T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber security

Assignment 3

Company overview

v1.1: Specimen assessment materials
21 November 2023
603/6901/2

Internal reference: DSS-0013-06

NCFE

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA)

Cyber Security

Company overview

Assignment 3

Contents

Company overview

This document is included in the 30 minutes reading time for assignment 3.

Introduction

Willow Technology is a reasonably new company that develops software for audio-visual/conferencing communication. It has over 100 employees of which a large number are remote workers. There is a small administrative team based in the head office along with an IT support team. Remote workers visit the site regularly to get access to the network and use the hot desks. There is also a first floor in the building that facilitates a range of developers and designers. The developers are working on Windows-based systems whilst the designers utilise Apple Macs.

Physical security

The office is based on an industrial site that has its own 6-foot perimeter fence and gate. This gate is left unlocked for the purpose of convenience. Dummy cameras are situated at all 4 corners of the fencing. The building is also surrounded by a car parking area that is used by many people and not necessarily just employees and visitors.

Entrance to the building is through the main door that then leads to the reception on the ground floor. This is left unlocked throughout the day to allow access for visitors. There is an additional entrance for remote workers that leads straight through to the hot desk area. This office space is utilised on a regular basis as this is encouraged by management. There is a fire door on the ground floor. at the rear of the building. In hot weather the fire door is left open to allow cool air into the building. None of the entrances are currently alarmed. Due to the age of the building, there is currently no air conditioning available throughout. However, there are multiple large windows scattered throughout the building that can be opened to allow air flow, although occasionally these have been left open after the building closes.

Currently, the reception has a sign-in book on the desk and this is manned part time. The computer is usually left logged in at the desk to allow easy access as required. The manager and IT teams have their own office whilst all other workers utilise either the hot desk area or the first floor workspace, which is open plan, although desks do have dividing panels to allow staff some privacy whilst working. There is also a server room at the back of the ground floor of the building.

The management team have identified a need for physical security measures but are unsure which measures would be the easiest to implement, the best to install, and the most cost effective.

IT systems

All IT systems are currently housed internally so the team can maintain control of everything. The server room contains everything required for employees to access software and files as well as supporting the company website.

Typical IT operations include:

- ground floor:
  - 1 x manager computer (Windows)
  - 3 x IT support staff (Windows)
  - 1 x reception (Windows)
  - 1 x server
  - 1 x file server
  - 1 x web server
  - 4 x printer
  - 32 x network ports within the hot desk area
  - public wireless network access point
- first floor:
  - 3 x developer manager computer (Windows)
  - 3 x designer manager office (Mac)
  - 14 x developers (Windows)
  - 10 x designers (Mac)
  - 12 x network ports within the hot desk area
  - public wireless network access point

Process and procedures

As this is a new company, they are aware that they currently do not have the required policies and procedures in place, and the ones they do have may not be tested or reliable. They do have a procedure in place for new employees starting at the company. All new staff are issued with a company laptop and phone. As all designers are based on site, and they are the only people using MacOS. All company laptops are Windows based.

Cloud services

All users have access to cloud services enabling the storing of documents and data. Users can share and collaborate using the cloud and can access their areas from home.

Backups

Full data backups are taken once a month and stored in the server room to allow easy recovery if required.

Laptops

All laptops are connected to the company virtual private network (VPN).

Username: company email address (firstname.surname@willowtechnology.com)

Password: Pa$$w0rd

It is recommended that employees change their password within the first week of receiving the laptop, and then change it every 6 months. It is also recommended that employees do not use their name or email address as a password.

As many remote workers are software developers, all employees have local administration rights for their laptops so they can install software as required.

As most staff are competent software developers, it was identified that there is no requirement for additional anti-virus and a firewall as the operating system has enough protection built into it, and staff are competent in their IT use.

Mobile phones

Smartphones are provided to all staff working remotely. These are Android devices with no security restriction in place. This allows staff to install apps as required.

ID cards

All staff are issued with ID cards, although there are no rules enforcing them to use these.

Wireless network access

Public WiFi is available to staff and visitors to allow easy internet access.

Users

As employees may be working across multiple projects all staff have access to everything, which has reduced administration tasks.

IT team

The IT team consists of a network manager, one 1st line support staff member and one apprentice. All correspondence with the IT team is through phone or email as there is currently no ticket-based system.

