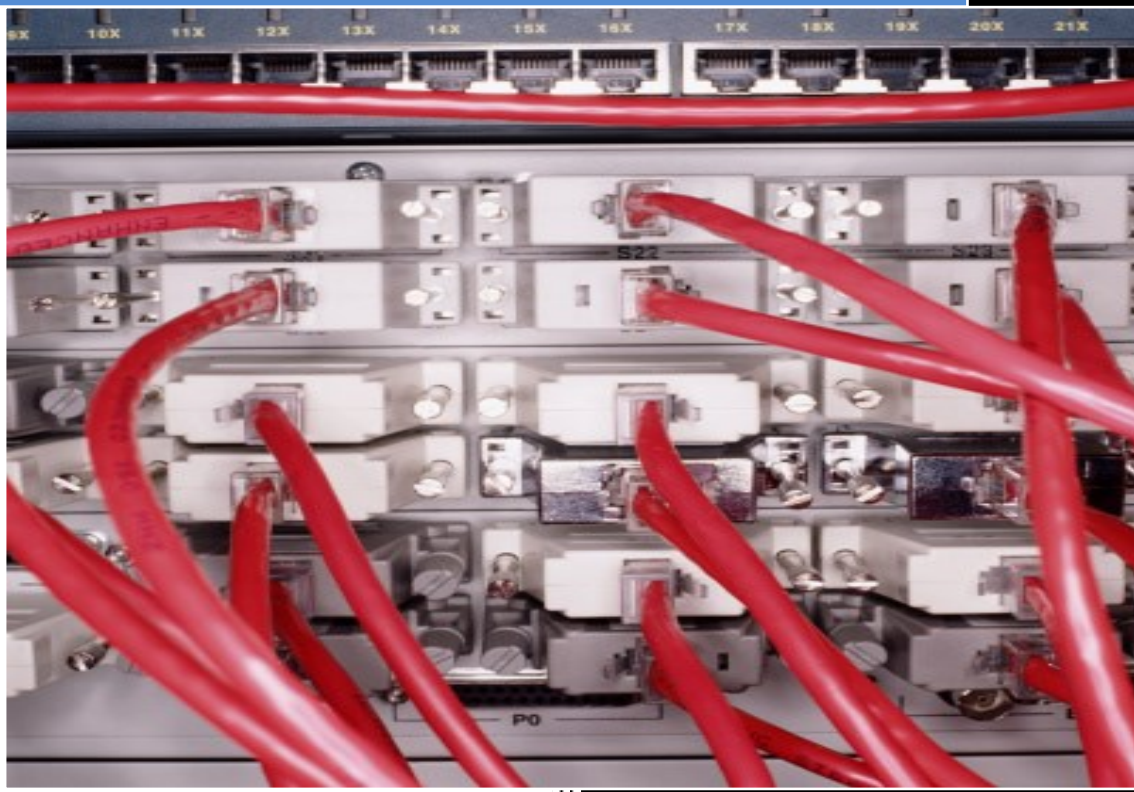
YourIT!
Your Logo Goes Here

GDPR Assessment

Site Walkthrough Checklist



Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company

1/18/2018

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.

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