ASSIGNEMNT BRIEF

HTU Course No: 30201140	HTU Course Name: Security
BTEC UNIT No: Unit 5 (K/615/1623)	BTEC UNIT Name: Security

Assignment Brief Number: 6

Version 1

Assignment Brief

Student Name/ID Number	
HTU Course Number and Title	**30201140: Security**
BTEC course number and title	**Unit 5 (K/615/1623) Security**
Academic Year	2021/2022 (Fall Semester)
Assignment Author	Eng. Moath Sulaiman
Course Tutor	Eng. Moath Sulaiman
Assignment Title	X-Power
Assignment Ref No	Assignment 6
Issue Date	**16-12-2021**
Formative Assessment dates	**30/12/2021 , 13/1/2022**
Submission Date	**26/1/2022**
IV Name & Date	**Dr. Eyad Taqieddin 13/12/2021**

Submission Format

The submission for this assignment is:

1. An individual written **detailed report** that provides thorough, evaluated or critically reviewed technical information on all of the points illustrated in the *Assignment Brief and Guidance* section. A security policy should be included in the document as Appendix.
2. A 15-minute **presentation** as per the instructions in the assignment brief.

General notes:

- Your report should:
    - be written in a concise, formal business style using single spacing and font size 12.
    - make use of headings, paragraphs, subsections, and illustrations as appropriate,
    - be supported with research and referenced using the Harvard referencing system.
    - PDF format and Not exceeding 30 pages.

Note: Soft copies submissions should be done through the university's eLearning system within the deadline specified above using the link: http://www.elearning.htu.edu.jo/

Unit Learning Outcomes

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

LO3 Review mechanisms to control organisational IT security.

LO4 Manage organisational security.

Assignment Brief and Guidance

You have recently joined X-Power company to work as a junior IT security Analyst. X-Power is a three-year-old start-up company that started to get some good profit due its pioneer ideas and solutions in managing and controlling renewable energy planets like wind farms and solar farms distributed in different locations in Jordan especially Ajloun, Maan and Madaba. Their solution is based on collecting information from those farms and send them to a centralized database for monitoring, analysis and decision making. This information is gathered manually and entered to the database server located in the company office.

X-Power recently move to a new location in Irbid and decided to enter the 4th industrial revolution by introducing IoT and digitally transforming most of its services to be electronic services. As part of the security team, you were asked to review the network layout designed by the network and systems administrators (figure -1), to give your feedback and to provide a security report to your manager. Based on the new design, information gathered from the farms (IoT components) will be sent via the Internet to the servers located in the company office.

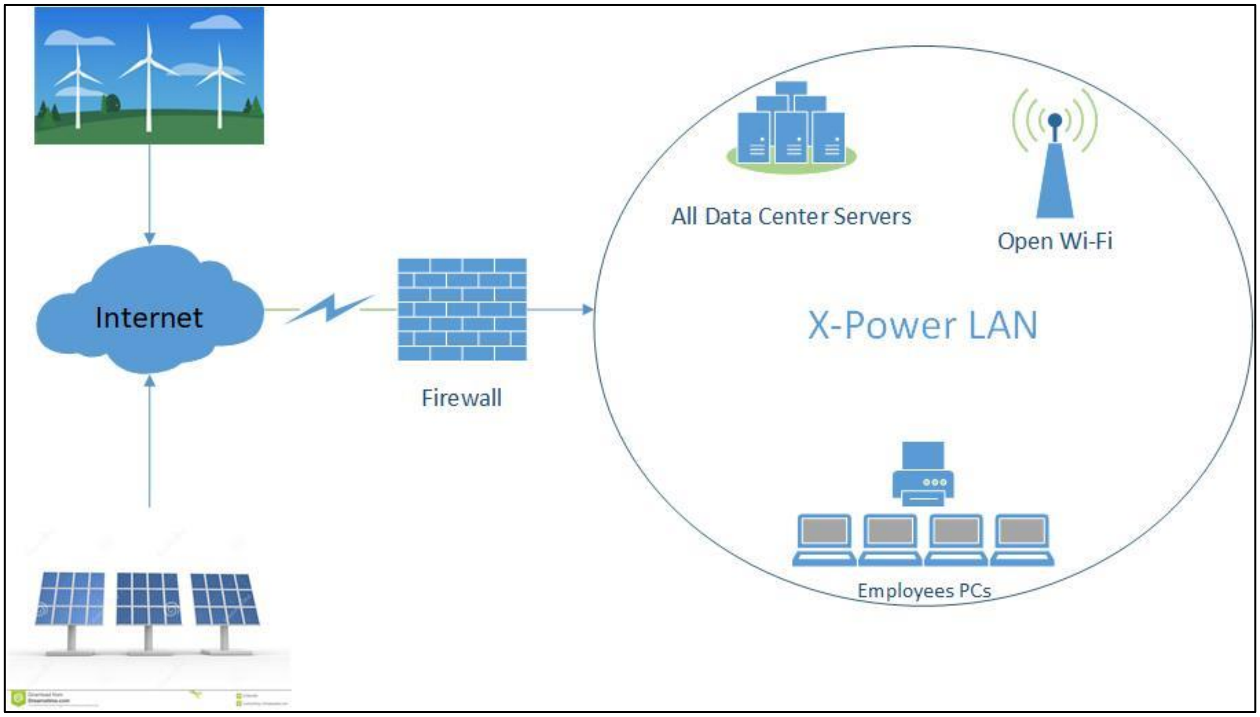

Figure-1 : X-Power Network diagram

Part of your responsibilities is to ensure the confidentiality, integrity, and availability (C.I.A) of the data and related services. You did a security check on most of the applications, systems, policies & procedures, and devices and noticed the following:

1- Not all existing devices (endpoints) are well secured.

