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 2 of 2
Assessor's Name	John Terry
Hand out Date	W/C 11th November 2019
Hand in Date	17th January 2020
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	P5 (LO3)	Discuss risk assessment procedures.
5	P6 (LO3)	Explain data protection processes and regulations as applicable to an organisation.
5	M3 (LO3)	Summarise the ISO 31000 risk management methodology and its application in IT security
5	M4 (LO3)	Discuss possible impacts to organisational security resulting from an IT security audit.
5	D2 (LO3)	Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.
5	P7 (LO4)	Design and implement a security policy for an organisation.
5	P8 (LO4)	List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.
5	M5 (LO4)	Discuss the roles of stakeholders in the organisation to implement security audit recommendations.
5	D3 (LO4)	Evaluate the suitability of the tools used in an organisational policy.

Transforming Lives Through Learning

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: P5 (L03) Discuss risk assessment procedures. Unit 5: M3 (LO3) Summarise the ISO 31000 risk management methodology and its application in IT security.
Evidence	Report
MK Agents are looking to you to create a risk assessment for the company's IT Infrastructure. You must formulate a document for distribution to senior managers discussing risk assessment procedures that the company should follow. Add to your report a summary of the ISO 31000 risk management methodology within this context.	

Task 2	**Grading Criteria Covered:** Unit 5: P6 (LO3) Explain data protection processes and regulations as applicable to an organisation.
Evidence	Presentation
MK Agents must abide by the law in respect of the collection and storage of personal information. Create a presentation where each slide explains a different aspect of data protection law. The explanation of each principle of data protection must include a second slide for each stating what MK Agents needs to do to comply with each principle.	

Task 3	**Grading Criteria Covered:** Unit 5: M4 (LO3) Discuss possible impacts to organisational security resulting from an IT security audit. Unit 5: M5 (LO4) Discuss the roles of stakeholders in the organisation to implement security audit recommendations. Unit 5: D2 (LO3) Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.
Evidence	Briefing document (3-5 pages)
MK Agents have discussed the need to undertake a security audit. They have asked you to investigate the process and feed back to the next management meeting. You must prepare a briefing document that discusses first the possible impacts to the organisation's security as a result of an IT security audit. Then, discuss the roles of different stakeholders within the organisation in relation to the implementation of a security audit's recommendations. As part of this document, you have been asked to consider how the implementation of IT security can be matched up with the organisational policy, including what internal policies may be affected by this and the security impact of not updating the company policies.	

Task 4	**Grading Criteria Covered:** Unit 5: P7 (LO4) Design and implement a security policy for an organisation. Unit 5: D3 (LO4) Evaluate the suitability of the tools used in an organisational

	policy.
Evidence	Security Policy Document
Create a security policy document that can be implemented by MK Agents to help protect their (and their customers') data. Provide an evaluation of the tools to be used that have been mentioned in the above policy.	

Task 5	**Grading Criteria Covered:** Unit 5: P8 (LO4) List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.
Evidence	Disaster Recovery Plan Document Contents Page(s) & Justification
Create the contents page(s) for the company disaster recovery plan. On the next page, you should justify why you have included each of the sections / chapters.	

Feedback

Module Number	Criteria included in this assessment		Met or Not Met	Comments
Task 1				
5	P5 (LO3)	Discuss risk assessment procedures.		
5	M3 (LO3)	Summarise the ISO 31000 risk management methodology and its application in IT security.		
Task 2				
5	P6 (LO3)	Explain data protection processes and regulations as applicable to an organisation.		
Task 3				
5	M4 (LO3)	Discuss possible impacts to organisational security resulting from an IT security audit.		
5	M5 (LO4)	Discuss the roles of stakeholders in the organisation to implement security audit recommendations.		
5	D2 (LO3)	Unit 5: D2 (LO3) Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.		
Task 4				
5	P7 (LO4)	Design and implement a security policy for an organisation.		
5	D3 (LO4)	Evaluate the suitability of the tools used in an organisational policy.		
Task 5				
5	P8 (LO2)	List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.		
Assessor's Feedback				
What Went Well? **Even Better If…** **SPaG & Maths Feedback**				
Assessor Signature:			**Date:**	
Student Signature:			**Date:**	

Transforming Lives Through Learning

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:**

Transforming Lives Through Learning