INTERNATIONAL SCHOOL OF MANAGEMENT AND TECHNOLOGY   
 NEPAL



**FACULTY OF COMPUTING**

|  |  |  |  |
| --- | --- | --- | --- |
| UNIT TITLE | Unit 5: Security | | |
| UNIT CODE | D/618/7406 | LEVEL | 4 (Core) |
| STUDENT NAME |  | CREDIT VALUE | 15 |
| ASSESSMENT TITLE | Managing Network Security for an Organisation | WORD COUNT |  |
| ASSESSOR | Jagdish Sharma | I.V. |  |
| ASSIGNMENT ISSUE DATE | 16/07/2023 | ASSIGNMENT SUBMISSION DATE | 15/09/2023 |
| ORIGINAL SUBMISSION |  | ASSIGNMENT NO. | 1 |

**ASSESSMENT CRITERIA TO BE ASSESSED IN THIS ASSIGNMENT**   
*(Identify all criteria to be assessed in this assignment)*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Assignment Criteria | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 | |  | |
| Achieved |  |  |  |  |  |  |  |  | |
|  | **Merit Criteria** | | | | | | **Distinction Criteria** | | | | |
| Assignment Criteria | M1 | M2 | M3 | M4 | M5 |  | D1 | D2 | D3 | |  |
| Achieved |  |  |  |  |  |  |  |  | |

**Important:**

* **Read the plagiarism notice and requirements at Page 12**
* **Word-limit- 8000 words** *(excludes cover page, table of content, figures, graphs, reference list, appendix and logbook)*
* **Accepted Sources: Research Papers** *(Journal Articles, Conference Proceedings, Thesis), Text Books, Governmental Data, Websites (only a registered organization, an educational institution, government agency)*
* **Information taken from unreliable sources will not be accepted**
* **Must follow Harvard Reference Style**
* **Assignment must be submitted through the Plagiarism Detection Tool**

|  |
| --- |
| **Assignment submission format** |
| The assignment submission is in the form of the following.  **A formal 10-minute presentation (10–20 slides as a guide, with supporting speaker notes)** to communicate an evaluation of your investigation to a non-technical audience, highlighting key information regarding the range of IT security risks that organisations face and the IT security solutions for them. The presentation will also include an assessment of the current organisational security procedures and an evaluation of both the physical and virtual security countermeasures presented.  **A process review** to assess the existing risk assessment procedures in an organisation and review and summarise standard risk management approaches that could be applied. The review will show how implementing IT security should work in conjunction with an organisation’s policy.  The recommended word limit is 1,000–1,500 words, although you will not be penalised for exceeding the total word limit.  **A written report** to review the security incident and recommend and justify a suitable security policy for audit trail can be identified. The report will evaluate the suitability of the security tools selected to meet the needs of the business.  The recommended word limit is 1,000–1,500 words, although you will not be penalised for exceeding the total word limit.  Note: You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. |

|  |
| --- |
| **Learning outcomes covered** |
| * LO1 Assess risks to IT security * LO2 Describe IT security solutions * LO3 Review mechanisms to control organisational IT security * LO4 Manage organisational security. |

