be authorised by the Managing Director

3.14 A.11.2.6 Security of Off-Site Assets

Protection of equipment off-site should be equivalent to that for on-site equipment. The following controls should be in place:

- Cables that carry data or support key information services must be protected from interception or damage
- Equipment and media should not be left unattended in public places
- When travelling assets should be carried as hand luggage
- Compliance is ensured to manufacturers' instructions for protecting equipment
- Adherence is made to A.11.2.9 Clear Desk and Screens Policy
- Laptops are protected with access controls
- All assets should be protected according to the data stored on the device. Accordingly, off-site assets should be treated as per Information Classification Policy

3.15 A.11.2.7 Secure Disposal and Re-Use

When equipment or media is no longer needed it should be returned to Digital Power UK Ltd Senior Management and, on its return, updated in the support inventory and data erased permanently using dedicated disk wiping software according to Information Classification Policy.

When obsolete equipment or media has reached the end of its life it must be destroyed. If data has been erased this should be in an environmentally friendly manner using companies that follow the Waste Electrical and Electronic Equipment Directive Regulations. If any data cannot be wiped from the equipment or media, then it should be destroyed using a trusted third party who should be required to issue a Certificate of Secure Destruction.

3.16 A.11.2.8 Unattended User Equipment

When equipment is unattended the User should adhere to the A.11.2.9 Clear Desk and Screens Policy.

3.17 A.11.2.9 Clear Desk and Screens Policy

Digital Power UK Ltd Clean Desk and Clear Screens policy should ensure that all classified materials are non-visible and secured when not in use and that data on Computer Screens should only be viewable by the intended user. In this policy, 'desk' refers to the employees' desktop, chair, computer, phone and surrounding floor area. 'Classified' refers to anything that is classified as restricted or confidential according to Information Classification Policy.

The following policy applies to all Shared Services Staff:

- All classified information in hardcopy or electronic form is secure and locked away when not in use or when the employee leaves their workstation
- Filing cabinets containing classified information must be kept closed and locked when not in use
- Keys for access to classified information must not be left at an unattended desk
- When unattended in the office, laptops must be either locked with a locking cable, locked in a drawer, or locked to a docking station
- Passwords must not be written down except if locked away and treated as classified. The password owner must be the only key holder if the password is locked away.
- Printouts containing classified information must be immediately removed from the printer
- Upon disposal, protected and classified documents should be destroyed by the cross-cut shredder.
- Whiteboards containing classified information should be erased
- Storage devices such as USB Drives should be treated as classified and secured in a locked drawer when not in use
- Computer workstations must be locked when the desk is unoccupied
- Computer workstations shall automatically lock after 10 minutes of inactivity
- Computer workstations should be completely shut down at the end of the workday

4 Internal Audit

Digital Power UK Ltd will conduct ad hoc internal audits of the Physical Security in place at all sites in order to assess and document the effectiveness of the physical security measures at protecting the company's assets. These audits will occur at least once annually.

Digital Power UK Ltd will adopt an assessment method which is closely aligned to the CPNI guidance on physical security (Security Assessment for Protectively Marked Assets (SAPMA)) or equivalent.

According to this standard, Digital Power UK Ltd should maintain the following minimum-security requirements for protected, restricted and confidential assets.

This is based on threat agents who may attempt to compromise the system through physical vulnerabilities:

