**Company Physical Security Policy**

**Doc A11**

**Version: 1.0**

Publication Date: January 2019

Current Status: Published

Author(s): Michael Woolard

Reviewed By: Michael Woolard

**Table of Contents**

1 Company Physical Security 3

1.1 Scope 3

1.2 Responsibilities 3

1.3 Security Breaches and Weaknesses 3

2 The Approach to Physical Security 3

2.1 Risk Assessment 3

3 Physical Security Controls 3

3.1 Perimeter 3

3.2 Building Alarms 4

3.3 CCTV 4

3.4 Secure Zones 4

3.5 Equipment siting and protection 4

3.6 Supporting utilities 4

3.7 Cabling security 4

3.8 Equipment Maintenance 5

3.9 Removal of Equipment and Security of equipment off-premises 5

3.10 Care of equipment 5

3.11 Secure disposal or re-use of equipment 5

3.12 Unattended User Equipment 6

3.13 Clear Desk / Clear Screen / Clear Board 6

3.14 Lighting 7

3.15 Server Rooms 7

3.16 Building Construction 7

4 Procedures 7

4.1 Visitors 7

4.2 Access Card Systems 8

4.3 Keys and Alarm Codes 8

5 Document Control and Approval 9

5.1 Distribution 9

5.2 Version Information 9

Annex A: Site Managers 10

1. Overview 10

2. Site Manager List 10

Annex B: Local Policies 11

Spain 11

France 11

EU 11

# Company Physical Security

## Scope

This policy is applicable to all areas within the scope of the Information Security Management System (ISMS) as defined in the ISMS Manual.

Failure to comply with this policy may result in disciplinary action under the Company’s Disciplinary Procedure and in serious cases, may be treated as gross misconduct leading to dismissal.

Where local laws and regulations may require a custom policy change, this must be reviewed by Wacky Widget legal team and the CISO. All local policies are documented in Appendix B

## Responsibilities

Each Wacky Widget office will have a designated site manager who takes overall responsibility for physical security for that office – documented in Annex A.

## Security Breaches and Weaknesses

All Staff are required to note and report any observed or suspected security weaknesses in, or threats to, physical security.

Unless there is an emergency situation, Information Security weaknesses, events and incidents must be raised to the service desk ticketing portal, or phone the help desk, as soon as they are seen or experienced.

# The Approach to Physical Security

## Risk Assessment

Appropriate physical security controls will be implemented at each location based on an assessment of the risks that apply.

The risk assessment will be carried out by the Site Manager and must be reviewed when circumstances change.

It is not necessary for all controls to be implemented at all locations.

# Physical Security Controls

## Perimeter

All offices and data centers in scope have a secure perimeter which ensures that persons not in scope do not have ready access to secure areas. The boundary between public and private areas of the site must be clearly indicated.

Some buildings in scope may be managed by landlords, in such cases, the Site Manager maintains the relationship with the landlord for ensuring appropriate information security controls are in place.

## Building Alarms

The building must be protected by an intruder detection system, which will be activated while the building is not occupied, to detect an intruder and sound an external alarm.

## CCTV

CCTV cameras are installed in accordance with the relevant laws that apply in the country where the office is located. See Appendix B.

CCTV cameras must be installed in a secured server room and access to the CCTV system must be carefully restricted to appropriate staff only.

CCTV equipment should be installed in such a way to prevent tampering. This may include installing key equipment such as that holding the recordings, in a secure area.

## Secure Zones

Access to secure areas / areas where open or confidential information is processed (including in conversation) or stored is restricted to authorized persons. Depending on the sensitivity of the work carried out in a part of the building, or of the information stored, other secure zones with restricted access may be sensible.

Access to secure zones may be controlled by access card system, key lock or other appropriate control.

## Equipment siting and protection

All equipment is sited so as to minimize breach of security from external and environmental threats. Computer screens and other documents are positioned/angled so as to minimize opportunities for viewing by unauthorized persons. Screen protectors are used where appropriate.

## Supporting utilities

Power supplies (fixed wiring) are inspected and tested on a periodic basis.

## Cabling security

Data cables are routed via protective trunking where required. Internal cabling is set into conduit buried in walls, ceilings and floors to minimize interference. Power cabling is similarly protected and where necessary are separated from network cables to minimize interference.

## Equipment Maintenance

Infrastructure equipment (air conditioning systems, electrical wiring etc.) are subject to regular planned maintenance. Relevant records of maintenance are retained (e.g. faults and remedies as well as preventive and corrective maintenance).

All repair and maintenance is conducted by suitable qualified and authorized personnel or subcontractors.

## Removal of Equipment and Security of equipment off-premises

All equipment allowed off-site is authorized 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 authorization is granted automatically as part of the job holder’s duties. If you are permanently issued with portable IT equipment such as a laptop or smart phone you will be given the appropriate form at the time the equipment is issued to you.

All IT equipment taken off site requires a manager in IT, a Manager or a Director to approve such removal, and will be logged on the relevant form.

Certain types of loan equipment (loan laptops, projectors) are tracked separately and the responsibility for tracking the location of the equipment rests with the issuing party.

When returned, such property will be checked as necessary by IT and wiped of any information as appropriate.

Equipment (including media) taken off site must not be left unattended in a public place (e.g. airport, railway station etc.).

## Care of equipment

Laptops and other portable equipment, are assigned by the Company to Staff whose jobs require them. It is the responsibility of Staff to take appropriate care of such equipment to minimize the likelihood of damage or theft.

* No piece of computer equipment is to be left unattended in a motor vehicle overnight
* IT devices containing sensitive data should not be left on desks in the office overnight
* Loaned equipment should always be returned to reception at the end of the day unless noted.