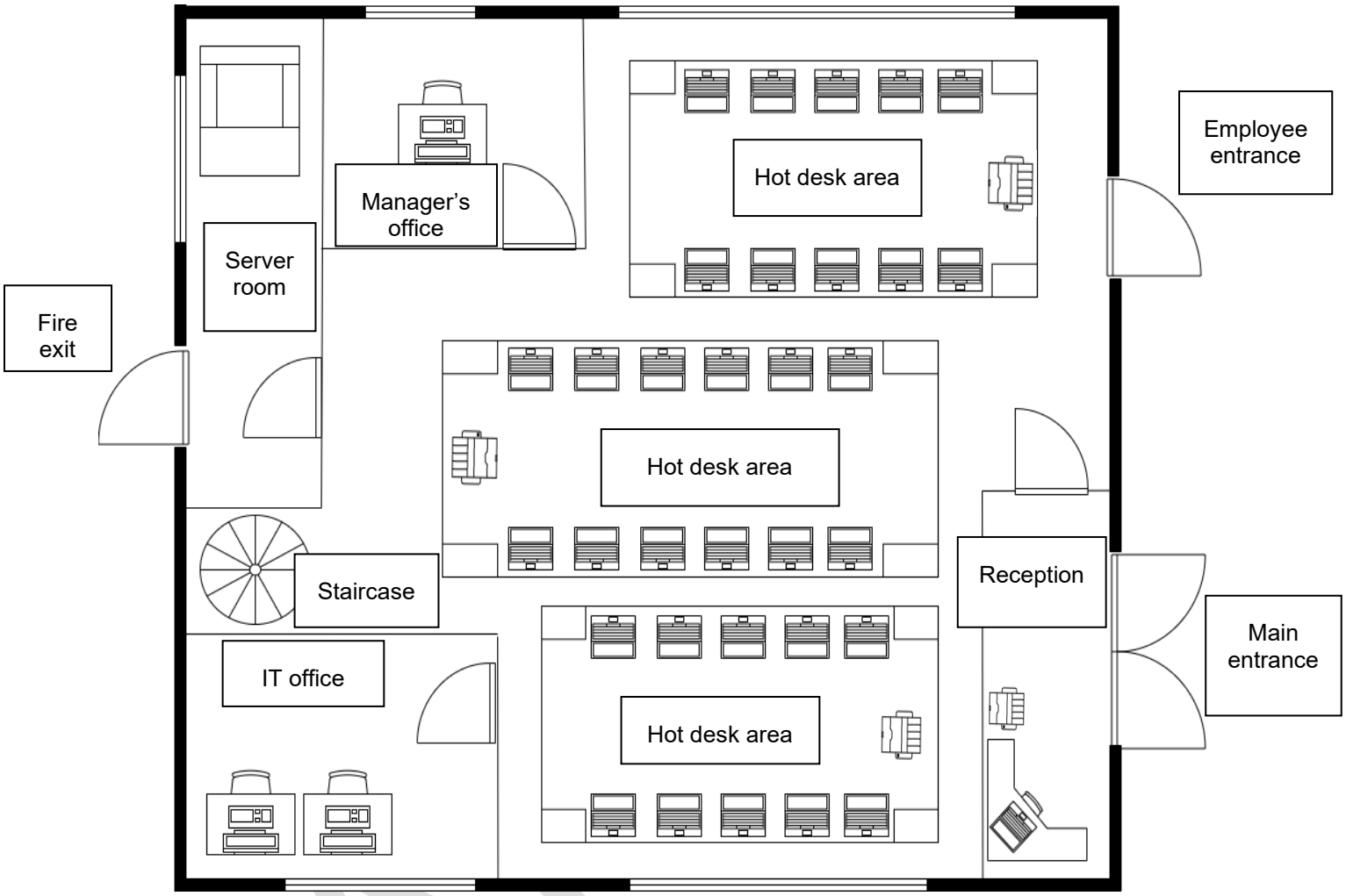
Staff training

All staff are told about the importance of keeping desks clear of private information and have awareness of email scams, but there is currently no formal mandatory training.

