T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 1

Assignment brief

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

Digital Support

Assignment brief

Assignment 1

Contents

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider during a set 2 week window.

The assignment will be completed under supervised conditions.

You must complete all tasks in this assignment independently. You are required to sign a declaration of authenticity to confirm that the work is your own. This is to ensure authenticity and to prevent potential malpractice and maladministration. If any evidence was found not to be your own work, it could impact your overall grade.

Internet access is only allowed for task 2. Internet access is available for this task to allow you to install, configure and update operating system and software applications. You are **not** permitted to use the internet for any other purpose, such as research. A copy of your browsing history must be submitted as part of your evidence for this task.

Your provider will provide the licensed software necessary for the tasks.

You have 19 hours to complete all tasks within this assignment. Each task has the following number of hours:

Task 1
8 hours (this task will be spread over 2 days – one day for task 1(a) and one day for task 1(b).

Task 2
11 hours (this will be provided after completion of task 1. This task will be spread over 3 days. There may be significant periods of time whilst waiting for installations to take place and therefore task 2(a), 2(b) and 2(c) may be completed in parallel).

Individual tasks must be completed within the timescales stated within each task, but it is up to you how long you spend on each part of the task, therefore be careful to manage your time appropriately.

Marks available across all assignment 1 tasks: 76.

Details on the marks available are provided in each task.

You should attempt to complete all of the tasks.

Read the instructions provided carefully.

Take all photographs using the digital camera supplied by your provider. Use of personal mobile phones is **not** permitted.

Performance outcomes (POs)

Marks will be awarded against the skills and knowledge performance outcomes (POs):

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

PO2: Install, configure and support software applications and operating systems

PO3: Discover, evaluate and apply reliable sources of knowledge

Scenario

You are a digital support specialist who has been contracted to work for a new small food manufacturing company (the client) based in the North of England.

The client requires your digital expertise in planning to support a future network. There are currently no business control techniques in place as the company is only just starting out, and they are unaware of any measures on how to operate their data systems effectively, appropriately and securely.

The client also requires your immediate support with preparing and installing a smaller network of computers and a mobile device for the employees within the company.

Task 1: prepare for installation

Time limit

8 hours

Task 1(a) must be completed prior to starting task 1(b).

Task 1(a) is allocated 3 hours 30 minutes.

Task 1(b) is allocated 4 hours 30 minutes.

You can use the time how you want but each task must be completed within the time limit.

(20 marks)

Student instructions

Based on the scenario, you are required to complete the relevant preparation that will enable you to set up 100 computers, a switch, server and 5 colour printers including identifying the relevant software for the client in the future. The network would be required to be set up within a 2 week window, to ensure all employees are up and running as quickly as possible.

You are required to:

1(a) Create a report to explain the security considerations required for the installation, configuration and support of end-user services to ensure confidentiality, integrity and availability including:

- suitable recommendations on implementing business control techniques within the workplace (physical/administrative)

- explanations on how the client should operate the new data systems effectively, appropriately and securely, considering GDPR/DPA 2018 and its principles

(8 marks)

1(b) Plan and complete the relevant network planning documentation:

- health and safety risk assessment for the work to be undertaken

- network planning, including:

  o   timescales

  o   network design, including IP addressing scheme

  o   inventory

- security risk assessment for the work to be undertaken, according to ISO 27001 principles

(12 marks)

You will have access to the following equipment:

- a computer with office software pre-installed

Evidence required for submission to NCFE

The following evidence should be submitted:

- summary of all business controls documentation required (word processing document)

- summary of how to secure data systems effectively (word processing document)

- health and safety risk assessment (worksheet in appendix 1)

- network planning documentation including timescales and network design (word processing document)

- inventory log (worksheet in appendix 1)

- security risk assessment (worksheet in appendix 1)

Task 2: install and configure a small network

Time limit

11 hours

You can use this time how you want but all parts of task 2 must be completed within the time limit.

