ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date	11/01/2021	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Pham Cao Nguyen	**Student ID**	GCC18074
Class	GCC0801	**Assessor name**	Le Huynh Quoc Bao

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	CaoNguyen

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			
Unit Tutor			
Issue date		**Submission date**	
IV name and date	Khoa Canh Nguyen, Michael Omar, Nhung 9th/01/2020		

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:
The security risks faced by the company.
How data protection regulations and ISO risk management standards apply to IT security.
The potential impact that an IT security audit might have on the security of the organization.
The responsibilities of employees and stakeholders in relation to security.

Part 2
Following your report:
You will now design and implement a security policy
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		

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.	**D3** Evaluate the suitability of the tools used in an organisational policy.

Contents

Discuss risk assessment procedures.

1. **Risk definition**
    - Risk is a business concept-an organization's potential financial loss. Three factors determine risk: what is a danger, how fragile the system is, and how critical or unavailable the asset may be.
2. **Definition risk assessment.**
    - Risk assessment is the identification of hazards that could negatively impact an organization's ability to conduct business. These assessments help identify these inherent business risks and provide measures, processes, and controls to reduce the impact of these risks to business operations.
    - Companies can use a risk assessment framework (RAF) to prioritize and share the details of the assessment, including any risks to their information technology (IT) infrastructure. The RAF helps an organization identify potential hazards and any business assets put at risk by these hazards, as well as potential fallout if these risks come to fruition.
3. **What does a risk assessment include?**
    - Risk assessment includes inspection, change management, privilege management, incident management, risk calculation, and representation of risk information.
    - The risk assessment check should include an inspection of the technology assets to identify any gaps. The software scans the software automatically for any known security weaknesses through a system and then generates a report of those potential exposures.
    - Intrusion testing system: Engineers and cybersecurity experts will play the role of a hacker, then penetrate the system from outside and inside to identify vulnerabilities as well as potential threats to the system website, intranet.
4. **Why assess risk?**
    - Because the company always has security holes.
    - Comprehensive network security risk assessment will help you know the system's weaknesses before the hacker comes in.
    - Help comprehensive data security.
    - Create awareness about the dangers and risks.
    - Determine who may be at risk.
    - For a particular hazard the determination of a control program is necessary.
    - Determine if current control measures are adequate.

  - Priority hazards and control measures.

5. **The objective of risk assessment.**

- The objective of the risk assessment process is to determine hazards, then remove the danger or reduce the risk level by adding the controls necessary.
- The objective of risk assessment is to answer the following questions:
  - What can happen and under what circumstances?
  - What are the possible consequences?
  - How likely are the consequences possible?
  - Is risk effectively controlled, or what is the next course of action?
- Some common goals and objectives for conducting risk assessments across industries and business types include the following:
  - Developing a risk profile that provides a quantitative analysis of the types of threats the organization faces.
  - Developing an accurate inventory of IT assets and data assets.
  - Justifying the cost of security countermeasures to mitigate risks and vulnerabilities.
  - Developing an accurate inventory of IT assets and data assets.
  - Identifying, prioritizing, and documenting risks, threats, and known vulnerabilities to the organization's production infrastructure and assets.
  - Determining budgeting to remediate or mitigate the identified risks, threats, and vulnerabilities.
  - Understanding the return on investment, if funds are invested in infrastructure or other business assets to offset potential risk.
- The ultimate goal of the risk assessment process is to evaluate hazards and determine the inherent risk created by those hazards. The assessment should not only identify hazards and their potential effects but should also identify potential control measures to offset any negative impact on the organization's business processes or assets.

6. **Risk assessment plan.**

  - Risk assessment scope (' Wheelie good ' firm)
  - Necessary resources (technical staff, information protection equipment, etc.)
  - Type of risk analysis method (test, exploit flaw, etc.)
  - Who are the stakeholders (Company, test software provider, etc.)
  - Relevant laws, legislation, rules, or guidelines may apply within the jurisdiction of the organization, as well as policies and procedures entitled "Wheelie fine."