2- The new systems are based on front-end back-end architecture.

3- All devices connected to the local network are configured to use the same subnet.

4- Information collected from the farms well be sent to the company office via the Internet and to be stored in a database server for analysis and reporting. The transmission of data is done through a web application published over the Internet.

5- When you checked the data centre, you noticed that the door is always open, so, servers and networking devices are easily accessed by anyone. The door is open due to the high temperature inside the room.

6- X-Power is open to provide some of those information to researchers as part of its CSR policy (Corporate Social Responsibility). Those researchers should subscribe to a dedicated website, hosted by X-Power, by creating an account and providing some of their personal information. Such information is protected by regulations.

7- On the other hand, because of COVID-19 containment strategy, “Work from home” approach was adopted at X-Power, and hence, some employees have VPN access to the CBA (Core Business Applications) and other supporting applications like ERP system to facilitate their work from home.

8- Some other third parties are granted VPN access like EDCO (Electricity Distribution Co) and JEPCO (Jordanian Electric Power Company).

9- Very minor security procedures taken by X-Power as well as some misconfigurations on some network security devices like firewalls and VPN.

Your manager asked you to prepare a **detailed report and a presentation** regarding IT security for X-Power services and environment. The report is to be submitted to the CEO to get approval for further security policy enforcement. <u>In your report you should:</u>

A. Discuss **IT security risks** that might put the applicants and X-Power data into danger, taking into consideration all data situations (being entered, transmitted, processed, and stored). Your discussion should include:

1. **Identifying** those IT security risks
2. Proposing a method to **assess** them.
3. Proposing a method to **treat** them.

B. Discuss **risk assessment** procedures

C. Explain how you can take benefit of the **ISO** risk management methodology by **summarizing** it and highlighting its application in IT security of this project.

D. Recommend ways to improve IT security via:

1. Describing **different security procedures** that X-Power could apply to protect business critical data and equipment.
2. Explaining **data protection** processes and **regulations** that might help X-Power to enhance IT security.
3. Discussing the **benefits of IT security audit** and its impact to X-Power IT security.

E. Discuss, in details, the **security impact of any misalignment** of IT security with X-Power policy.

F. **Design and implement a security policy** for X-Power.

G. Evaluate the **suitability of the tools** used in this policy

H. A discussion of the roles of stakeholders in the X-Power to implement security audit recommendations.

I. List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.

In your **presentation**, you should be able to cover the followings in front of the system/network admins:

1. Identify and discuss the **potential impact** of **incorrect** configuration of some network security devices on IT security.
2. Implementing different techniques in network security (such as DMZ, static IP and NAT). You should provide a detailed recommendation and explanation based on the scenario above for each technique showing how it will enhance security.
3. Discussing the benefits and justification of using a **Network Monitoring Systems**.
4. Evaluating a minimum of three of physical and three virtual security measures that can be employed to ensure the integrity of IT security.

Learning Outcomes and Assessment Criteria		
Pass	**Merit**	**Distinction**
LO1 Assess risks to IT security		**LO1 & 2** **D1** Evaluate a minimum of three of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
P1 Identify types of security risks to organisations. **P2** Describe organisational security procedures.	**M1** Propose a method to assess and treat IT security risks.	
LO2 Describe IT security solutions		
P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs. **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.	**M2** Discuss three benefits to implement network monitoring systems with supporting reasons.	
LO3 Review mechanisms to control organizational IT security		
P5 Discuss risk assessment procedures. **P6** Explain data protection processes and regulations as applicable to an organization.	**M3** Summarise the ISO 31000 risk management methodology and its application in IT security. **M4** Discuss possible impacts to organisational security resulting from an IT security audit.	**D2** Consider how IT security can be aligned with organizational policy, detailing the security impact of any misalignment.
LO4 Manage organizational security		
P7 Design and implement a security policy for an organisation. **P8** List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.	**M5** Discuss the roles of stakeholders in the organization to implement security audit recommendations.	**D3** Evaluate the suitability of the tools used in an organizational policy.

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

Student name: **Student ID:** **Is the student repeating this unit? YES NO**		**Assessor name:** Eng. Moath Sulaiman
Issue date: 16/12/2021	**Submission date:** 26/1/2022	**Submitted on:**
Programme: Computing		
HTU Course Name: Security **HTU Course Code:** 30201140	**BTEC Course name:** Security **BTEC Course Code:** Unit 5 (K/615/1623)	
Assignment number and title: Assignment 6: X-Power		

Plagiarism

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

Student declaration
I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student signature: **Date:**