|  |  |
| --- | --- |
| University of Derby  **The School of Computing and Mathematics** | |
| **In-course Assignment Specification** | |
| **Module Code and Title: 6CC541** **Security Management** | |
| **Assignment Title: Security Management of HandM Network (You can choose other Title based on the keywords used in your design)** | |
| **Assessment Tutor:** | **Weighting Towards Module Grade:** 100% which is further divided as follows:  **Final Report: 100%** |
| **Date Set**: **01-10-2019** |  |
| |  | | --- | |  | | **Late Submission**  There are 3 distinct processes in place to deal with differing student circumstances:   1. Assessed Extended Deadline (AED): Students with disabilities or long-term health issues are entitled to a Support Plan. 2. Exceptional Extenuating Circumstances (EEC): The EEC policy applies to situations where serious, unforeseen circumstances prevent the student from completing the assignment on time or to the normal standard. Students who submit a successful EEC claim will usually be required to complete a different assessment to that which was originally set. [**http://www.derby.ac.uk/eec**](http://www.derby.ac.uk/eec) 3. Late Submission: Requests for late submission will be made to the relevant Head of Discipline (or Head of Joint Honours for joint honours students) who can authorise an extension of up to a maximum of one week. [**http://www.derby.ac.uk/campus/support**](http://www.derby.ac.uk/campus/support) | |  | | |  |  |  | | --- | --- | --- | |  | | | |  | **Level of Collaboration**:  NONE |  | |  | | | | **Anonymous Marking**  All submitted assignments for this module will appear in an anonymous format to the Marking Tutor and internal moderators. As such you are requested not to identify yourself anywhere within your submitted assignment (e.g. by putting your name on the front cover sheet). This will maintain your anonymity to your Marking Tutor and Internal Moderators. The principle behind the usage of anonymous marking of assignments is to reassure students that all assignments are marked in an equitable and unbiased manner, thereby ensuring the maintenance of high academic quality standards within the marking of the assessments. Please use your Student Number. | | | | |  | |  | | |
|  | |
|  | |
| **Learning Outcome**  This project provides an opportunity to apply the competencies gained in the lessons of this course to develop a Security Management plan for a fictitious organization to replace its outdated plan. The following are learning outcomes of this assessment:   1. Analyse and discuss core business security policy issues that ensure the delivery of good and workable security policies. 2. Critically evaluate the requirements for the design of a security policy for a given scenario and evaluate it under various constraints 3. Demonstrate the application of security management principles in the safety and the prevention processes   **Learning Objectives and Outcomes**  You will gain an overall understanding of Security management, its importance, and critical processes required when developing a formal Security management plan for an organization.  The following tools and resources that will be needed to complete this project:   * Course Lectures * Internet access for research * Word Processor   **Deliverables**  As discussed in this course, Security management is an important process for all organizations. This is particularly true in information systems, which provides critical support for organizational missions. The heart of Security management is to plan the system that protects network assets from external and internal threats, develop a business continuity and disaster management system, develop the training for the employee, etc. The project activities described in this document allow you to fulfill the role of an employee participating in the Security management process in a specific business situation.  The project tasks are structured as follows:   |  |  | | --- | --- | | **Tasks** | **Deliverable** | | Project Part 1 | **Task 1**: Identification of Core Assets of the Organization | |  | **Task 2:** Developing the System to protect the Assets of the Organization (Information as well as data) | |  | **Task 3:** Development of Policies for Password Change, Password Length, Data Use, and Usage of VPN in the Context of COVID-19 Outbreak | | Project Part 2 | **Task 1:** Business Impact Analysis (BIA) Plan | |  | **Task 2:** Business Continuity Plan (BCP) | |  | **Task 3:** Disaster Recovery Plan (DRP) | |  | **Task 4:** Computer Incident Response Team (CIRT) Plan | | Project Part-3 | **Task1:** Design Training and Awareness campaign for phishing emails and strong passwords  **Task 2:** Organizing all tasks and Final Submission |   **Submission Requirements**  The Project parts are submitted at once on the specific deadline mentioned above. However, there are two checkpoints to evaluate and provide you feedback. The checkpoint reports and final project submissions should follow this format:   * Format: Microsoft Word or compatible * Font: Arial, 12-point, double-spaced * Citation Style: the one you like but be consistence * Should have appropriate tables and good resolution figures where necessary   **Scenario**  You are a newly hired security engineer in the HandM Network, Inc., a fictitious health services organization headquartered in London UK. HandM has over 600 employees throughout the organization and generates £500 million in annual revenue. The company has two additional locations in Derby and the Edinburg, which support a mix of corporate operations. Each corporate facility is located near a co-location data center, where production systems are located and managed by third-party data center hosting vendors.  ***Company Products***  HandM Network has three main products: HNetExchange, HNetPay, and HNetConnect.  **HNetExchange** is the primary source of revenue for the company. The service handles secure electronic medical messages that originate from its customers, such as large hospitals, which are then routed to receiving customers such as clinics.  **HNetPay** is a Web portal used by many of the company’s HNetExchange customers to support the management of secure payments and billing. The HNetPay Web portal, hosted at HandM production sites, accepts various forms of payments and interacts with credit-card processing organizations much like a Web commerce shopping cart.  **HNetConnect** is an online directory that lists doctors, clinics, and other medical facilities to allow HandM customers to find the right type of care at the right locations. It contains doctors’ personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer. Doctors are given credentials and are able to update the information in their profile. HandM customers, which are the hospitals and clinics, connect to all three of the company’s products using HTTPS connections. Doctors and potential patients can make payments and update their profiles using Internet-accessible HTTPS Web sites.  ***Information Technology Infrastructure Overview***  HandM operates in three production data centers that provide high availability across the company’s products. The data centers host about 1,000 production servers, and HandM maintains 650 corporate laptops and company-issued mobile devices for its employees.  *Threats Identified*  Upon review of the current security management plan, the following threats were identified:   * Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on * Loss of Customers and regulator’s fine due to lost data * Internet threats due to company products being accessible on the Internet * Insider threats * Changes in the regulatory landscape that may impact operations   ***Management Request***  Senior management at HandM has determined that the existing protection and security management plan for the organization is out of date and a new management plan must be developed. Because of the importance of security management to the organization, senior management is committed to and supportive of the project to develop a new plan. You have been assigned to develop this new plan.  Additional threats other than those described previously may be discovered when re-evaluating the current threat landscape during the design phase.  The budget for this project has not been defined due to senior management’s desire to react to all material that is identified within the new plan. Given the company’s annual revenue, reasonable expectations can be determined.  **Project Part 1**  **Project Part 1 Task 1: Assets Identification Project Plan**  For the first part of the assigned project, you must create a list of core assets (Network and Data) for which you like to develop the protection mechanism. To do so, you must:   1. Develop and provide an introduction to the plan by explaining its purpose and importance. 2. Define the scope and boundaries of the plan in terms of communities of Interest.   **Project Part 1 Task 2: Protection Mechanism and Policies**  After creating an initial draft of the security management plan, the second part of the assigned project requires you to create a protection mechanism for protecting the core assets of the organization. It also includes designing policies for various network scenarios mentioned above. Develop an introduction to the plan explaining its purpose and importance.   * Concern has been raised about the authentication of customers and employees of the HandM. Describe 2 methods HandM could use for improved authentication. Justify the use of each method. * Describe 2 methods HandM could use for file protection (sensitive data of Patients). Justify the use of each method. Compare the strengths and weaknesses of each method in contrast to the other method. * Create an outline for the Protection Mechanism plan with some block diagram connecting all offices and placement of different protection devices e.g Intrusion Detection Systems, Firewall, etc. * Identify the key policies for password change, password length, data use, and usage of a VPN. Circle your discussion around system-specific and user-specific policies. Have a look at the following link for some example policies:   <https://policy.kennesaw.edu/>  **Project Part 2**  **Project Part 2 Task 1: Business Impact Analysis (BIA) Plan**  This part of the project is a continuation of Project Part 1 in which you prepared a security plan and an attack detection plan for HandM. Senior management at the company has decided to allocate funds for a business impact analysis (BIA). Because of the importance, senior management is committed to and supportive of performing a BIA. You have been assigned to develop the BIA plan.  **Project Part 2 Task 2: Business Continuity Plan (BCP)**  After having reviewed and being impressed by your business impact analysis (BIA), senior management at HandM has decided that your team must also develop a BCP. Management has allocated all funds for a BCP and your team has their full support, as well as permission to contact any of them directly for participation or inclusion in your BCP plan. You have been assigned to develop this new plan.    Winter storms on the North of England have affected the ability of HandM employees to reach the Scotland offices in a safe and timely manner. However, no BCP plan currently exists to address corporate operations. The Scotland office is the primary location for business units, such as Finance, Legal, and Customer Support. Some of the corporate systems, such as the payroll and accounting applications, are located only in the corporate offices. Each corporate location is able to access the other two, and remote virtual private network (VPN) exist between each Production data center and the corporate locations.  The corporate systems are not currently being backed up and should be addressed in the new plan. The BCP should also include some details regarding how the BCP will be tested.  You may refer to the following additional resources to help you and your team develop a BCP, and you may use a BCP template if found during your research.  **References:**   * Guide to Business Continuity Management: Frequently Asked Questions (Protiviti, 2013), http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-BCM-Third-Edition-Protiviti.pdf * Business Continuity Plan (Ready.gov), http://www.ready.gov/business/implementation/continuity   **Project** **Part 2 Task 3: Disaster Recovery Plan (DRP)**  Your project on Security management, the BIA, and the BCP have been well received by senior management at HandM. They now want you to develop a DRP in order to overcome any mishaps that might occur in the future. You may research and use the National Institute of Standards and Technology (NIST) templates to develop a DRP plan for the company.  **Project Part 2 Task 4: Computer Incident Response Team (CIRT) Plan**  By now you should have developed a Protection Mechanism, Defined Policies for the network usage, and a BIA, BCP, and DRP.  In this part of the project, you will create a CIRT plan for HandM Network. The company headquarters (HQ) handles all incidents because the information security organization is located in London, so the plan will have its roots at HQ.  **Evaluation Criteria (For reference only, check Rubrics for the marking)**   * Did the student develop a sound CIRT plan?   **Security Management Training and Awareness and Final Submission**  After creating the CIRT plan, develop a simple training and awareness campaign for your employees for the Phishing Emails and Strong password. Compile all project parts and submit Via Turnitin submission point Final Project. Make sure to incorporate your instructor’s feedback on the checkpoints in the final Security management plan.  **Evaluation Criteria (For reference only, check Rubrics for the marking)**   * Did the student consider the inputs provided in their earlier checkpoints? * Did the student develop sound plans based on the requirements described during the project phases? * Did the student provide clear and easy-to-understand documentation, which may include tables and other presentation elements? * Did the student create a professional, well-developed report with proper grammar, spelling, and punctuation?   **Word Count:** **4000 Words (+, - 250) excluding references. Follow the Springer template.** | |
|  | |
| **The requirement for Assessment:**  You must be able to demonstrate the ability to:   * The effort made while understanding the security management core methods and techniques. * Referencing while providing your claims and methods * The explanation of your chosen method and presentation.   Your report (**4000 words**) should be structured as follows:   1. **Abstract** 2. **Introduction (**With following points) 3. Background about the problem you are addressing some statistics about security breaching 4. What is security management, who are the stakeholders and why it is important to have the management system for information security (It should be aligned with the organization information) 5. What this report is all about (summary of all tasks) 6. How the report is organized 7. **Tasks (1-3 with subtask, in order)**, Discussion on a specific task. It’s up to you how you are organizing these tasks. I recommend organizing your work into sections & subsections and make the appropriate connection between the content. Provide reference where appropriate. 8. **Conclusions (**Your core findings, how to improve further if you saw some issue with the existing system while performing your tasks**)** 9. **References** | |

|  |
| --- |
| **Submission:**  You must submit one electronic paper along onto Blackboard through **Turnitin** by the above deadlines.  **Project Checkpoints**  There are **two checkpoints**. Written and Verbal feedback will be provided for each checkpoint report. The report is discussed in a face to face or team meeting. Ideally, I would like to see some progress on the Tasks. Write a concise status report (no more than two pages) answering the following questions:   1. What have you accomplished so far? Which do you have left to do? 2. Are you on track to complete what you are doing? 3. What you have done so far in terms of Tasks, which tasks you have already addressed. 4. Have you encountered any surprises or unexpected problems while addressing tasks? |

**Deliverable Paper (100%) (In order)**

|  |  |
| --- | --- |
| Abstract | 05% |
| Introduction | 05% |
| Main Tasks (in order) | 60% |
| Grammars and spellings | 05% |
| Presentation/Organization | 05% |
| Conclusions | 05% |
| References list and citation. | 05% |
| Assessment Management (Checkpoints) | 10% |

**Assessment Criteria – Report**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Section/Criteria** | 70% | 55-70% | 40-55% | <40 | 0 | Pts. |
| **Abstract** | Clearly States the question being asked. Gives the hypothesis being tested. Highlights the most important findings with enough information to understand the tasks and information presented. State major findings and conclusions. Is a concise summary of the question and findings. | States clearly the question being asked. Gives the hypothesis being tested. Does not Highlights the most important findings with enough information to understand the tasks and information presented. Does not state major findings and conclusions. | Does not state clearly the problem being investigated. Does not give an overview that leads directly to the reader being able to state the major findings of the study | The important component of the abstract is missing. Is not written in a scientific style Includes references in the abstract. No conclusion or results of the information provided | No Content | 05% |
| **Introduction** | Strong introduction of the topic’s key question(s), terms. Clearly delineates subtopics to be reviewed. Specific task/project statements. The author has retained nearly all of the knowledge presented in class. He/She is able to synthesize this knowledge in new ways and relate to material not covered in the course. | The author competently addresses the main question or issue but does not add much new insight into the subject. That said, it is clear that the author has learned a great deal in class and is able to communicate this knowledge to others. | The author attempts to address the main question or issue but fails. The author has retained some information from the course, but does not fully understand its meaning or context and cannot clearly convey it to others. | Does not adequately convey the topic. Does not describe subtopics to be reviewed. The essay does NOT address the main question or issue, and it is obvious that the author has not retained any information from the course. | No Content | 05% |