7. **Steps for risk assessment.**

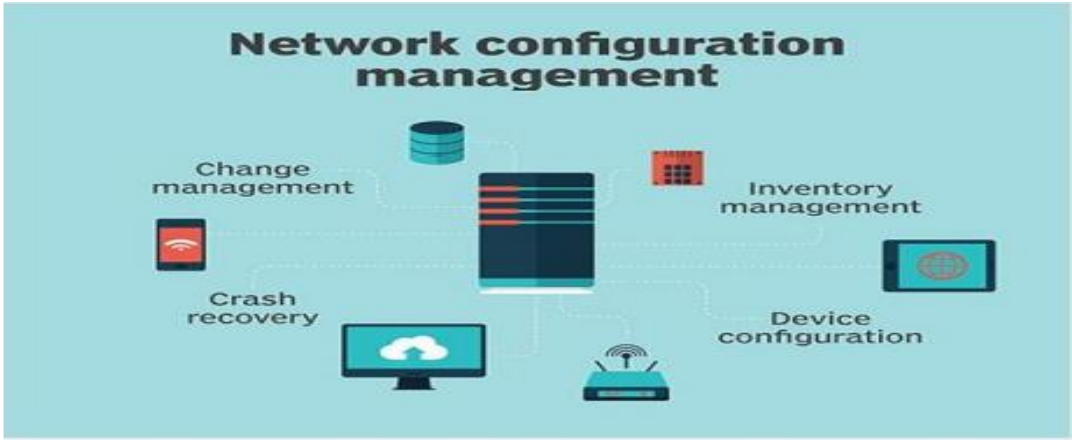
- How a risk assessment is conducted varies widely depending on the risks unique to the type of business, the industry that business is in and the compliance rules applied to that given business or industry.
  - Step 1: Identify the hazards. The first step in a risk assessment is to identify any potential hazards that, if they were to occur, would negatively influence the organization's ability to conduct business. Potential hazards that could be considered or identified during risk assessment include natural disasters, utility outages, cyberattacks, and power failure.
  - Step 2: Determine what, or who could be harmed. After the hazards are identified, the next step is to determine which business assets would be negatively influenced if the risk came to fruition. Business assets deemed at risk to these hazards can include critical infrastructure, IT systems, business operations, company reputation, and even employee safety.
  - Step 3: Evaluate the risks and develop control measures. A risk analysis can help identify how hazards will impact business assets and the measures that can be put into place to minimize or eliminate the effect of these hazards on business assets. Potential hazards include property damage, business interruption, financial loss and legal penalties.
  - Step 4: Record the findings. The risk assessment findings should be recorded by the company and filed as easily accessible, official documents. The records should include details on potential hazards, their associated risks and plans to prevent the hazards.
  - Step 5: Review and update the risk assessment regularly. Potential hazards, risks and their resulting controls can change rapidly in a modern business environment. It is important for companies to update their risk assessments regularly to adapt to these changes.
- Risk assessment tools, such as risk assessment templates, are available for different industries. They might prove useful to companies developing their first risk assessments or updating older assessments.

8. **How to use a risk assessment matrix.**
   - A risk assessment matrix, as shown in the example above, is drawn as a grid with one axis labeled "likelihood" and the other axis labeled "consequence." Each axis progresses from "low" to "high." Each event is plotted on one line in terms of its low to high likelihood. On the other line, the event is plotted on one line in terms

of its low to high consequence. Where they meet determines the plot point on the matrix.

