# Luminus Technical University College - Assignment Brief (RQF)

## Higher National Diploma in computing

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Student Name** | | **Rashed Hasan** | | | **Language of assessment** | | | **AR** | **EN** |
| **College ID:** | | |  | |
| **Pearson ID:** | | |  | |
| **Unit Number and Title** | | **5.** | **Security** | | | | | | |
| **Academic Year** | |  | | | | | | | |
| **Unit Tutor** | |  | | | | | | | |
| **Internal Verifier Name and Approval (Signature)** | |  | | | |  | | | |
|  | | | |  | | | |
| **Assignment number and Title** | | **1** | **Managing Organizational Security** | | | | | | |
| **Issue Date (1St Submission)** | |  | | **Submission Date (1st Submission)** | | |  | | |
| **Issue Date (2nd Submission)** | |  | | **Completion Date (2nd Submission)** | | | |  | | --- | |  | | | |
| **Submission Format** | | | | | | | | | |
| The submission is in the form of:   * An individual written report. This should be written in a concise, formal business style using single spacing and font size 12.  You are required to make use of headings, paragraphs, and subsections as appropriate. * The research question must provide good details. | | | | | | | | | |
| **Unit Learning Outcomes** | | | | | | | | | |
| **LO1** | Assess risks to IT security. | | | | | | | | |
| **LO2** | Describe the IT security solution | | | | | | | | |
| **LO3** | Review mechanisms to control organizational IT security | | | | | | | | |
| **LO4** | Manage organizational security | | | | | | | | |
| Transferable skills and competencies developed | | | | | | | | | |
| * **TASK A: Risk Assessment and identification** * **TASK B: Studying issues to find solutions** * **TASK C: Security Controls and mechanisms** * **TASK D: Organizational Security Management** | | | | | | | | | |
| **Vocational scenario:** | | | | | | | | | |
| You work for a mid-sized software development company that creates and sells enterprise software. Your manager has tasked you with conducting a vulnerability assessment of the company's flagship product, which is used by many of its customers to store sensitive data.  Your job will be to identify any potential vulnerabilities in the software, assess the severity of the vulnerabilities, and provide recommendations to the development team on how to address them. To conduct the vulnerability assessment, you will need to use a variety of tools and techniques, such as network scanning, and penetration testing. You will need to work within established security protocols and best practices, to ensure that the assessment is conducted in a safe and controlled manner.  Once you have completed the assessment, you will need to prepare a report detailing your findings and recommendations. The report should be written in clear and concise language, so that it can be easily understood by the development team and other stakeholders.  Throughout the process, you will need to maintain a strong focus on customer data protection, ensuring that the software is as secure as possible, and that any potential vulnerabilities are identified and addressed promptly. Your work will be critical to ensuring that the company's customers can trust the software to keep their data safe and secure. | | | | | | | | | |
| Assignment activity and guidance | | | | | | | | | |
| * **TASK A: Risk Assessment and identification**   Your company has tasked you with your team to evaluating the level of dedication to information security processes. It is necessary to understand the potential risks to the company's IT security to maintain a secure system. As a result, the team is required to present their findings to senior management.  1. Name a risk table outlining the different kinds of security threats and vulnerability for each risk that can impact businesses.  2. Summarise The security controls that your organization needs to adhere to the risk that been provided in the previous task in order to safeguard its systems against potential risk in the future.  3. Then set a strategy for evaluating and addressing IT security threats.   * **Task B: Studying issues to find solutions**   As mentioned before the organization uses a firewall system, and an anti-virus system, in addition to relying on manual backup services for major databases. Describing the IT security solutions for security issues is one of your main duties related to your position, so you must provide the company with a study about all types of solutions that can be applied to the business to assure the highest security for their systems. In your study you must complete the following:   1. Show how IT security could be compromised by incorrectly set up firewall policies and third-party VPNs. 2. Exhibit an illustration of how a DMZ, static IP, and NAT can enhance network security by giving an instance for each. 3. Negotiate three advantages of integrating network monitoring systems and support your points with justifications. 4. Assess at least three physical and virtual security measures that aim to maintain the CIA triad standards of information systems, with a particular focus on "Integrity," and provide critical feedback. (Note: your answer must be detailed research) | | | | | | | | | |
| **Recommended Resources**  **Please note that the resources listed are examples for you to use as a starting point in your research – the list is not definitive.**  **Textbooks** | | | | | | | | | |

**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. | **M2** Discuss three benefits to implement network monitoring systems with supporting reasons. |
| **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network  Security. |  |