T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 1

Assignment Brief

Paper number: P002589
v1.0 Summer 2025
19 March 2025 to 20 March 2025
603/6901/2

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

Cyber Security

Assignment Brief

Assignment 1

Contents

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider over two days. The times and dates will be specified by NCFE.

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 allowed for tasks 1 and 2.

Ensure all print screens have been labelled with a brief description of what is being shown.

Submit the written work as a single .pdf file at the end of the assessment. Any video evidence submitted should be clearly labelled.

Electronic files should be named using the following format for identification purposes – Surname_Initial_student number_evidence reference for example: Smith_J_123456789_Task1_project proposal.pdf.

Timing

You have 11 hours to complete all tasks within this assignment.

Task 1 = 5 hours 30 minutes (this will be completed in one day)

Task 2 = 5 hours 30 minutes (this will be completed in one day)

Individual tasks must be completed within the timescales stated for 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: 50 marks.

Task 1 = 30 marks

Task 2 = 20 marks

Details on the marks available are provided in each task.

You should attempt to complete all of the tasks.

Read the instructions provided carefully.

Performance outcomes (POs)

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

Task 1

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data [10 marks]

PO3: Discover, evaluate and apply reliable sources of knowledge [20 marks]

[30 marks]

Task 2

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data [5 marks]

PO2: Propose remediation advice for a security risk assessment [10 marks]

PO3: Discover, evaluate and apply reliable sources of knowledge [5 marks]

[20 marks]

Scenario

Hawker Tech Solutions UK is a growing organisation which sells assistive technology solutions and consultancy services to small- and medium-sized enterprises (SMEs). Following a recent cyber security attack, it is looking to improve all aspects of its network security and to modernise its enterprise network. The source of the attack was an attacker using compromised credentials to access the company network via a virtual private network (VPN) connection.

Brief

Hawker Tech Solutions UK would like you to research and recommend some security products to be integrated into its network, and to recommend alternative secure solutions for external access to internal network resources. The proposal will be submitted to the board and will be addressed in the budget for next year.

Additionally, at the beginning of next month a new junior sales colleague will be joining the sales team. Initially the colleague will be office-based, but there is scope for them to work from home two days per week. You have been asked to set up a device so that they are able to work from both the office and remotely. In addition to configuring the device, you will also have to install any software agreed by your line manager, as well as set up an administrative account for yourself and a user account for the new colleague.

Task 1: project proposal

Time limit

5 hours 30 minutes.

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

[30 marks]

Instructions for students

You are required to complete a project proposal that researches three secure software products. For each of these you will compare two available security solutions and recommend which would be best for the company. Additionally, you will need to recommend the most appropriate method for user access solutions.
You will provide a rationale to justify any recommendations you make, stating why you feel the product / solution chosen is better than any other available, whilst considering price, reviewer feedback from other users, and certification.
You should create a project proposal that includes:

- your research into the following three secure software products:
  - anti-malware
  - back-up solution
  - full disk encryption
- for each one of these you should compare two similar products and recommend the best solution based on price, user reviews, technical specification and if applicable, certification
- references to sources used for validating the credibility of the software chosen
- any legal / security requirements that need to be addressed when considering the software chosen and how this software may be used
- recommendations for the most appropriate methods to implement user access control for the device in the scenario either locally, remotely, or both

Resources

For this task, you will have access to the following resources:

- internet access
- word processing software

Evidence required for submission to NCFE

The following evidence should be submitted:

- a project proposal, in PDF format

Task 2: set up devices, network and access

Time limit

5 hours 30 minutes.

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

[20 marks]

Instructions for students

Install the supplied operating system (OS) on the device that has been provided to you (laptop / computer / virtual machine (VM)) and configure a local administration account and a local user account.
Secure the device through the installation of the supplied software:

- anti-malware
- back-up solution
- full disk encryption
- demonstrate your ability to complete the installation by correctly configuring the supplied software
- run a scan to check everything works and if any software programs have not been successfully installed and configured, undertake remedial action to rectify the issue

Whilst doing this task, you must create a log that demonstrates:

- the steps followed for the installation of all software programs that have been installed
- evidence of the supplied software functioning correctly
- results of any scans you have run, and all remedial action undertaken if problems are identified

The log should include screenshots as appropriate.

Resources

For this task, you will have access to the following resources:

- internet access
- word processing software
- device with no operating system (OS) installed (this may be a laptop / computer / VM)
- an operating system (OS) to install (for example, Windows 10)
- software for installation:
- anti-malware solution (for example, Windows Defender, MalwareBytes, Comodo Internet Security Free)
- back-up solution (for example, File History, ToDo Backup Free, Veeam)
- full disk encryption software (for example, BitLocker, VeraCrypt, DiskCryptor)

Evidence required for submission to NCFE

The following evidence should be submitted:

- a word-processed log containing all evidence required including screenshots in PDF format

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

NCFE is authorised by the Institute for Apprenticeships and Technical Education to develop and deliver this Technical Qualification.

Owner: Head of Assessment Solutions.