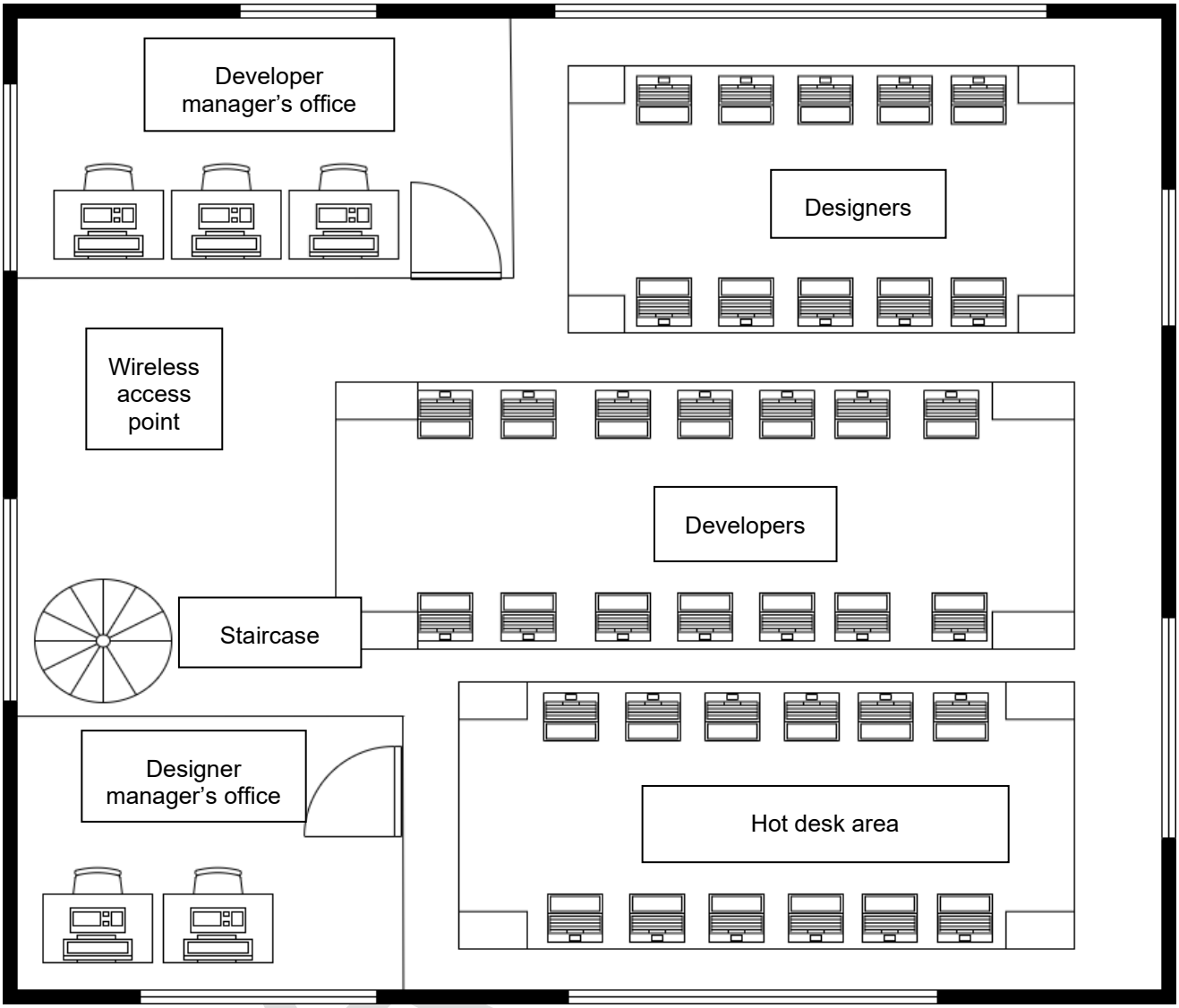
Problem identified

The IT manager has highlighted to management that there has been a rise in cyber attacks and is concerned that future attacks could adversely affect the business. They are considering how well the business would cope if this were to happen. They are concerned the business, as a new and expanding company, does not have all its policies or procedures in place yet to deal with this kind of emergency. The management team have highlighted that in the event of an incident the network and services would need to be operational within no more than 3 days.

Ground floor plan



First floor plan



Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication		01 June 2023
v1.1	Sample added as a watermark	November 2023	21 November 2023