## Secure disposal or re-use of equipment

Hard disks are cleared of all software and all Company information prior to disposal or re-use, as set out below.

The Internal IT Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is carried out by the IT department.

A log is retained showing what media were destroyed, disposed of, and when.

The asset inventory is adjusted once the asset has been disposed of.

Devices containing confidential information are wiped prior to disposal and are never re-used. If necessary, the device(s) are put beyond practical use.

Devices containing confidential information that are damaged should be assessed 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.

All media are disposed of in line with US DOD standards on disposal of computer equipment, through an approved contractor. The contractor is a licensed waste carrier and relevant Waste Transfer Notes are retained by IT for minimum of two years.

Documents containing confidential information which are to be destroyed are shredded by their owners or disposed of as confidential waste. The contractor employed is a registered waste carrier and provides Certificates of Destruction where appropriate and Waste Transfer notes which are retained for a minimum of two years.

## Unattended User Equipment

Laptops and printers are not left logged on when unattended and are protected by passwords. Tethers are used where appropriate.

All information, especially Confidential or Restricted information, when printed, is cleared from printers immediately.

All laptops are protected by passwords, screen savers or equivalent controls when not in use.

Staff must lock computer screens when leaving their computer equipment unattended.

## Clear Desk / Clear Screen / Clear Board

The Company operates a clear desk policy at all of its offices. This means that all Staff are expected to leave their desks clear, tidy and free of paperwork classified at, or above, restricted at the end of each working day. This not only includes documents and notes, but also post-its, business cards and removable media (CDs, floppy disks, memory sticks).

When leaving desks in an open area for any length of time (e.g. at the end of the working day) staff should clear away classified documents.

Company Sensitive, Personally Identifiable or PCI, and Company Secret information must be locked away when not required.

All staff are required to lock their screen when leaving their desk/computer using the [WIN]+L combination.

All whiteboards in shared meeting spaces must be wiped as soon as the meeting is adjourned. Individual whiteboards used in employee areas may not store any information classified company sensitive and above.

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.

## Lighting

Appropriate internal and external lighting should be set to deter intruders.

## Server Rooms

Server rooms and other sensitive areas containing infrastructure must be secured so that only authorized Staff are permitted entry.

Server rooms must be physically separated from the main office areas.

Server rooms must not contain windows.

Server rooms must have continuous environmental monitoring of temperature, humidity, smoke, water.

## Building Construction

Buildings are built in compliance with local, relevant building regulations where applicable, and away from known environmental hazard locations, such as flood plains.

Required construction materials include:

* Fire retardant materials to minimize the spread of fire should a fire occur.
* External doors must be sufficiently strong to either prevent or deter an attacker from forcing unauthorized entry.
* External windows should provide some resistance to forced attack.

# Procedures

## Visitors

Visitors must be recorded upon entry and exit to the building. The following minimum information must be recorded:

* Name and Company of visitor
* Name of Staff being visited
* Time and date of entry
* Time and date of exit

With an exception of trusted suppliers:

* External visitors should be escorted by a Staff member at all times.
* External visitors must not be given keys or swipe cards to permit independent travel through the building unless they are on the approved supplier list.

External visitors must be clearly identifiable. They must wear a visitor badge.

If Staff see some-one that they think may be an unaccompanied visitor, they should escort the visitor back to their host or back to reception. If this is not possible Staff should notify a manager immediately.

## Access Card Systems

Some offices will be equipped with card based door access systems to ensure that only authorized Staff can access certain parts of the building, and to keep a log of each access when it occurs.

The access card system will be administered by the Site Manager or this may be delegated to a specific Access Controller.

Measures will be taken to ensure the access card system cannot be tampered with and to ensure that changes to the system can only be made by the designated Access Controller.

Access cards will be issued to Staff when they join the company. Access to main Staff areas will be permitted to all Staff. Certain restricted areas will require separate approval by the relevant management.

At offices where access cards are issued, Staff must display their access card at all times whilst in the office. This applies to visiting staff using visitor access cards and staff using cards issued to them.  Lanyards can be used allow these to be hung around the neck or they can be clipped to clothing.

Access cards must only be used by the person they were issued to.

Access cards must be returned when Staff leave the company. It is the line Manager’s responsibility to ensure this happens. If an access card is not returned it must be disabled so that it cannot be used.

All issued access cards and their access will be reviewed annually.

Access must be adjusted as appropriate if Staff change job roles.

Loan passes may be borrowed by Staff visiting from other offices or who are temporarily without their own passes. The issue and return of these must be tracked and maintained.

## Keys and Alarm Codes

Keys and alarm codes will be issued to authorized key holders for each location.

Approval to be a key holder must be given by the relevant site manager or a director.

A log must be kept for all keys issued. This must be updated when keys are returned.

Alarm codes should be changed regularly (at least annually) or when a key-holder who knows the code leaves the company.

# Document Control and Approval

The Chief Information Security Officer 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 and is the published version.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Annex A: Site Managers

## Overview

This Annex lists the Site Managers who are responsible for physical security at each Company office.

## Site Manager List

Chicago, US John Doe

Barcelona, Spain Alejandro Doe

Lyon, France Jean Deux

Bengaluru, India Sanjay Doe

# Annex B: Local Policies

## Spain

In Spain it has been agreed that fire drills may be undertaken every two years. This is consistent with local laws and matches the standard services provided by both landlords.

## France

In France it has been agreed that fire drills may be undertaken every two years. This is consistent with local laws and matches the standard services provided by both landlords.

## EU

Signage stating CCT cameras are in use is required under GDPR.