**ASSIGNMENT SCENARIO**

|  |
| --- |
| **Scenario** |
| You have been employed as a Junior Network Security Specialist for Phaeton Security Solutions Limited (PSS). PSS provides network security solutions for a range of clients from multiple industry sectors. The services offered by PSS include:   * providing a security audit of an organisation’s network in the context of its business requirements * reviewing and recommending improvements to an organisation’s network security * implementing network security solutions.   PSS usually has large, multinational corporations as their clients, but the CEO has received an unusual request from a new client and has decided that this would be an ideal project for you to handle by yourself.  The client is the Dowding Federation, an Academy chain consisting of three sixth form colleges (SFC). The Dowding Federation has a chief executive officer and manages an educational budget of UKP £16.4 million.  One of the colleges that is part of this chain is ISMT College, a large SFC with 2000 students that specialises in computer science, maths and engineering.  ISMT College has 65 members of staff, both teaching and non-teaching, and has an operating budget of UKP £5.3 million.  All staff data, both personal and for payroll, are kept on dedicated Human Resource (HR) servers located within the Network Server Room.  All student data is kept on the college Student Information System (SIS), which contains data such as:   * contact details for students and parents * medical history and other sensitive information * assessment data from homework and examinations as well as historical GCSE data * attendance data – Present/Not Present/Authorised Absent for all lessons while at college * any Special Educational Needs (SEN) data.   All college files were located on a shared public access fileserver. This contained all educational resources created by teachers, as well as areas for students to upload and download coursework assignments and homework.  Students logging in to any computer on the college network had Read Access to the fileserver; teachers had Read/Write access.  The college maintained its own email exchange server, holding all staff and student emails as well as historical emails from all previous years.  The email server, fileserver, backup NAS drive and Network Domain Server were located in a non-secured room in the IT Technicians’ office. This room was never locked in case staff or students needed IT support.  The college had a Virtual Learning Platform (VLP), that provides a web interface to the fileserver and provides a way for students to access course materials.  The college computers ran older versions of Windows 8.1, as it was determined to be too expensive to migrate to the current version of the software.  To save money, a freeware VPN had been set up to allow teachers to access college materials from home using college laptops installed with a VPN client software. It was still possible for staff members to access the fileserver directly using Remote Desktop.  Since the college was deemed to be at a low risk of cyber-attacks, most of the security countermeasures were designed to minimise a threat from malicious damage from students:   * all IT labs were locked and cannot be opened without a swipe card * college policy was that no student can be in an IT lab unsupervised * virus scanners had been configured to automatically scan any USB drive plugged into a device * all optical drives had been removed from each college computer.   An Acceptable Use Policy was created for students (see Appendix 1). Staff were not considered to be a security threat, so no staff policies were created.  Similarly, the college had a simple firewall, however this was configured to just block attempts at network intrusion from known malicious blacksite IP addresses.  The Federation CEO deemed the college to be a low-priority threat, and data backups involved a single 8TB Network Attached Storage (NAS) Drive, where data was backed up each week.  Security procedures were not strictly followed as it was thought there was no requirement because the college was a ‘soft target’.  Just prior to the pandemic in March 2020, ISMT College suffered a massive security breach.  A ransomware virus was downloaded and deployed onto all the college servers resulting in a complete and total loss of:   * all personal student and staff data * all data on the backup NAS drive * all coursework and teaching resource data on the public fileserver and VLP * all current and historical attendance data * all financial data on the HR servers, meaning college staff and contractors could not be paid * all current and historical email data.   The college did not have the finances to pay the ransom and so a completely new IT system was purchased. All data was lost.  As part of a review after the incident, it was determined that a teacher working from home at the weekend, in trying to find extra teaching materials, inadvertently downloaded a virus containing a malicious payload to their staff laptop from a compromised website. The teacher was not using the VPN.  The ransomware was activated only when the laptop was connected to the college network on the following Monday. The ransomware virus then deployed and copied itself onto all network devices from the target location, encrypting all data on all servers, resulting in a total, catastrophic loss of all data.  In the aftermath of the incident, the client wants you to review the risk assessment procedures that were in place and provide a new risk assessment procedure that is ISO compliant.  They also want you to clearly demonstrate how any new security will still allow ISMT College to carry out its normal operations, with a greater emphasis on lessons being delivered remotely.  To make sure that something like this does not happen again, the client also wants you to design a suitable security policy, identifying key stakeholders, justifying your plan and the IT tools selected. The new plan needs to cover a wide range of potential IT threats.  You have been given the current IT Use Policy from ISMT College, as well as their current Risk Assessment plan. These documents are given to you in Appendices 1 and 2. Make sure you study them before attempting this assignment.  As part of your work for PSS, your CEO wants you to put together a presentation on IT security threats and countermeasures. You will present this to the CEO and four senior Security Specialists, so that you can demonstrate you have the breadth of knowledge required to begin to work with larger clients on your own. |

