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	Nguyen Quoc Viet	**Student ID**	GCC18157
Class	GCC0701-1623	**Assessor name**	THAI MINH TUAN

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	Nguyen Quoc Viet

Grading grid

P5	P6	P7	P8	M3	M4	M5	D2	D3

❒ Summative Feedback:	❒ Resubmission Feedback:

Grade:	Assessor Signature:	Date:
Signature & Date:		

Assessment Brief

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 organisation, after reading stories in the media related to security breaches, etc. in organisations 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.

- **Network Configuration and Change Management (NCCM)**

- Organizing and maintaining information on all components in a computer network becomes significantly easier.

- Network device configuration information will be stored on a centrally located server, where device settings are easily accessible.

- The network administrator looks to the network configuration control database to determine the best course of action when fixes, modifications or enhancements are needed.

- Comprised of inspection and use:

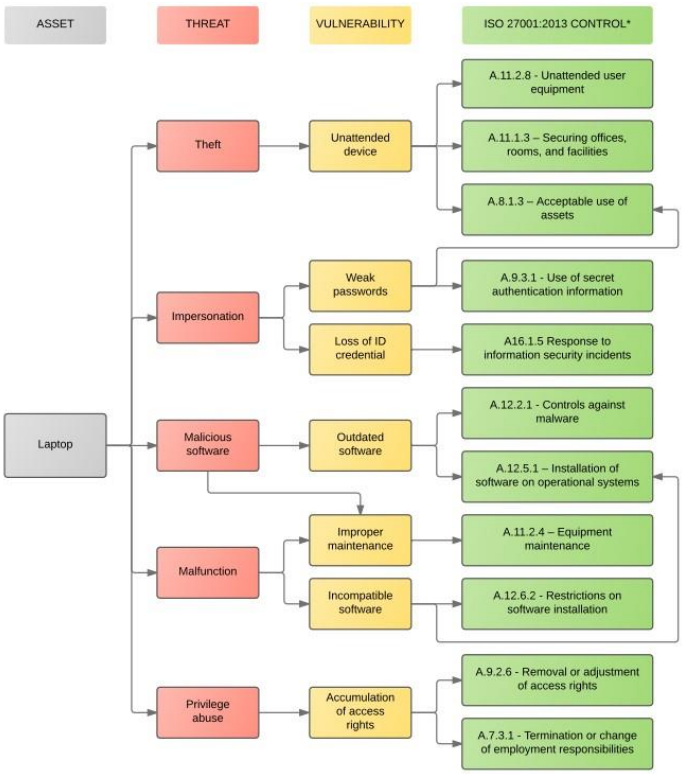
  - Regular testing of system configuration files to detect any configuration file modifications that might expose security attacks and possible failures.
  - Making major improvements such as introducing widespread modifications of passwords on computers across the network.
  - Auditing and monitoring so that information about network elements can be easily tracked.

- **Business continuance**
  - While a security audit will find vulnerabilities that should be fixed, and a company will make every effort to correct those shortcomings, there will always be a chance of breach of security.
  - It is for this reason that a risk analysis and a contingency plan should be drawn up.
  - The contingency plan will cover replication, offsite storage, systems for data recovery, access to urgent equipment repair, plus insurance for upgrade, company failure and all recovery work.
- **Audit control**
  - A company that is unsure of how and where violations of security could arise will quickly be faced with a problem that would cause costly.
  - Alternatively, a vulnerability assessment should be performed to test what could go wrong, and to prepare changes before a hacker–or some other person–takes advantage of the situation.
  - Audits could include:
    - Review and management: Example, when you login into systems or websites, that need to monitored.
    - Establishment and review of trust in personnel, business and technical matters.
- **Potential loss of data/business**
  - **Loss of data**
  - When data is lost, data recovery expenses will be borne.
  - A backup should be available if information is compromised, but the repair would take time and incur staff costs.

- Depending on how serious a breach has been experienced, specialists may need to be consulted, and this too will entail additional costs

- **Loss of business**
  - A security breach will cause an ICT system to collapse.
  - The time when standard service is not available is considered downtime.
  - Organizations who rely on an ICT system to take orders during downtime will suffer a loss of revenue. Many clients will return later but some will not; they will have moved their company elsewhere already.
  - If a breach of security involves data loss, and it proves difficult to retrieve the data, then the outcome for an enterprise can be catastrophic.
- **Intellectual property**
  - Intellectual property protection lets you deter people from stealing or copying: the names of your goods or trademarks of your creations, the nature or image of your products, items you publish, create or produce
  - Name or brand of company's products: Example, bicycles of Wheelie good have a specific brand.
  - The company's bike designs can be designed with their own accents or decorative colors on the bike, accessories, …
  - All types of intellectual property protection include copyright, patents, designs and trade marks. You automatically get certain types of protection, others that you have to apply for.
- **Hardware and software**

To assess risks for hardware and software, we are based on ISO 27001 Risk Assessment and Treatment Process.