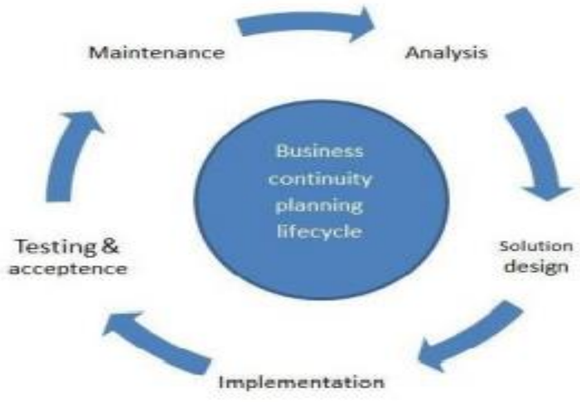
9. **Risk assessment and integrated enterprise risk management:**
    - Network change management
    - Audit control
    - Business continuance/disaster recovery plans,
    - Potential loss of data/business,
    - Intellectual property,
    - Hardware and software
    - Probability of occurrence
10. **Network configuration and change management.**
    - With this system/discipline in place, it becomes easier to organize and manage knowledge on all elements in a computer network.
    - Network system configuration information will be stored on a centrally located server where it is easy to download device configurations.
    - The network administrator refers to the network configuration management database to determine the best course of action when repairs, modifications, or upgrades are needed.

- Uses include:
    - Regular monitoring of system configuration data to identify any changes in configuration files that may expose cyber threats and potential failures
    - Creating bulk changes such as implementing mass changes to passwords on devices throughout the network.
    - Auditing and reporting enable easy tracking of network component information.
    - Creating bulk changes such as implementing mass changes to passwords on devices throughout the network.



11.Audit control

- An organization that is unaware of how and where security breaches could occur in the near future could face a costly and very embarrassing situation.
- Instead, a security audit should be conducted to check what might go wrong, and to plan improvements before a hacker – or some other individual – 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.
- An organization that is unaware of how and where security breaches could occur in the near future could face a costly and very embarrassing situation.
- For this reason, an analysis of risks should be carried out and a contingency plan was drawn up.
- This contingency plan will include backup, off-site storage, data recovery procedures, immediate equipment replacement access, plus replacement insurance, business loss, and all recovery work.
- 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.



12.Backup/restoration of data

- Employees who are responsible for data recovery should also know the procedures to follow

- The objective should be to prepare accordingly so that within a given time scale, such as 24 hours, the whole device can be up and run again.
- Then, if the worst-case situation arises, the recovery from disasters can be as quick as possible. In order to take any eventuality into account, the contingency strategy must be built from a complete risk analysis.

13.Potential loss of data/business

➢ Loss of data

- If data is lost, costs are incurred in recovering the data.
- If software is corrupted, a copy should be available, but the replacement will take time and incur staff costs.
- There will be a requirement to contact experts, based on how serious a violation has been encountered, and this, too, can incur potential costs.

➢ Loss of business

- A security breach can result in the collapse of an ICT system.
- The time during which normal service is not available is called downtime.
- During the outage, companies that rely on an ICT system to take orders will experience a loss of revenue. Such clients will come back eventually, but some will not; they will have moved their company elsewhere already.
- If a security breach causes data loss, and it proves difficult to recover that data, then the result can be disastrous for an organization.

14.Intellectual property.

