Digital Technologies

Learner Name	
Course	Pearson BTEC Higher National Certificate in Computing
Awarding Body	BTEC (Pearson)
Module Name(s)	Unit 5 – Security (2019 rev)
Assignment Title & Number	Assignment 1 of 2
Assessor's Name	John Terry
Hand out Date	W/C 30th September 2019
Hand in Date	15th November 2019
Feedback Date	+3 weeks

Assessment Brief IQA by: *(Name & Signature)*		Assessment Brief sample by Lead IQA: *(Name & Signature)*	
Date:	?/?/2019	**Date**	

Specific outcomes and criteria being assessed		
Module	**Grading Criteria**	**Description**
5	P1 (LO1)	Identify types of security risks to organisations.
5	P2 (LO1)	Describe organisational security procedures.
5	M1 (LO1)	Propose a method to assess and treat IT security risks.
5	P3 (LO2)	Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.
5	P4 (LO2)	Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.
5	M2 (LO2)	Discuss three benefits to implement network monitoring systems with supporting reasons.
5	D1 (LO1&2)	Evaluate a minimum of three of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.

English, maths and other Skills for Success covered in this assignment	**English** Written reports and presentations.	**Maths** -	**Skills for Success** Describing and explaining concepts
Learner submission sampled by IQA: (Name and signature)		**Learner submission sampled by Lead IQA: (Name and signature)**	
Date		**Date**	

COPYING DISCLAIMER

I confirm that all the work contained in this assignment, being presented for assessment, is my own work.

I also confirm that I have not copied this work from other people's papers, electronically from their disk, from textbooks, CD ROM or from the Internet.

I also understand that if I hand in an assignment that has work in it that has been copied, this will be subject to disciplinary action and may cause me to lose my place on the course.

Student Signature:		Date:	

Assessor declaration	I certify that the evidence submitted for this assignment is the learner's own. The learner has clearly referenced any sources used in the work. I understand that false declaration is a form of malpractice.		
Assessor signature	John Terry	Date	
Date of feedback to learner			
Resubmission authorisation by Lead Internal Quality Assurer*		Date	

* All resubmissions must be authorised by the Lead Internal Verifier. Only one resubmission is possible per assignment, providing:
- The learner has met initial deadlines set in the assignment, or has met an agreed deadline extension.
- The tutor considers that the learner will be able to provide improved evidence without further guidance.
- Evidence submitted for assessment has been authenticated and accompanied by a signed and dated declaration of authenticity by the learner.

**Any resubmission evidence must be submitted within 10 working days of receipt of results of assessment.

Vocational Scenario

MK Agents is an estate agency with multiple branches in and around Milton Keynes. It uses networking at each site and between sites in order to carry out its business including authentication and file servers.

Task 1	Grading Criteria Covered:
	Unit 5: P1 (LO1) Identify types of security risks to organisations.
Evidence	Report

MK Agents is facing a range of IT security risks, both physical and logical. You have been asked to create an initial chapter for a company resilience report identifying the types of security risks that the company needs to consider.
You should start the report that gives the following:
- A bullet point list of the different security risks that the organisation could face
- A hierarchy chart categorising the different types of issue

Task 2	Grading Criteria Covered:
	Unit 5: P2 (LO1) Describe organisational security procedures.
	Unit 5: M1 (LO1) Propose a method to assess and treat IT security risks.
Evidence	Report

MK Agents have requested that you expand on the report you started by creating another chapter followed by an appendix.
The additional chapter should describe the security procedures that the company should undertake in order to maintain security within the organisation.
Additionally, the appendix you create should give your method of assessing and treating IT security risks.

Task 3	Grading Criteria Covered:
	Unit 5: M2 (LO2) Discuss three benefits to implement network monitoring systems with supporting reasons.
	Unit 5: D1 (LO1&2) Evaluate a minimum of three of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
Evidence	PowerPoint Presentation / Sway Presentation /

MK Agents have had their bi-yearly budget meeting, and have identified some additional funding that can be used on capital projects. You have been asked to present the following:
A discussion of 3 benefits of implementing network monitoring with supporting reasons (2 slides per benefit)
An evaluation of 3 physical and 3 virtual security measures that could be employed giving benefits and disadvantages, finally giving your choice as to which the budget could be best spent on.

Task 4	Grading Criteria Covered:
	Unit 5: P3 (LO2) Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.
Evidence	Intranet Wiki Article

The company has asked you to create a pair of articles for their intranet support Wiki identifying the possible impact to the security of the organisation if the firewall or VPN were to be incorrectly configured.

Give approximately an A4 page towards identifying and briefly describing the issues that can affect each of these devices (2 pages overall).

Task 5	Grading Criteria Covered: Unit 5: P4 (LO2) Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.
Evidence	Report with Packet Tracer screen shots

You have been asked to investigate the benefit that can be gained by implementing a range of security methods and show your results.

Use Packet Tracer to implement:
- A DMZ
- Static IP addresses
- A NAT router

And using these diagrams, explain how each can help improve network security.

Feedback

Module Number		Criteria included in this assessment	Met or Not Met	Comments
Task 1				
5	P1 (L01)	Identify types of security risks to organisations.		
Task 2				
5	P2 (LO1)	Describe organisational security procedures.		
5	M1 (LO1)	Propose a method to assess and treat IT security risks.		
Task 3				
5	M2 (LO2)	Discuss three benefits to implement network monitoring systems with supporting reasons.		
5	D1 (LO1 & LO2)	Evaluate a minimum of three of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.		
Task 4				
5	P3 (LO2)	Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.		
Task 5				
5	P4 (LO2)	Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.		
Assessor's Feedback				

What Went Well?

Even Better If…

SPaG & Maths Feedback

Assessor Signature:	Date:
Student Signature:	Date:

Student's Target (Student to complete from feedback)
Using the feedback provided, consider how you will improve the quality of your assessed work and identify targets to achieve this.

Signature:	Date: