**ASSIGNMENT FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 5: Security** | | |
| **Submission date** |  | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** |  | **Student ID** |  |
| **Class** |  | **Assessor name** |  |
| **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’s signature** |  |

**Grading grid**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P5 | P6 | P7 | P8 | M3 | M4 | M5 | D2 | D3 |
|  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Signature & Date:** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 5: Security | | |
| **Assignment title** | Security Presentation | | |
| **Academic Year** | 2018 – 2019 | | |
| **Unit Tutor** |  | | |
| **Issue date** | 31 Dec 2019 | **Submission date** | **1st: 14 Jan 2020**  **2nd: 17 Jan 2020** |
| **IV name and date** |  | | |

|  |
| --- |
| **Submission Format** |
| Part 1 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, subsections and illustrations as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system. The recommended word limit is 2,000–2,500 words, although you will not be penalised for exceeding the total word limit. Part 2 The submission is in the form of a policy document (please see details in Part 1 above). Part 3 The submission is in the form of an individual written reflection. 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, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system. The recommended word limit is 250–500 words, although you will not be penalised for exceeding the total word limit. |

|  |
| --- |
| **Unit Learning Outcomes** |
| **LO3** Review mechanisms to control organizational IT security.  **LO4** Manage organizational security. |
| **Assignment Brief and Guidance** |
| You work for a security consultancy as an IT Security Specialist.  A manufacturing company “Wheelie good” in Ho Chi Min City making bicycle parts for export has called your company to propose a Security Policy for their organization, after reading stories in the media related to security breaches, etc. in organizations and their ramifications. Part 1 In preparation for this task you will prepare a report considering:   1. The security risks faced by the company. 2. How data protection regulations and ISO risk management standards apply to IT security. 3. The potential impact that an IT security audit might have on the security of the organisation. 4. The responsibilities of employees and stakeholders in relation to security.  Part 2 Following your report:   1. You will now design and implement a security policy 2. While considering the components to be included in disaster recovery plan for Wheelie good, justify why you have included these components in your plan.  Part 3 In addition to your security policy, you will evaluate the proposed tools used within the policy and how they align with IT security. You will include sections on how to administer and implement these policies |

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO3** Review mechanisms to control organisational IT security | | **D2** Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment. |
| **P5** Discuss risk assessment procedures.  **P6** Explain data protection processes and regulations as applicable to an organisation. | **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. |
| **LO4** Manage organisational security | | **D3** Evaluate the suitability of the tools used in an organisational policy. |
| **P7** Design and implement a security policy for an organisation.  **P8** List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion. | **M5** Discuss the roles of stakeholders in the organisation to implement security audit recommendations. |

**P5. Discuss risk assessment procedures.**

With daily growing threats to sensitive data in both number and sophistication, organizations are unable to afford a scattershot approach to security. Instead, in their unique security posture, they need to focus their limited IT budgets and resources on the specific vulnerabilities.

To do this, the threats to the security, credibility or functionality of their records or information systems must be defined, evaluated and prioritized depending on both the probability of the incident and the degree of effect it would have on the enterprise. So, process is called an assessment of the IT risk.

Most regulatory regulations require an IT risk assessment. Of starters, if your company is required to comply with HIPAA or is likely to face GDPR audits, then information security risk assessment is a must for your organization to minimize the risk of non-compliance and huge fines.

**Step 1**: **Collect the information you need to assess risks.**

Here are a few ways to do it:

* Interview management, data owners and another employee.
* Analyze your systems and infrastructure.
* Review documentation.

**Step 2: Find all valuable assets across the organization that could be damaged by the threats. Here are just a few examples:**

* Severs
* Website
* Client contact information
* Trade secrets
* Customer credit card data

Because most organizations have a limited risk management budget, you'll actually need to narrow the project's focus to mission-critical properties. Thus, you need to identify a norm to assess each asset's value.

