Assignment front sheet – ATHE

Qualification		**Unit number and title**
ATHE L4/5 Extended Diploma in Computing (240 Credit)		Unit 5.1 Cyber Security
Learner name	**Student No**	**Assessor name**
		Mr. Shahid Mustafa

	Date issued	**Hand in deadline**	**Submitted on**
First Submission	12-10-2020	30-11-2020	
Re-Submission	14-12-2020	05-01-2021	
Note: students must get feedback within 15 days. Students have 10 working days to resubmit			

Assignment No. & title	1, Cyber Safenet Inc

In this assessment you will have opportunities to provide evidence against the following criteria.

LOs	**Criteria reference**	**To achieve the criteria the evidence must show that the learner is able to:**	**Task no.**	**Evidence/ Page No.**
LO1	1.1	Analyse current cyber security risks to organisations		
	1.2	Critically assess the vulnerability of computer network security in a chosen organisation		
	1.3	Evaluate the impact of cyber security on a chosen organisation		
LO2	2.1	Evaluate different controls to manage cyber security risks		
	2.2	Critically evaluate cyber security strategies within an organisation against industry standards		
LO3	3.1	Determine possible improvements to a client's secure network		
	3.2	Develop network security training plan for a client		

Learner declaration
I certify that the work submitted for this assignment is my own. I have clearly referenced any sources used in the work. I understand that false declaration is a form of malpractice. Learner signature: Date:

Assignment brief

Qualification	ATHE L4/5 Extended Diploma in Computing (240 Credit)		
Unit number and title	Unit 5.1 Cyber Security		
Assessor name	Mr. Shahid Mustafa		
	Date issued	**Hand in deadline**	**Submitted on**
First Submission	12-10-2020	30-11-2020	
Re-Submission	14-12-2020	05-01-2021	
Note: students must get feedback within 15 days. Students have 10 working days to resubmit			

Assignment No. & Title	1, Cyber Safenet Inc

Scenario

You have just gained employment in a Cyber Safenet Inc organisation which provides cyber consultancy to a range of business clients. Your specific role will be to test their systems for vulnerabilities and to recommend improvements to secure the client's network. Your manager has asked you to participate in the induction programme. At the end of the induction you will need to present the file to your line manager.

Some parts of the file require you to apply information to a particular organisation and you should discuss and agree the choice of the organisation with your tutor who will act as your line manager. The file should contain the data expected in the tasks provided below.

Task 1

a) An analysis of current cyber security risks to organisations
b) A critical assessment of the vulnerabilities of the computer network security of your chosen organisation
c) An evaluation of the different controls that can be used to manage cyber security risks

LO1, LO2 Assessment Criteria 1.1, 1.2, 2.1

Task 2

a) An evaluation of the impact of cyber security on your chosen organisation
b) A critical evaluation of the cyber security strategies that are used within your chosen organisation, mapping these to industry standards

LO1, LO2 Assessment criteria: 1.3, 2.2

Task 3

Based on your analysis and evaluation of the vulnerabilities within the chosen system

a) Produce a **presentation** which you would use with a client. The presentation materials must identify "possible improvements" to make the system secure.
b) Produce a training plan for improving network security including user awareness and prevention mechanisms.

LO3 Assessment criteria:3.1, 3.2

Guidelines for assessors
The assignments submitted by learners must achieve the learning outcomes and meet the standards specified by the assessment criteria for the unit. The suggested evidence below is how learners can demonstrate that they have met the required standard.