| **Tasks**  **(1-3)** | All material is clearly related to the subtopic, main topic. Strong organization and integration of material within subtopics. Strong transitions linking subtopics, and the main topic. The essay contains a clear argument—i.e., lets the reader know exactly what the author is trying to communicate. Presents easy-to-follow steps which are logical and adequately detailed without including standard procedures that all scientist know how to do. Work considerably consider the recommendations provided in NIST, ISO 27000. | All material is clearly related to subtopics, main topic, and logically organized within subtopics. Clear, varied transitions linking subtopics, and main topic. Most steps are understandable but some lack detail or are confusing. The student tried to follow the recommendation presented in NIST ISO 27000 but only to some extent. | Most material is clearly related to the subtopic, main topic. Material may not be organized within subtopics. Attempts to provide a variety of transitions. Recommendation from ISO 27000 standard has not been followed but provided some discussion for the design choice. | Little evidence material is logically organized into topic, subtopics, or related to the topic. Many transitions are unclear or nonexistent. No attempt is made to articulate an argument. Is lacking several critical details so that it is impossible to understand what has been done to carry out the tasks. Many steps are missing in describing steps in designing and presenting the solution. | No Content | 60% |
| **Conclusion** | A strong review of key conclusions. Strong integration with the project statement. An insightful discussion of the impact of the researched material on the topic. | A strong review of key conclusions. Strong integration with the project statement. Discusses the impact of researched material on the topic. | Review of key conclusions. Some integration with the project statement. Discusses the impact of researched material on the topic. | Does not summarize evidence with respect to the project statement. Does not discuss the impact of researched material on the topic. | No Content | 05% |
| **Organization** | The essay contains an intro, main body, and conclusion. The introduction lays out the main argument and gives an outline of what the reader can expect in the essay. The conclusion brings everything together, acknowledges potential shortcomings of the paper, and gives the reader a sense of what further work might be done to advance the subject matter described in the paper. Content presented with proper, tables, and figures. | The essay contains an intro, main body, and conclusion. The introduction lays out the main argument but gives the reader little idea of what to expect in the essay. The conclusion nicely summarizes the main argument and evidence but does not move beyond what has already been presented in the paper. A few figures and tables are provided. | The essay contains an intro, main body, and conclusion. The introduction gives the reader an idea of what to expect in the paper but does not effectively lay out the main argument. It may begin with a set of rhetorical questions, or an anecdote that is never fully explained. The conclusion does little more than restate the problematic introduction. Intro and/or conclusion may be too wordy or short. Figures and tables have been provided without referencing and numbering | The essay has no clear organizational pattern.No figures and tables have been provided. The sections are poorly organized and are not well connected. | No Content | 05% |
| **Grammar/Spellings** | Grammar, punctuation, spelling is virtually flawless. Language and word choice are appropriate throughout. | Limited flaws in grammar, punctuation, and/or spelling do not detract from the the overall message of the paper. Some minor problems with language and word choice are noted but not overly problematic. | Significant flaws in some grammar, punctuation, spelling, language, and/or word choice. | Many sources are absent. Inappropriate format. References not most relevant/appropriate to study | No Content | 05% |
| **Citations & References** | All cited sources present, No references not cited in the body present. In an appropriate format.References all highly relevant | All cited sources present. In an appropriate format.References relevant and appropriate | Most cited sources present. Generally in the appropriate format. References relevant and appropriate. | Reference and citation errors detract significantly from paper | No Content | 05% |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Checkpoints** | Perform all the checkpoints task effectively, actively engaged in discussion in the face to face meeting, actively performed project tasks, fully incorporated the feedback suggestions in the final report. | Performs all assigned tasks, attends the face to face meeting, identified some interesting points during performing the project tasks, incorporated the meeting feedback in the final project report. | Performed assigned tasks with some progressing on achieving the final goals. Attends the face to face meeting. Does not pay much attention to assessment tasks as the ongoing activity. Included feedback in the final report to some extent. | perform assigned checkpoint tasks to some extent, submitted the report, however, misses the face to face meetings, does not incorporate the feedback in the final submission. | No checkpoint report has been submitted or report has been submitted but without any content | 10% |