**STEP 3: Identify threats and their level:**

* Natural disasters: Floods, hurricanes, earthquakes, fire and other natural disasters can destroy much more than a hacker.
* System failure: The likelihood of system failure depends on the quality of your computer for relatively new, high-quality equipment, the chance of system failure is low.
* Accidental human interference: This threat is always high, regardless of your business. Everyone can make mistakes such as accidentally deleting important files, clicking on links to malware, or accidentally damaging a piece of equipment.
* Malicious humans:

Interception is traditional hacking, where your data is stolen.

Interference is when someone causes harm to your company by removing records, designing a distributed denial of service (DDOS) against your website, taking a device or server physically, and so on.

Impersonation is abuse of the identities of someone else, which are often obtained or bought on the dark web via social engineering attacks or brute-force attacks.

**Step 4: Assess the Impact a Threat Could Have.**

* The mission of the system, including the processes implemented by the system.
* The criticality of the system, determined by its value and the value of the data to the organization.
* The sensitivity of the system and its data.

An intrusion or adverse occurrence may result in security, credibility and functionality of the information system being damaged or destroyed. As with the estimation of chance, it is important to assess the impact on the system qualitatively like large, medium or low.

The following additional items should be included in the impact analysis:

* A weight calculation based on the relative impact of a particular threat that exploits a particular weakness.
* The estimated frequency of the threat’s exploitation of a vulnerability on an annual basis .
* The approximate cost of each of these occurrences.

**Step 5: Prioritize the Information Security Risks.**

For each threat/vulnerability pair, determine the level of risk to the IT system, based on the following:

* The likelihood that the threat will exploit the vulnerability.
* The impact of the threat to exploit the vulnerability successfully.
* The adequacy of current or planned security controls of the information system to eliminate or reduce the risk.

**P6. Explain data protection processes and regulations as applicable to an organization.**

**Step 1. Encrypt the data information.**

This is the first step in the process of preservation of the information system. You're familiar with reading newspapers nowadays, buying goods, trading on the Internet. All online activities on the network have the potential for data and information security. Encode important data is one of the answers to this problem.

**Step 2. Use a strong password**

Here are some tools that will help you create a strong password that even a large attack can be difficult to crack. Tools to help create strong passwords include:

* PC Tools Random Password Generator
* Strong Password Generator
* Good Password
* GRC Ultra High Security Password Generator

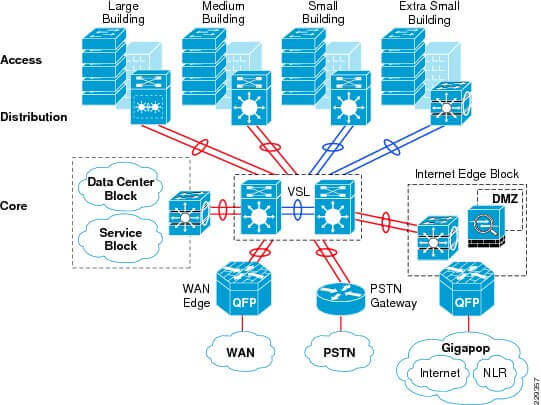
But it will sometimes make it harder for you to recall using strong passwords. Using the LastPass is the answer. It device will help you safely and effectively maintain your passwords.

**Step 3: 2-step verification**

Even if you have set a strong password and your data is encrypted, you may still lose your password when it is transmitted over an insecure wireless network such as a Wi-Fi network at a cafe or a school network. To be able to protect data yourself, in the third step of the information system security process, you use 2-step verification mode, also known as 2-layer authentication. This means that in addition to your password, you need another information to log in to the website or service.

**Step 4. Secure comprehensive network system**

Another aspect of security of information is how you connect with the outside world. What network protocol are you using at the moment? How often are low-security networks accessed? By switching off SSID Broadcast, turning on MAC Address Filtering and AP Isolation, you can increase security when setting up the WIFI router. Enable firewalls on your router and computer to prevent the application.



**Step 5. Use anti-virus software**

If this information system has viruses or malicious software that illegally entered your system to help hackers gain control, the above security steps will be useless. Remote control of your device or simply steal your device's data. The answer to this problem is the use of anti-virus software. Some antivirus software like Avira, Avast, can be used! Or maybe AVG...

**P7. Design and implement a security policy for an organisation.**

* Policy brief & purpose

Our Company Data Privacy Policy relates to our dedication to handling with utmost care and secrecy details about staff, clients, partners and other stakeholders.

This policy refers to all parties that provide us with any amount of information (employees, job candidates, customers, suppliers, etc.).

* Who is covered under the Data Protection Policy?

This policy must be followed by our company employees and their subsidiaries. Also covered are contractors, consultants, partners and any other outside entity. Our policy generally refers to anyone with whom we collaborate or act on our behalf and may require access to data from time to time.

* Policy elements

We need to get and process information as part of our operations. This information includes any offline or online data making a person identifiable, such as names, addresses, usernames and passwords, digital footprints, photographs, numbers of social security, financial data, etc.

Our organization gathers this information in a transparent manner and only with the partners ' full cooperation and expertise. Once we have this knowledge, the following rules apply.

* Our data will be:

Precise and up-to-date

Collected fairly and only for lawful purposes

The business is operating within its legal and moral limits

Protected from any illegal or unauthorized access by internal or external parties

* Our data will not be:

Communicated informally

Stored over a specified time period

Transferred to companies, states or countries where data protection laws are insufficient

Distributed to any party other than the ones agreed by the owner of the data (exempting legitimate law enforcement requests).

**Actions**

To exercise data protection, we’re committed to:

Restrict and supervise access to sensitive data

Develop transparent procedures for the data collection

Train staff in data protection and security measures online

Establish secure networks to protect online data against cyber-attacks

Set clear procedures for reporting privacy infringements or data misuse

**Public policy**

Make public use policies and share information with customers. Respect the privacy of customers by disclosing information in a transparent way such as IP address, search history, preferences ..., the purpose and how to use this information and the treatment information processing and / or sale of information to third parties.

**Empower customers**

Reserve the right to decide to share and use information for customers by allowing customers to choose to be an exception to the general policy (for example, not sharing customer information with partners). As such, these solutions emphasize users' right to know and decide on their own personal information.

Once a business has established a transparent privacy policy, customers will feel more confident when deciding to share information, and can change privacy options at any time. The study also shows that at businesses with a clear privacy policy, customers have a positive response to the fact that they are not being used for market research, feel more confident and tend to provide more accurate and sympathetic information when businesses encounter information security incidents and contribute to strengthening the company's brand.

When detecting a hacked system, through signs such as traffic, information (traffic) increased unexpectedly, the system is unusually slow, the following basic steps should be taken:

Step 1: Disconnect from the network.

Step 2: Copy the logfile and all data of the system to the storage device.

Step 3: Coordinate with agencies and organizations specialized in cyber security to find out the causes and solutions.

Step 4: Restore the system by transferring the latest backup data for the system to work.

**Account management organization of information systems:**

Information system account management organization, including: establishment of an account, activation of accounts created, alteration of account information, disabling and elimination of accounts. At the same time, auditing information system accounts at least once a year and using software to support IS account management.

Manage 03 times the number limit for consecutive logins in an account. The system will automatically lock account or isolate account for a certain period of time before continuing to log in if it incorrectly logs in exceeding prescribed times.

Organize management of user identification and decentralization of users in groups (departments and boards). Provisions on rights and limits on access time to users' information systems.

**Responsibilities of agencies and organizations:**

Arranging sufficient civil servants, administrators and technicians to ensure digital information systems are safe. Planning professional training for officials and employees of digital information security, training, disseminating knowledge and skills for computer users on prevention and control of risks of information insecurity number when using the Internet.

When incidents or risks of information insecurity occur, the head of the unit must promptly direct and apply all measures necessary to overcome and limit damage.