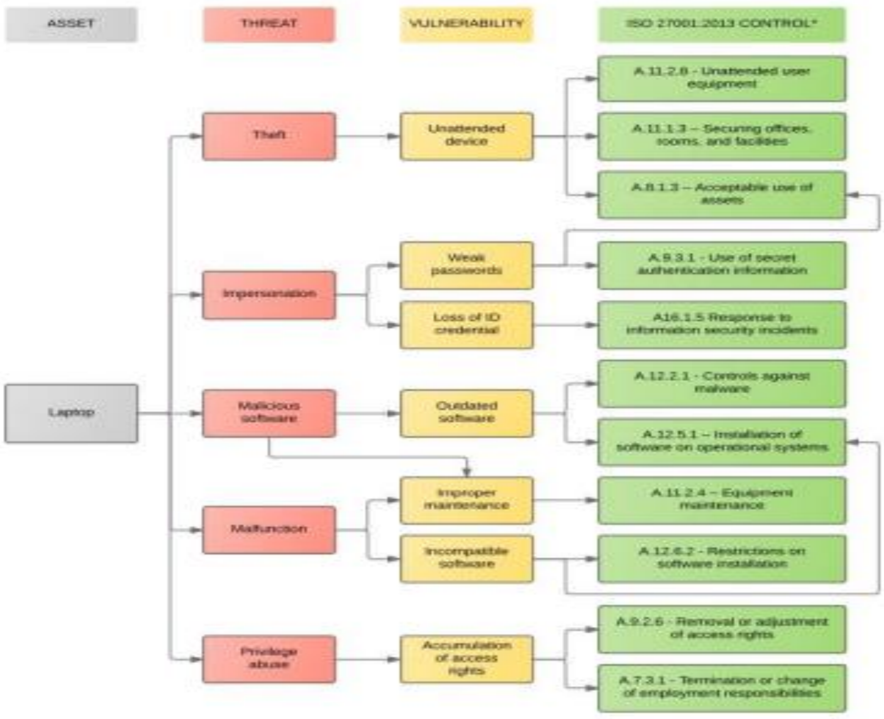
➢ Intellectual property protection helps you to stop people stealing or copying:

- The names of your products or brands
- Your inventions
- The design or look of your products
- Things you write, make, or produce
- Both forms of intellectual property rights are copyright, patents, designs, and trademarks. Automatically, you get certain forms of security, others you have to apply for.
- 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 trademarks. You automatically get certain types of protection, others that you have to apply for.

15.Hardware and software

- The risk may be considered as a potential opportunity that could be eventually exploited resulting in undesired consequences or negative impact on the operations.
- If risk were to materialize it will become an issue. Risk management is the discipline in which the risks are identified in a proactive manner and treated or mitigated.
- Technology refresh programs are carried out across companies to identify and update those devices that have reached EOL (End of Life) and stop support for. One of the aims or end goals is to ensure that in the early stages the hardware and software risks posed by these outdated systems are addressed.
- EOL hardware devices and software suite are not so effective and come with multiple ways in which they could be exploited.
- Risk symptoms are known as triggers.


ASSET
THREAT
VULNERABILITY
ISO 27001:2013 CONTROL*
Laptop
Theft
Impersonation
Malicious software
Malfunction
Privilege abuse
Unattended device
Weak passwords
Loss of ID credential
Outdated software
Improper maintenance
Incompatible software
Accumulation of access rights
A.11.2.8 - Unattended user equipment
A.11.1.3 – Securing offices, rooms, and facilities
A.8.1.3 – Acceptable use of assets
A.9.3.1 - Use of secret authentication information
A16.1.5 Response to information security incidents
A.12.2.1 - Controls against malware
A.12.5.1 – Installation of software on operational systems
A.11.2.4 – Equipment maintenance
A.12.6.2 - Restrictions on software installation
A.9.2.6 - Removal or adjustment of access rights
A.7.3.1 - Termination or change of employment responsibilities

- ➢ Hardware Security Risks:

1. Computers with conventional BIOS

2. Computers with PBA (Preboot authentication) or TPM (TrustedPlatform Module)
3. Routers that run on outdated hardware
4. Drives that don't encrypt or decrypt automatically

➢ Software Security Risks:

1. Unpatched and outdated Operating systems
2. Unpatched or outdated office automation and productivity suite ie MS office
3. Unpatched web browser
4. Legacy custom applications
5. Out of date plug-ins
6. Old Mobile OS

16.Old IoT device

➢ List of Places to identify Risks

- Annual Budgets
- Project Schedule
- Scope or requirement changes Technical
- Issues
- Hardware Contracts
- Business Rick
- Legal Risk
- Environment Risk

➢ Tools and Techniques to identify Risk

- Documentation Review
- Assumption Analysis
- Information gathering checklists techniques (brainstorming, Delphi technique, interviewing, strength and weakness analysis, nominal group technique).