(56 marks)

Student instructions

The client has asked you to install a new small network, against a set of requirements. These devices can be either virtual, physical or emulator.

All employees will use the computers centrally within head office, and any off-site employees will use a mobile device (laptop, tablet or phone) to be able to work remotely via the approved remote working solution.

The computers need to be set up allowing the employees to email, write letters to suppliers, update financial spreadsheets and create weekly presentations.

The computers will also need to access the internet and have instant messaging/video conferencing software such as Skype, GoToMeeting or Teams on Microsoft office 365 installed. Employees will require access to project management software in order to help them plan upcoming projects.

The client wants to ensure there is suitable software installed to mitigate any vulnerabilities to the system, including suitable back up security controls in place.

The client has also asked you to create installation notes for the software installations that took place, in order to support their staff responsible for IT. Your final task is therefore to create a useable document that briefs these individuals on the set-up of your system.

You will have access to the following equipment:

- 3 computers with full administrator rights, or virtual/emulator machine and software
- internet
- operating system
- word processing, presentation and spreadsheet software
- email software
- instant messaging software
- project management software
- mobile device or emulator
- IP address allocations for task 2 in line with provider's own network IP addressing schema
- digital camera

2(a) You must install, configure and support a small-scale network which includes 3 workstations and one mobile device via WiFi and evidence (you should reference the IP addressing schema allocated to you by your provider):

- implementing physical network and network security measures to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data (CIA and IAAA)
- install Windows Server and create Active Directory

- software licence management (software install log within appendix 1)

Note: you will need to provide annotated screenshots for the processes you follow and the implementations you make along with any key explanations for all decisions. As you carry out the various tasks, you will log all network security measures that have been implemented along with any software installations that are planned and how software licenses will be managed in the provided installation and configuration log (security risk assessment and software install log worksheets in appendix 1).

(18 marks)

Evidence required for submission to NCFE

The following evidence should be submitted:

- annotated screenshots (if using virtual machines) or photographs (if using physical machines/devices) showing the setup and successful implementation of the network and server/active directory install

2(b) Provide evidence of the following for the client:

- installing and setting up an operating system and antivirus software
- join computer to active directory domain
- installing and configuring application software suitable for the client
- implementing back up security controls
- install/update device drivers

Whilst waiting for the installation to take place, set up and configure a WiFi mobile device for network connectivity:

- configure a mobile device to include device lock security measures, mobile locator application and back up
- carry out all necessary mobile device updates including anti-virus

Note: You will need to provide annotated screenshots/photographs for the processes you follow and any implementations you make. This will include completing the software installation log (worksheet in appendix 1) and explaining your justifications for your decisions. You will also need to show evidence of any drivers which require installing, alongside taking screenshots of device manager. When updating any software/OS updates, you must evidence that there are no further updates required on the system. The installation may take some time to complete and therefore you should continue with task 2(c).

(22 marks)

Evidence required for submission to NCFE

The following evidence should be submitted:

- screenshots (if using virtual machines) or photographs (if using physical machines/devices) showing the setup and successful implementation of software, device driver status and mobile device

2(c) Review the installation and configuration notes and log (started in task 1) that report the following information to the client, making sure it is up to date and correct:

- record of all operating system/software application installations and utilities, upgrades, uninstalls and any major configuration changes

- identify and explain any vulnerabilities detected in the current system set-up/network

- recommend actions to mitigate any vulnerabilities found

Note: You will have been filling in the installation and configuration log as you have been completing the task. You will need to review what you have done, ensure that all information contained is correct and also identify the vulnerabilities and mitigations required.

Apply your communication skills appropriately, using standard English. Use accurate spelling, punctuation and grammar. Consider your target audience.

(16 marks)

Evidence required for submission to NCFE

The following evidence should be submitted:

- completed installation and configuration log (appendix 1)

Document information

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2020-2023.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

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.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication.		December 2020
v1.1	Branding and formatting final updates. NCFE rebrand.		September 2021
v1.2	Sample added as a watermark.	November 2023	20 November 2023