**ASSIGNMENT TASKS**

|  |
| --- |
| **Assignment Task** |
| **Activity 1**  **Produce a formal presentation (with supporting notes)** on a review of the range of IT security threats that are faced by an organisation like ISMT College, and describe and evaluate the range of countermeasures, both physical and virtual.  Your presentation should include a section on security risks, including:   * a discussion of the different types of security risks to an organisation like ISMT College * an assessment of the organisational security procedures presented in the given scenario (Appendix 1 – Current Security Policy for ISMT College) * an analysis, with reasons, of the benefits of implementing network monitoring systems.   In your presentation you should go on to discuss a range of security countermeasures for the identified risks, including the following.   * A discussion of the potential security impact of incorrect configuration of:   + firewall policies   + third party VPN clients and servers. * A discussion, using a specific example from either your research or the ISMT College scenario, of how implementing each of the following can improve network security:   + a De-Militarized Zone (DMZ)   + a Static IP   + Network Address Translation (NAT). * A proposal for a method to assess and treat IT security risks * An evaluation of the range of countermeasures that can be employed to make sure that an organisation’s integrity is not compromised. Organisational Integrity could be either Data Security or Operational Continuance. Make sure that you include both physical and virtual security countermeasures.   You should support any points you make in the presentation with well-chosen examples from any research you have carried out on related sectors or security scenarios.  **Activity 2**  **Produce a process review document** to assess the current mechanisms and legislation for data security in ISMT College. Your process review should include the following.   * A review of the current risk assessment procedures in ISMT College (Appendix 2 – Risk Assessment) * An explanation of data protection processes and regulations applied to ISMT College * A summary of an appropriate risk-management strategy or applied ISO standard and its application to IT security at ISMT College * An analysis of the possible impact on security at ISMT College following the results of an IT security audit * A recommendation, with supported reasons, on how the IT security at ISMT College can be aligned with its organisational policy.   You should detail explicitly the security impact if there is a misalignment. You should support any points you make in the presentation with well-chosen examples from any research you have carried out on related sectors or security scenarios.  **Activity 3**  Present a written report on the design of a suitable security policy, based on the supplied evidence and operational requirements, for ISMT College. Your report should include the following:   * A suitable security policy, including the main components of a disaster recovery plan for the college * Identification and discussion of the stakeholders and their roles in implementing a security audit * Justification, with reasons, for the designed security plan, including the selected physical, virtual and policy elements * An evaluation of the suitability of the tools used in the security policy designed for ISMT College on how it meets their needs.   You should support any points you make in the report and your presentation with well-chosen examples from any research you have carried out on related sectors or projects, as well as the existing scenario and any associated documentation. |

**Appendix 1 – Current Security Policy for ISMT College**

|  |
| --- |
| **ISMT COLLEGE STUDENTS ACCEPTABLE USE POLICY** |
| **Background and Definitions** |
| This document provides the basis for determining the acceptability of the use of ISMT College IT facilities. It defines unacceptable usage, to which users are expected to adhere at all times. Using the systems appropriately also helps the equipment to be used efficiently and to be available when needed. Use of the ISMT College computing resources and facilities is subject to UK law and any illegal use will be dealt with appropriately. |
| **Acceptable Use** |
| ISMT College provides each student with access to the college network, access to the internet, use of a desktop terminal and an email account. This use is permitted and encouraged by the college where such use is suitable for academic and teaching purposes and supports the college’s goals and objectives. The internet is to be used in a manner consistent with the college’s standards of conduct and as part of any study-related activities. Use of the network, internet/intranet and email, including data sent on it, may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources. |
| **Unacceptable Use** |
| The ISMT College network may not be used for any of the following:   1. The creation, viewing or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material 2. The creation, viewing or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety 3. The creation or transmission of defamatory communications (for example insulting, derogatory or slanderous email) 4. The creation, viewing or transmission of offensive materials (for example adult materials, images or pornography) 5. The transmission of material such that this infringes the copyright of another person 6. The transmission of unsolicited commercial materials or advertising 7. Deliberate unauthorised access to facilities or services accessible via the ISMT College network 8. To examine, change, or use another person's files, output, or username or password for which they do not have explicit authorisation 9. Deliberate activities with any of the following characteristics:  * Wasting staff effort or networked resources, including time on end systems accessible via the ISMT College network and the effort of staff involved in the support of those systems * Corrupting or destroying other users' data * Violating the privacy of other users * Disrupting the work of other users * Using the ISMT College network in a way that denies service to other users (for example deliberate or reckless overloading of access links or of switching equipment. This includes the unwarranted use of internet audio and video) * Use of a VPN or proxy service to disguise or forge identity or usage while using the college network to browse the internet * Using college network facilities for the playing, downloading, installing or distribution of games, web-games, or materials, software or media which is copyrighted by a third party * Attaching items of equipment or peripherals that do not belong to the college to any college computers, networks or systems without explicit authorisation from the IT Services team * The uploading of images from digital cameras as part of BTEC Photography coursework is deemed acceptable.   Where the ISMT College network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the ISMT College network. |
| **Compliance** |
| It is the responsibility of all users to take all reasonable steps to ensure compliance with the conditions set out in this policy document and to ensure that unacceptable use of the ISMT College network does not occur.  Where necessary, service may be withdrawn from a user. This may take one of two forms:   1. an immediate, temporary withdrawal of service should a violation of any of these conditions occur after appropriate warnings have been given 2. an immediate suspension of service should a serious violation of the policy occur or a violation that causes disruption to computer services.   All service withdrawals would be made on the judgement of the Chief Technology Officer, and the Principal, Head of School, Class Teachers, and Parents / Guardian would then be immediately informed.  The use of ISMT College facilities is subject to UK law and any illegal use will be dealt with appropriately. |