Confidential	Other sites of Digital Power UK Ltd Offices	Main office
Physical Barrier requirements	Severe	Severe
Justification	A burglar poses a moderate threat level to the data centre. Physical barriers should be severe to ensure that access is not possible by compromise of the physical barrier. E.g. Breaking in through a window. Level of requirements is raised to 'Severe' due to the confidential classification of the asset.	A burglar poses a moderate threat level to the Ransom Hall South Office. Physical barriers should be severe to ensure that access is not possible by compromise of the physical barrier. E.g. Breaking in through a window. Level of requirements is raised to 'Severe' due to the confidential classification of the asset.
Access Control Requirements	Severe	Moderate
Justification	Staff of other data centre tenants pose a moderate threat. As they will have authorised access to the data centre, further access controls such as 'escorting visitors' are required to ensure they are only granted access to their respective data racks. Due to confidential classification of the asset, requirement level is set to 'severe'.	Highest physical threats with regards to access control are from unauthorised access to the office from Digital Power UK Ltd Staff and unsupervised cleaners or visitors. The threat levels of these agents are all 'Negligible.' Due to the confidential classification of the asset, requirement level is set to 'Moderate.'
Detection Requirements	Severe	Severe
Justification	Other sites of Digital Power UK Ltd Staff are of moderate threat to data centre as they will have authorised access. To mitigate this risk substantial detection systems should act as a deterrent to compromise the asset. Level of requirements is raised to 'Severe' due to the confidential classification of the asset.	A burglar poses a moderate threat level. Severe detection systems should be used as a deterrent for burglars. Level of requirements is raised to 'Severe' due to the confidential classification of the asset.

Restricted	Other sites of Digital Power UK Ltd Offices	Main office
Physical Barrier requirements	Substantial	Substantial
Justification	A burglar poses a moderate threat level to the data centre. Physical barriers should be substantial to ensure that access is not possible by compromise of the physical	A burglar poses a moderate threat level. Physical barriers should be substantial to ensure that access is not possible by compromise of the physical barrier. E.g. Breaking in

	barrier. E.g. Breaking in through a window. Level of requirements is raised to 'substantial' due to the restricted classification of the asset.	through a window. Level of requirements is raised to 'Severe' due to the restricted classification of the asset.
Access Control Requirements	Substantial	Moderate
Justification	Staff of data centre pose a moderate threat. As they will have authorised access to the data centre, further access controls such as 'escorting visitors' are required to ensure they are only granted access to their respective data racks. Due to restricted classification of the asset, requirement level is set to 'substantial'.	Highest physical threats with regards to access control are from unauthorised access to the office from Digital Power UK Ltd Staff and unsupervised cleaners or visitors. The threat levels of these agents are all 'Negligible.' Due to the restricted classification of the asset, requirement level is set to 'Moderate.'
Detection Requirements	Substantial	Substantial
Justification	Other sites of Digital Power UK Ltd Staff are of moderate threat to data centre as they will have authorised access. To mitigate this risk substantial detection systems should act as a deterrent to compromise the asset. Level of requirements is raised to 'Substantial' due to the restricted classification of the asset.	A burglar poses a moderate threat level. Substantial detection systems should be used as a deterrent for burglars. Level of requirements is raised to substantial due to the restricted classification of the asset.

Protected	**Other sites of Digital Power UK Ltd Offices**	**Main office**
Physical Barrier requirements	Moderate	Moderate
Justification	A burglar poses a moderate threat level to the data centre. Physical barriers should be moderate to ensure that access is not possible by compromise of the physical barrier. E.g. Breaking in through a window.	A burglar poses a moderate threat level. Physical barriers should be moderate to ensure that access is not possible by compromise of the physical barrier. E.g. Breaking in through a window.
Access Control Requirements	Moderate	Low
Justification	Staff of data centre pose a moderate threat. As they will have authorised access to the data centre, further access controls such as 'escorting visitors' are required to ensure they are only granted access to their respective data racks.	Highest physical threats with regards to access control are from unauthorised access to the office from Digital Power UK Ltd Staff and unsupervised cleaners or visitors. The threat levels of these agents are all 'Negligible.' As no classified data should be stored with any aspects of physical security measures as 'Negligible' this is

		raised to 'Low'
Detection Requirements	Moderate	Moderate
Justification	Other sites of Digital Power UK Ltd Staff are of moderate threat to data centre as they will have authorised access. To mitigate this risk moderate detection systems should act as a deterrent to compromise the asset.	A burglar poses a moderate threat level. Substantial detection systems should be used as a deterrent for burglars. Level of requirements is raised to substantial due to the confidential classification of the asset.

5 Policy Change Control

This Policy document will be formally controlled and used as the basis for monitoring and measuring compliance of Physical Access processes and procedures.

Any changes to this policy shall only occur after completing a risk assessment against the changes for Digital Power UK Ltd, and its effected customers.

Consequences

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers. If any employee is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).