Physical Security Policy

Document Ref.	**GDPR-DOC-10-5**
Version:	**1**
Dated:	**16 May 2018**
Document Author:	**Steve Brown**
Document Owner:	**Steve Brown**

Revision History

Version	Date	Revision Author	Summary of Changes
1	16/05/2018	Steve Brown	N/A

Distribution

Name	Title
Public	Available via website

Approval

Name	Position	Signature	Date
Steve Brown	GDPR / Data Protection Officer		15/05/2018

Contents

1 Introduction

The protection of the physical environment is one of the most obvious yet most important tasks within the area of information security. A lack of physical access control can undo the most careful technical precautions and potentially put lives at risk.

Ipswich Rugby Football Club Limited is committed to ensuring the safety of its employees, contractors and assets and takes the issue of physical security very seriously. This policy sets out the main precautions that must be taken and, together with the supporting documented listed, forms a significant part of our information security control set.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Ipswich Rugby Football Club Limited systems.

2 Secure Areas

Sensitive information must be stored securely. A risk assessment must be conducted to identify the appropriate level of protection to be implemented to secure the information being stored.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. A building must have appropriate control mechanisms in place for the classification of information and equipment that is stored within it.

These may include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours
- Window and door locks
- Window bars on lower floor levels
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building)
- CCTV cameras
- Staffed reception area
- Protection against damage - e.g. fire, flood, vandalism

Staff working in secure areas must challenge anyone not wearing a badge.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by persons authorised to access those areas and must not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge.

An organization employee must monitor all visitors accessing secure areas at all times.

Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by the Facilities Manager, as appropriate.

Where breaches do occur, or an employee leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) must be recovered from the employee and any door/access codes should be changed immediately.

3 Paper and Equipment Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification. Appropriate information security controls must be put in place to protect it according to the provisions in the relevant asset handling procedures.

Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a secure area protected by access controls

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration
- Limit the risk of theft – e.g. if necessary items such as laptops should be physically attached to the desk
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people

Data must be stored on network file servers where available. This ensures that information lost, stolen or damaged via unauthorised access can be restored and its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment.

Business critical systems must be protected by an Un-interruptible Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.

All items of equipment must be recorded in the IT Service Desk inventory. Procedures must be in place to ensure the inventory is updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number must be recorded in the IT Service Desk inventory.

Cables that carry data or support key information services must be protected from interception or damage.

Power cables must be separated from network cables to prevent interference. Network cables must be protected by conduit and where possible avoid routes through public areas.

4 Equipment Lifecycle Management

Ipswich Rugby Football Club Limited and relevant 3rd party suppliers must ensure that all of Ipswich Rugby Football Club Limited's IT equipment is maintained in accordance with the manufacturer's instructions and any documented internal procedures to ensure it remains in effective working order.

Staff involved with maintenance must:

- Retain all copies of manufacturer's instructions
- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorised technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements
- Record details of faults incurred and actions required

A service history record of equipment must be maintained so that decisions can be made regarding the appropriate time for it to be replaced.

Manufacturer's maintenance instructions must be documented and available for support staff to use when arranging repairs.

The use of equipment off-site must be formally approved by the user's line manager.

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organization (e.g. returned under a leasing agreement) data removal must be achieved by using approved, appropriately secure software tools.

Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process must confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.

Loading areas and holding facilities must be adequately secured against unauthorised access and all access must be auditable.

Subsequent removal of equipment must be via a formal, auditable process.

Information security arrangements must be subject to regular independent audit and security improvements recommended where necessary.