- Diagram of ISO 27001 risk assessment and treatment process EN.pdf:

https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/Diagram_of_ISO_27001_risk_assessment_and_treatment_process_EN.pdf

- The probability of occurrence
- Theft: computer theft is highly likely. Especially when the business is a company of bicycles and machinery, this is simple for those who wish to rob. Tools that include keyboards, monitors, mouse, hard drives,... Even items that criminals can target when not strictly controlled.
- Disaster: Natural disasters are what most of the world's businesses worry about, and this is unintended and can have major consequences. The organization also has to have predetermined scenarios so its workers have the skills to deal with in the case of a natural disaster.Data Protection Act (2018:
    - Implementation of General Data Protection Regulation(GDPR)
    - Stringent rules dubbed ' data protection standards ' Improved legal protection for more sensitive information
    - Sets out rights to learn what information the government and other institutions store on you
- Computer Misuse Act (1990):
    - Protect users of computers from attacks and information theft.
    - Common action:
        - Hacker.
        - Access to the system without permission
        - Distribute viruses
- ISO 31000 standards:

• The purpose of ISO 31000 is to provide criteria and general guidelines for risk management. ISO 31000 aims to provide a universally recognized paradigm for professionals and companies using risk-management processes to replace the myriad of existing standards, methodologies and paradigms that differ between industries, topics and regions.

• Strategies for risk management include: planning, implementing, assessing and understanding.

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

Data protection is the process of safeguarding important information from corruption, compromise or loss

Process of data protection:

1. Evaluate network security risk

Once you've got all the data your organization has, you need to do an assessment of the risks that your organizational data may encounter:

+ In case of occurring network security incidents..

+ In case of occurring incident natural disasters such as fires and earth quakes

After performing risk identification for the data you need to protect, you need to take security measures for your organization's network system. This will allow you to know exactly what security risks are and will already happen to the general organizational network and data security of organizations in particular. Since then, implementing patching measures, protect the system or deploy security solutions that are suitable for models and finance and organization requirements.

2. Raise awareness about data security for employees

One of the most potential hazards with an organization's data security is the human factor. Therefore, the implementation of measures to train and raise employees' awareness about data security is one of the leading and most effective measures to ensure data safety in your organization.

Enterprises need to organize awareness programs, training data security for organization and network security periodically. It is the most important solution to minimize organizational data breaches, save financial outsourcing security services outside. At the same time, the organization needs to have documents and documents on data security policies and work processes, use data in the company to apply management standards and ensure data safety such as ISO 27001, PCI DSS. These documents will also be used to train awareness and apply data security policies in the enterprise...

3. Data security administration

Security risks to organization data always occur at any time. Therefore, it is not possible to implement security measures in a short period of time but need to be carried out regularly and continuously. If possible, each organization should have a specialized leader or individual, with knowledge about the security and data security of the organization responsible for monitoring the implementation of security measures and processes ensure data safety. This will help minimize the risks of network security for businesses and organizational data.

4. Fix and manage problems

Documents on the response process when incidents of security for the network and data of enterprises occur are necessary to minimize the damage caused by network security incidents to enterprises.

A wildfire like security incident. You need to prevent damage if you have discovered an incident and its source. This may include disabling network access for virus or other malware infected machines (so that they can be isolated) and installing security patches to prevent them. Solve vulnerabilities in malware or network. You may also need to reset passwords for employees whose accounts have been compromised, or block people's accounts in the company that may cause the issue. Furthermore, your company should support all affected systems in order to maintain their current forensics status.

Next, move on to any needed service recovery, including two important steps:

1. Perform system / network verification and validation to certify all systems are operational.

2. Reconfirm any compromised components, both operational and safe.

In general, look at the cause of the incident. In cases where there was a successful external attacker or malicious insider, consider the event as more severe and respond accordingly. At the right time, review the pros and cons of launching a full-fledged cyber attribution investigation.

5. Training should be given so that employees know what to do, for example, if they suspect a virus attack:

Who should they contact first?

Should they turn their ICT system off?

Employees also need to know what to do if they think their login ID is being used by someone else:

Who should they inform of their fear?

What methods might be used to trap the culprit?

What procedures should be followed to prevent similar lapses in security in future.

Business continuance

While a security audit will recognize deficiencies that need to be fixed and a company will make every effort to correct those vulnerabilities, there is always a chance of a breach of security.

For this reason, a risk analysis and a contingency plan should be drawn up.

The contingency plan would include backup, offsite storage, procedures for data recovery, access to immediate equipment repair, plus insurance covering replacement, company failure, and all recovery work. Ability of an organization to maintain essential functions during, as well as after, a disaster has occurred.

6. Hardware and software

Risk assessment of this take place through ISO Risk Assessment and Treatment Process.

7. **Probability of occurrence**

Consider the following when outlining likelihood of security risks:

+Disaster

+Theft

How can a company meet the following

+Data Protection Act (2018Computer Misuse Act (1990)

+ISO standards.

What are staff responsibility's in this process? Explaining why data is collected, how it is stored, management of data, following security guidelines.

8. **Data Protection Act 2018**

Implementation of General Data Protection Regulation(GDPR)

Outlines strict rules called ‘data protection principles”

There is stronger legal protection for more sensitive information, such as:

Race, ethnic background, political opinions, religious beliefs, trade union membership, genetics biometrics (where used for identification), health, sex life or orientation

Outlines rights to find out what information the government and other organisations store about you.

9. Computer Misuse Act (1990)

Protect computer users against attacks and theft of information.

Offences under the act include:

+ Hacking,

+ Unauthorized access to computer systems

+ Purposefully spreading malicious and damaging software (malware), such as viruses.

10. ISO standards

Provides guidelines for dealing with today’s threats

Not requirements, and is therefore not intended for certification purposes.

Risk management guidelines include:

+Planning

+Implementing

+Measure

+Learn.

11. **Company regulations: Site or system access criteria for personnel;**

It should not be easy to walk into a facility without a key or badge, or without being required to show identity or authorization.

Controlling physical access is your first line of defense, by protecting your data (and your staff) against the simplest of inadvertent or malicious intrusions and interferences.

Physical security types could include e.g. biometrics, swipe cards, theft prevention (Cameras).

P7 Design and implement a security policy for an organization.

Information Technology Security Policy

CONTENTS

I. Introduction

The ease with which data can be passed inside and outside the College, often by computer, is an undoubted advantage for employees involved in the provision of services. All those concerned must be aware of the legal obligation to protect the confidentiality of College information.

Several tools are available today to eliminate external threats to the network-firewalls, antivirus software, intrusion detection systems, email filters and other devices-these services are mostly used by IT personnel and are not detected by users.

However, proper network usage in a company is a management issue. Acceptable use policy(AUP) implementation, according to the definition that governs employee behavior.

This IT Security Policy is based on that expectation, but also recognizes that college staff will need controlled access to learner, financial, and staff information to ensure the college functions effectively, efficiently, and in a safe manner.

II. Definitions

- "User" is anyone who uses College hardware or software.

- "College equipment" means hardware, software, or any other system related to IT operated by the College.

- "Confidentiality" means ensuring that information is accessible only to those authorized to have access.

- "Integrity" means safeguarding the accuracy and completeness of information and processing methods.

- "Availability" means ensuring that authorized users have access, when required, to information and associated assets.

III. Rationale

The College must protect its information asset, defined as computers, equipment, networks, software and all the data it contains, and its credibility, for the purposes of this Policy. This will help the College in:

+ Ensure that a high quality service is offered to our staff, students and other clients.

+ Ensure that it does not lose opportunities for funding through a poor reputation for information security.

+ Maintain and improve its reputation and meet the legal obligations and strategic business and professional goals of university student management.

+ Prevent data loss.

+ Ensure that users are aware of their personal responsibilities for protecting data in accordance with College or any external organization's guidelines.

IV. Core Principles

The College must comply with a variety of legislation in this regard, including but not limited to:

The Data Protection Act 1998;

The Human Rights Act 1998;

The Computer Misuse Act 1990;

The Regulation of Investigatory Powers Act 2000;

The Freedom of information Act 2000;

The Copyright, Designs and Patents Act 1988;

The Electronic Communications Act 2000;

- University system security will be monitored proactively and security breaches will be reported, investigated and the cause rectified as soon as possible.

- Only appropriate use will be made of University equipment and in particular of the data held within.

- Notwithstanding the requirements of the Data Protection Act, the College retains its right to monitor the use of its systems by any user in order to protect its legitimate business and reputation.