17.Probability of occurrence

- Theft: The theft of devices is very likely. Especially when the Company is a bicycle and equipment company, this is easy for those who want to steal. Tools such as keyboards, computers, mice, hard drives, ... when not strictly controlled are also things that thieves can target.
- Disaster: Natural disasters are what most companies in the world care about, which is unintended so can have great consequences. Therefore, the company needs to have predetermined situations so that its employees have the skills to handle in the event of a natural disaster.

18.Computer Misuse Act (1990)

- Protect computer users against attacks and theft of information.
- Offenses under the act include:
  - Hacking,
  - Unauthorized access to computer systems
  - Purposefully spreading malicious and damaging software (malware), such as viruses

19. **ISO 31000 standards:**
   - The purpose of ISO 31000 is to provide risk management principles and generic guidelines. 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.
   - Guidelines for risk administration include: Planning, implementing, measure, learn.
20. **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.
   - Types of physical protection can include, for example, biometrics, swipe cards, fraud prevention (Cameras).

Explain data protection processes and regulations as applicable to an organisation.

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

1. **Definition data protection.**
   - Data protection is the process of safeguarding important information from corruption, compromise or loss.
   - The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime that can make it impossible to access important information.

- Consequently, a large part of a data protection strategy is ensuring that data can be restored quickly after any corruption or loss. Protecting data from compromise and ensuring data privacy are other key components of data protection.

2. **Principles of data protection.**

- The key principles of data protection are to safeguard and make available data under all circumstances. The term data protection is used to describe both the operational backup of data and business continuity/disaster recovery (BC/DR). Data protection strategies are evolving along two lines: data availability and data management.
- Data availability ensures users have the data they need to conduct business even if the data is damaged or lost.
- There are two key areas of data management used in data protection: data lifecycle management and information lifecycle management. Data lifecycle management is the process of automating the movement of critical data to online and offline storage. Information lifecycle management is a comprehensive strategy for valuing, cataloging and protecting information assets from application and user errors, malware and virus attacks, machine failure or facility outages and disruptions.
- Data management has come to include finding ways to unlock business value from otherwise dormant copies of data for reporting, test/dev enablement, analytics and other purposes.
- Accurate and where necessary, kept up to date. Where Personal Data is inaccurate with regards to the purpose for which it is processed, every reasonable step must be taken to either erase or rectified it without delay.
- Not kept longer than necessary for the purpose for which the Personal Data is processed.
- Processed in a manner that ensures appropriate security of the Data Subject, including protection against unauthorised Processing and accidental loss, destruction or damage.
- Not transferred to people or organisations situated in countries without adequate protection without putting in place appropriate safeguards.

3. **What is the purpose of data protection?**

- Storage technologies that can be used to protect data include a disk or tape backup that copies designated information to a disk-based storage array or a tape cartridge device so it can be safely stored. Mirroring can be used to create an exact replica of a website or files so they're available from more than one place. Storage snapshots can automatically generate a set of pointers to information stored on tape or disk, enabling faster data recovery, while continuous data protection (CDP) backs up all the data in an enterprise whenever a change is made.

4. **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 earthquakes
   - 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.
5. **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...
6. **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.

7. 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:

  - Perform system/network verification and validation to certify all systems are operational.
  - 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.
  - 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 the 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. The ability of an organization to maintain essential functions during, as well as after, a disaster has occurred.

8. Hardware and software

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

9. 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.

10.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.

11.Computer Misuse Act (1990)

- Protect users of computers from threats and identity stealing.
- Under the act, offenses include:
    - Hacking,
    - Unauthorized access to computer systems
    - Purposefully spreading malicious and damaging software (malware), such as viruses.

12.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.

13.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.
- Types of physical protection can include, for example, biometrics, swipe cards, theft prevention (Cameras).

Design and implement a security policy for an organisation.

Information Technology Security Policy

- Introduction
- Definitions
- Rationale
- Core Principles
- Equality Analysis
- Implementation, Monitoring and Review

1. 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.