Task No	Assessment Criteria	Suggested Evidence
1	LO1, LO2 AC 1.1, 2.1	The work in this section of the file can be done from a theoretical standpoint. The learner will produce a comprehensive analysis of current cyber security risks to organisations. The learner will need to carry out research to identify what is "current" and examples should be used to illustrate the points made and to help demonstrate understanding. The learner will evaluate the different controls that organisations may use to control cyber security risks. The evaluation should be balanced identifying strengths as well as areas for development. This could include reviewing strategies, policies, identifying gaps or misaligned resources.
2	LO1, LO2, AC 1.2, 1.3, 2.2, 2.3	For work in this section of the file the learner will need access to an organisation and to their network which has vulnerabilities. This must be agreed with the tutor as the learner will need permission to test the system to reveal these vulnerabilities. The learner may need to be provided with help here to make this choice. The learner will test the system and analyse the benefits and drawbacks to identify security vulnerabilities. The learner needs to assess each of the vulnerabilities and report on their findings. The learner will evaluate the impact that cyber security has on their chosen organisation, outlining any current threats and attacks that have been evidenced recently. The learner will produce a critical evaluation of the cyber security strategies that the organisation uses and will research best practice and map these strategies, again identifying strengths and weaknesses for the organisation.
3	LO3 AC 3.1, 3.2	Following testing and analysis of the current system, the learner will make recommendations for improvements to the client's current system to secure their network. These should be directly related to the analyses which have been carried out for the organisation and recent good practice and industry standards. The presentation materials produced should be appropriate for the intended audience.

		The learner will then produce a training plan which outlines what the staff within the organisation need to know about network security to ensure the improvements are understood and retained. The training plan will cover user awareness, security training and prevention mechanisms as a minimum. The plan should be an outline of the training to be conducted but it will need to provide some detail so that the training plan can be carried out within the organisation.

Sources of information

- Clarke, R.A. and Knake, R.K. (2014) *Cyber war*. Tantor Media, Incorporated.
- Graham, J. (2010) *Cyber Security Essentials*. Auerbach Publications
- LeClaire, J. (2015) *Protect your organisation by building a security-minded culture*
- Singer, P.W. and Friedman, A. (2014) *Cybersecurity: What everyone needs to know*. OUP USA.
- Warren, P. Streeter, M & Whyatt, J. (2014) *Can we make a Digital World ethical?*

Websites:

- Cpni.gov.uk. (2019). *Cyber threats to national security | Public Website*. [online] Available at: http://www.cpni.gov.uk/advice/cyber/ [Accessed 26 Aug. 2019].
- Cyber Security Challenge UK. (2019). *Cyber Security Challenge UK*. [online] Available at: http://cybersecuritychallenge.org.uk [Accessed 26 Aug. 2019].
- Gov.uk. (2019). *Cyber security - GOV.UK*. [online] Available at: https://www.gov.uk/government/policies/cyber-security [Accessed 26 Aug. 2019].
- GOV.UK. (2019). *Cyber and Government Security Directorate*. [online] Available at: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance [Accessed 26 Aug. 2019].
- Ukcybersecurityforum.com. (2019). *UK Cyber Security Forum*. [online] Available at: http://ukcybersecurityforum.com/ [Accessed 26 Aug. 2019].

Guidelines for Submission of Assignments

- Submit softcopy of assignment report, in Turnitin Moodle link.
- Submit soft copy of assignment front sheet along with signed declaration and presentation slides in normal submission link as a zipped folder with your name as folder name.
- Please note assignment must be submitted on or before deadline date.

ASSESSMENT RECORD SHEET					
Programme	ATHE L4/5 Extended Diploma in Computing (240 Credit)	**Learner name**		**Learner No:**	
Unit no. & title	Unit 5.1 Cyber Security	**Assessor name**	Mr. Shahid Mustafa		
Assignment No. & title	1, Cyber Safenet Inc	**Target learning aims**	LO1, LO2, LO3		
1st Submission Issue Date	12-10-2020	**1st Submission Due date**	30-11-2020		
Resubmission Issue Date	14-12-2020	**Resubmission Due Date**	05-01-2021		
Resubmission authorisation (Name) by Lead Internal Verifier*		**Date Resubmission authorised by LIV****			

Task No	Target criteria	Criteria achieved? (Yes / No)	1st Submission tutor comment	Criteria achieved? (Yes / No)	Resubmission tutor comment
		1st Submission		**Resubmission**	
1.a	1.1				
1.b	1.2				
1.c	2.1				
2.a	1.3				

2.b	2.2				
3.a	3.1				
3.b	3.2				

General comments (tutor) – Please comment on the quality of student work, report structure and referencing.			
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		**Date**	
Learner comments			
Learner signature		**Date**	