- Appropriate internal and external systems will be employed to help the University ensure the security of its systems.

- Due thought and consideration will be given to information security risks prior to implementation of new systems.

V. Equality Analysis

Under the Equality Act 2010, schools are obligated to meet the following needs:

+ Eliminate unlawful discrimination and other prohibited conduct;

+ Advance equality of opportunity between people of different groups;

In implementing this Policy and associated procedures, the College will actively take these aims into account as part of its decision making process and will demonstrate how this has been undertaken.

Where necessary a full equality impact assessment will be undertaken.

VI. Implementation, Monitoring and Review

1. Responsibilities

- The E-Services department has responsibility for coordinating IT Security.

- Members of E-Services must be endowed with sufficient and appropriate authority, allowed direct access to all users and data, and be capable of establishing the effectiveness of the security procedures.

1.1 E-Services

+ Ensure that IT systems in use are properly tested for compliance with security and are secured in accordance with the IT security policy

+ Requests for systems by internal departments should incorporate an appropriate assessment of security requirements.

+ Ensuring backup systems remain fit for purpose.

+ Ensuring Anti-virus guards remain fit for purpose.

+ Ensuring external threats are mitigated through sufficient firewall protection.

+ Ensuring appropriate levels of access are provided to students.

+ Ensuring that the IT security standards are implemented effectively and reviewed.

1.2 Users

+ Comply with the University Information Security Policy and related policies and procedures.

+ Comply with Legislation and Guidelines.

+ Notify E-Services immediately of IT security breaches which come to their attention.

+ Be proactive in promoting network security, especially when it comes to learners understanding policies and procedures.

+ Notify the School immediately of any information breaches that come to their attention.

+ The School may be required to share information with external agencies.

2. Remote Services

- The school recognizes that remote access to systems is important and sometimes necessary to the learner experience due to the nature of delivery. The aim of the school is to provide remote access to systems with due security consideration. Not all systems are capable of remote control, nor should the presumption be that any device can be remotely accessed. An assessment of risk, technical capability and need would define the decision.

- The College website currently offers email, Virtual Learning Environment (Moodle), One Class, Extranet and the Box. Other networks can be reached using a Virtual Private Network Connection. Users are required to get approval from the line manager and sign a contract before they are equipped with VPN access.

- Where security information is required in order to access a remote system encryption must be implemented. EServices will advise of and provide the necessary certification.

- Third parties can sometimes require access to the College network (Example: to conduct maintenance tasks or to provide support. By checking with E-Services, users must not share the access information with the third party. EServices can specify an acceptable access method for a fixed period of time, depending on the requirements).

3. Anti-Virus

- The deliberate introduction of malicious software to a system is a criminal offence under the Computer Misuse Act 1990.

- E-Services will seek to minimize network contamination by remaining proactively up-to-date with applicable antivirus software. Users should be diligent in contacting E-Services on any system they have access to should they be concerned with Anti-Virus software.

- Where users suspect a virus, no files should be loaded on to any system from an external device without prior consultation with E-Services.

- All servers and most PCs have anti-virus software installed.

- Where a virus is detected this will be reported immediately to E-Services who will attempt to “clean” and rebuild the affected PC and update the anti-virus.

4. Mobile Devices

-The large scale rise in the use of mobile devices and hosted services, including but not limited to, laptops, USB/Flash memory, PDAs, Smartphones, External Hard Drives, “cloud” data storage and email, social networking, presents a challenge to the security of data.

- Laptops are capable of holding the users ' own personal "home" drives as "shadow copies." Access to the shared folders is via VPN only. Users must abide by Data Protection guideline and legislation when considering what to store on their allocated drives. Failure to give due consideration to the principles of the Data Protection Act could lead to disciplinary procedures, for example personal data of students should not be held on laptops.

- Use of USB sticks, flash cards or external storage should be given consideration, particularly in relation to personal data. Encryption tools are available with guidance from E-Services.

5. Protection of hardware

- Purchasing, maintenance and disposal of hardware must be done in conjunction with E-Services.

- No equipment should be removed from any site or room without the approval of E-Services, except for portable laptops or devices that are the responsibility of each named individual user or department.

- Hardware in particularly vulnerable areas or containing sensitive data should make use of physical security measures such as locking office doors or installing locking devices to secure hardware to desk.

- All personal computers and non-essential peripherals should be switched off when not in use for extended periods, such as overnight or during weekends, except for essential Server Room equipment or local site servers.

- Any storage needs to be stored in locked tables or fireproof equipment.

6. Protection of data from hardware loss

- Data should not be held locally on PCs or laptops, as this is not included in the automatic nightly backup of the network servers. Data should be saved to servers (ex: U:drive, shared folders, Moodle, extranet). E-Services cannot be held responsible for loss of data that is stored on a local drive.

- Backup sets will be stored securely through an appropriate strategy using School campuses, defined by the EServices Manager.

- Backup recovery procedures will be tested on a regular basis.

- The University Disaster Recovery plan is reviewed by the Vice Principal for Corporate & Business Development.

7. Protection of data from unauthorized access

- Staff account passwords controls must be implemented. Passwords will have the following characteristics enforced:

+ Be at least 6 characters long;

+ Contain letters and numbers;

+ Be different from the 5 previous passwords used;

+ Be user generated;

+ Will be required to be changed every 90 days.

- Learner passwords are set to have no time limit, however their accounts expire on the finish date of their course + 30 days, as set in the student records‟ system, therefore provision of accurate course details to are essential.

- System password details are recorded by E-Services and kept securely.

- To prevent others gaining access to network accounts care should be taken when logging in to the network to prevent "shoulder surfing".

- Account passwords should not be revealed to users other than yourself, nor written down and placed in areas of view (e.g. on monitors). Unauthorized access to data by a 3rd party due to negligence could lead to disciplinary procedures.

8. Localized data

E-Service cannot be held responsible for the management and protection of internal local databases that are developed without due consideration of risks or consultation. . Under the Data Protection Act, schools are required to notify administrators of the data they hold and process.

9. Software Control

A register of College owned software will be maintained by E-Services.

Software must not be copied or distributed, as this is an infringement of copyright and therefore illegal - unless specifically permitted by the licensing agreement.

All System Software media will be stored securely with E-Services. These are the only proof of a legal license to use the software, and may be required to be produced in evidence should the Federation against Software Theft (FAST) investigate.

10. Quality Assurance and Review

1. All staffs are expected to ensure that users of the network abide by the policy. Any breach of this policy should be reported in the first instance to a member of the E-Services team who will then define a method for resolution.
2. This Policy will be reviewed every three years and updated, as applicable, to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations

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

Start by taking stock: A good recovery plan for a tragedy begins by understanding what you've got, where you've got it and how it's designed. Start the inventory with evaluation of the physical space. Server spaces, centers for network processing, a data center–wherever IT hardware is housed. Remember the hardware in every single space.

Moving on to Virtual Machines, Systems, and Windows:

- Server Software
- Hypervisors
- Locally Hosted Applications
- Cloud Hosted Applications + Vendor Support Contact
- Any settings that would aid restore after a catastrophic event. (Lovinus dated 29 March 2018)

Business management rating systems by importance: Identify and rate critical systems according to their usefulness.

You must know, before a tragedy strikes:

1. What you need to get your systems restored
2. How long does it take
3. Who carries out every mission

Measure the cost of downtime in the Business Impact Analysis (BIA)

How you measure downtime costs for each business will be different, but here is a benchmark estimate that accounts for several common factors: downtime = lost income + lost productivity + lost equipment replacement costs + intangible expense.

Estimate lost productivity:

Consider lost productivity as the cost of paying workers for their labor, but not getting anything in exchange because they can't work during downtimes.

Potential replacement costs:

Traditional replacement costs for IT would include specialized suppliers to recover lost documents and any actual replacement items. Ensure that the direct costs of data that can not be recovered are factored into, and any effects of that data loss over time.

Make sure everyone knows their role:

Chaos prevails when a disaster strikes. The more prepared you are, the quicker you can get processes back up and running.

Rehearsing and upgrading whenever the processes and staff change:

- The IT disaster recovery plan is a living document. It's to be tested and tuned continuously. The most critical time to review the proposal is when it will be yours too

REFERENCE

Lovinus, A., March 29, 2018. *12 Elements of an IT Disaster Recovery Plan.* [Online]
Available at: https://www.neweggbusiness.com/smartbuyer/datacenter/12-elements-disaster-recovery-plan/

Robinson, N., Graux, H., Botterman, M. and Valeri, L., 2009. Review of EU data protection directive: summary. Information Commissioner's Office.

Policy, I.C.R., 2012. Procedures. Policy, 1, p.6.

ccohs.ca, 2017. *Risk Assessment.* [Online]
Available at: https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html
[Accessed 14 January 2020].

file:///D:/Sercurity/New%20folder/Security%20Policy%20Templates/IT%20Security%20Policy%20%20SLC.pdf
[Accessed 14 January 2020].