**Appendix 2 – Current Risk Assessment for ISMT College**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Priority 3:** Critical, must be deal with immediately.  **Priority 2:** Medium, deal with as and when funds become available.  **Priority 1:** Low, not considered a likely event   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Asset** | **Threat** | **Probability** | **Impact** | **Risk Assessment** | **Priority** | | Computer Lab PCs | Virus | Very Likely | Minor | Medium | 1 | | Computer Lab PCs | Deletion of Data | Likely | Minor | Low | 1 | | Computer Lab PCs | Breach of Copyright | Very Likely | Moderate | High | 2 | | Computer Lab PCs | Transmission of Unauthroised Materials | Likely | Moderate | Medium | 2 | | Staff Laptops | Virus | Unlikely | Moderate | Low | 1 | | Staff Laptops | Deletion of Data | Unlikely | Moderate | Low | 1 | | Staff Laptops | Breach of Copyright | Unlikely | Moderate | Low | 1 | | File Server | Virus | Unlikely | Major | Medium | 1 | | File Server | Deletion of Data | Unlikely | Major | Medium | 2 | | Network | DDOS attack | Very Likely | Major | Extreme | 3 | | Network | Virus | Unlikely | Major | Medium | 1 | |

**LEARNING OUTCOMES AND ASSESSMENT CRITERIA**

|  |  |  |  |
| --- | --- | --- | --- |
| Pass | Merit | | Distinction |
| LO1 Assess risks to IT security | | | **LO1 & LO2**  **D1** Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security. |
| P1 Discuss types of security risks to organisations.  P2 Assess organisational security procedures. | | **M1** Analyse the benefits of implementing network monitoring systems with supporting reasons. |
| LO2 Describe IT security solutions | | |
| P3 Discuss the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.  P4 Discuss using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. | | **M2** Propose a method to assess and treat IT security risks. |
| LO3 Review mechanisms to control organisational IT security | | | **D2** Recommend how IT security can be aligned with an organisational policy, detailing the security impact of any misalignment. |
| P5 Review risk assessment procedures in an organisation.  P6 Explain data protection processes and regulations as applicable to an organisation. | | **M3** Summarise an appropriate risk management approach or ISO standard and its application in IT security.  **M4** Analyse possible impacts to organisational security resulting from an IT security audit. |
| LO4 Manage organisational security | | | **D3** Evaluate the suitability of the tools used in the organisational policy to meet business needs. |
| P7 Design a suitable security policy for an organisation, including the main components of an organisational disaster recovery plan.  P8 Discuss the roles of stakeholders in the organisation in implementing security audits. | | **M5** Justify the security plan developed giving reasons for the elements selected. |

**Plagiarism Notice**

You are reminded that there exist **Academic Misconduct Policy and Regulation** concerning **Cheating and Plagiarism**.

**Extracts from the Policy:**

**Section 3.4.1:** Allowing others to do assignments / Copying others assignment is an offence

**Section 3.4.2:** Plagiarism, using the views, opinion or insights / paraphrasing of another person’s original phraseology without acknowledgement

**Requirements**

* It should be the student’s own work – **Plagiarism is unacceptable**.
* Clarity of expression and structure are important features.
* Your work should be submitted as a **well presented**, word-processed document with headers and footers, and headings and subheadings.
* You are expected to undertake research on this subject using books from the Library, and resources available on the Internet.
* Any sources of information should be **listed as references** at the end of your document and these sources should be referenced within the text of your document using **Harvard Referencing** style
* Your report should be illustrated with screen-prints, images, tables, charts and/or graphics.
* All assignments must be typed in **Times New Roman**, **font size** 12, 1.5 **spacing**.

**The center policy is that you must submit your work within due date to achieve “Merit” and “Distinction”. Late submission automatically eliminates your chance of achieving “Merit and Distinction”. Also, 80% attendance is required to validate this assignment.**

|  |  |  |
| --- | --- | --- |
| **Assignment Prepared By**  Umesh Kisor Baral | **Signature**  **UMESH** | **Date** |
| **Brief Checked By**  Dhruba Babu Joshi | **Signature** | **Date**  20/04/2023 |