**P8. List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion.**

Often, the weakest part of a business’ preparedness and recovery plan is not taking seemingly minor or unlikely disasters seriously. Types of disasters that could affect a business include:

* Building fires
* Wildfires
* Earthquakes
* Landslides
* Biological threats
* Severe storms
* Power outages
* Acts of violence or terrorism
* Cyber-attacks and network intrusions

Having a strategy for recuperating a disaster does not mean preventing a disaster, but it will greatly reduce its impact. With the most important applications in production, a good disaster recovery plan will help businesses to recover fast.

1. Have full documentation

When a disaster recovery plan is fully documented, it is easy to get support from senior management and ensure that the stakeholders know what to do.

The disaster recovery strategy document should address goals and tactics, as well as roles and responsibilities - including emergency contact numbers - initial incident response and who is involved. at each stage of the plan.

1. Risk assessment

Best practice in business begins with a risk assessment and disaster recovery. A good disaster recovery strategy will look at all the functional areas of the business, ask them what potential threats they are facing and which IT resources they will rely on.

A complete inventory of IT machines and data audits can help accomplish this task by identifying all important software applications and any hardware infrastructure needed to run them.

1. Priority resilience

Disaster recovery is one of the enterprises that have to budget for IT resources with the expectation of never needing to use it. That's why redundancy is so critical in IT infrastructure structures and it has become a guiding principle.

The most important principle when it comes to resilience is to avoid having unique points of failure. If a main application runs from a single server and can only run from that server, then that is a potential weakness.

Failover connections, uninterruptible power supplies, backup generators and standby servers can all help reduce the risk of disaster.

1. Consider the cloud

Disaster recovery is a service (called DRaaS for short)! Not all cloud-based disaster recovery systems are the same or work the same way; some provide cloud-based backup and recovery; others use virtualization to maintain a copy of servers and applications.

Cloud disaster recovery has advantages and disadvantages, but like many other cloud-based services, it is accessible without paying an upfront investment fee for backup and recovery hardware.

1. Evaluate security practices

Safety is a separate subject, but is inextricably linked to solutions for recovery from disasters. In theory, well-implemented safety practices minimize the risk of catastrophe.

However, as part of a comprehensive approach for recovery from crises, it is important to analyze potential security weaknesses and take action as appropriate to strengthen them, as well as to anticipate what will happen if the safety mechanisms are breached.

1. Disaster recovery program

A disaster recovery plan should contain the following:

* Statement, overview and the Plan's main objectives.
* Contact information for key personnel and disaster recovery team members.
* Describe immediate emergency response actions following a disaster.
* Diagram of the entire IT network and recovery site. Don't forget to instruct staff on how to access the recovery site when needed.
* Identify key IT properties, and assess overall downtime. Understand the words Reference Recovery Point (RPO) and Time Goal (RTO) for Recovery.
* List of software, copyright codes and systems that will be used for recovery.
* Insurance contract summary.
* Proposals for addressing financial and legal issues, as well as access to media.

1. Create a disaster recovery team

IT team members responsible for the company's important IT infrastructure need to work together to implement the plan. Others who need to know the plan include executives or directors, department leaders, human resources, and public relations.

# References

Anon., n.d. [Online].

<https://luutru.gov.vn/su-can-thiet-phai-thuc-hien-chinh-sach-bao-mat-va-an-toan-thong-tin-so-trong-cac-co-quan,-to-chuc-78-vtlt.htm>

<https://www.triumph-motorcycles.com.vn/chinh-sach-bao-mat-va-thong-tin-ca-nhan>

<https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html>

<https://www.polygongroup.com/en-US/blog/top-5-components-of-the-best-business-disaster-recovery-plans/>

<http://ictvietnam.vn/tuong-tac/khoi-phuc-tham-hoa-dam-bao-tinh-hoat-dong-lien-tuc-cua-doanh-nghiep.htm>