

GDPR Assessment

Site Walkthrough Checklist

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the organisation specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the organisation or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 1/18/2018

Prepared for:
Your Company
Prepared by:
Wem Technology Ltd

18/01/2018

Table of Contents

1 - [Issue Checklist](#)

1.1 - [Issue Checklist](#)

Issue Checklist

1.1 - Issue Checklist

As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you find. Note: The end of each checklist item includes the associated section in ISO 27001, which details the information security controls necessary to achieve the ISO 27001 standard.

<input checked="" type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input checked="" type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input checked="" type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organizations information processing facilities (11.1.1g)
<input checked="" type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input checked="" type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)
<input checked="" type="checkbox"/>	Lack of authentication mechanism to secure areas (11.1.2b)
<input checked="" type="checkbox"/>	Lack of physical or electronic audit trail for all access to secure areas (11.1.2c)
<input checked="" type="checkbox"/>	Employees, contractors, or external parties in secure area without visible identification (11.1.2d)
<input type="checkbox"/>	Un-monitored third-parties in secure areas (11.1.2e)
<input type="checkbox"/>	Direct access by public to key facilities (11.1.3a)
<input checked="" type="checkbox"/>	Obvious signage indicating the presence of information processing activities (11.1.3b)
<input type="checkbox"/>	Computer monitors positioned such that they are visible from outside the facility (11.1.3c)
<input type="checkbox"/>	Directories or internal telephone books identify locations of confidential information processing facilities readily accessible to unauthorised personnel (11.1.3d)
<input type="checkbox"/>	Computer monitors are positioned such they are visible from unauthorised persons during their use (11.2.1b)
<input type="checkbox"/>	Storage facilities are not secured to prevent unauthorised access (11.2.1c)
<input checked="" type="checkbox"/>	Lack of cabling security could allow unauthorised access (11.2.3)
<input checked="" type="checkbox"/>	Sensitive information on paper found in unlocked areas (11.2.9a)