2. What is a Network Security Policy?

- IT security policies are the set of rules and practices that an organization uses to manage and protect its network infrastructure. These policies must be defined, documented, implemented, reviewed and evaluated to ensure network security. Hence, the need for network security policies in any organization cannot be overlooked. It determines how policies are enforced and how to lay out some of the basic architecture of the company security/ network security environment.
- Network security policies interpret, explain, and communicate the organization's position on security as stated in advanced security principles. It is a "living document" that notifies administrators, staff, managers, and other users of their required obligations for safeguarding technology and information assets. The phrase "living document" suggests that the document is never-ending and constantly modified with employee requirements and technological changes. Therefore, a proper network security policy:

- Stipulates the rules for required behavior
- Defends users and information
- Describes the penalties of violations
- Permits the workforce to observe, probe, and investigate network security threats

3. Types of network security policies?

- Program Policies
  - To address the objectives of network security within the organization to ensure confidentiality and service availability. The policy should Comply with existing laws, regulations, and state and federal policies by supporting organization's mission statement and organizational structure.
- System-specific policies
  - To address system related issues at all levels of security from access control rules to permissions among group of employees.
- Issue-specific polices
  - Address particular security issues such as, Internet access, installation of unauthorized software or equipment, and sending/receiving e-mail and attachments. Once the issues you need to address are identified, issue specific policies are developed.

4. Basic rules for developing security policies

- ✓ Explain the purpose and what security goals it will address
- ✓ Define what IT resources are covered like hardware, software, data and group of professionals
- ✓ Defining Roles & Responsibilities
- ✓ Establish the support from top management to enforce the policies
- ✓ Defining the relationship between the department for identification, implementation, budgeting and analysis.
- ✓ Cover the legal, compliance and regulatory aspects to facilitate approval
- ✓ Also establish any disciplinary process for breaches of the program policy

5. 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.

6. 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.

7. Core Principles

- In this respect, the college shall comply with a number of rules, 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 provisions of the Data Privacy Act, in order to safeguard its legal enterprise and integrity, the College maintains the freedom to control any user's use of its systems.

- In order to help the university ensure the security of its infrastructure, suitable internal and external systems may be employed.
- Due thought and consideration will be given to information security risks prior to implementation of new systems.

8. Equality Analysis

- Schools are expected, under the Equity Act 2010, 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.

9. Implementation, Monitoring and Review

a. 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.

➢ 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.

➢ 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 that 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.

b. **Remote Services**

- The school acknowledges that because of the essence of distribution, remote access to systems is possible and even appropriate for the learner's experience. 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.
- Email, Virtual Learning Environment (Moodle), One Class, Extranet and the Box are currently offered on the college website. It is possible to access other networks using a Virtual Private Network Connection. Until they are provided with VPN control, users are expected to get permission from the line manager and sign a contract.
- Where security information is required in order to access a remote system encryption must be implemented. E-Services 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).

c. **Anti-Virus**

- The deliberate introduction of malicious software to a system is a criminal offense under the Computer Misuse Act 1990.
- E-Services will seek to minimize network contamination by remaining proactively up-to-date with applicable anti-virus 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.

d. 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 guidelines 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.

e. 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 the 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.

f. 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 the 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.

g. Protection of data from unauthorized access

- Staff account password 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 the provision of accurate course details is essential.
- System password details are recorded by E-Services and kept securely.
- To prevent others from 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.

h. 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.

i. Software Control

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

j. Quality Assurance and Review

- All staff is 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.
- 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

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

- You can't stop the unthinkable from happening. IT has global standards for disaster recovery: "Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery, and restoration are put in place," is how the ISO/IEC standard reads.
- Each good recovery plan for a disaster starts with understanding what you have, where you have it, start your inventory by assessing physical space. Server rooms, network operation centers, a data center anywhere IT equipment is stored.
- Start with your main racks, and work outward.
    - Physical servers
    - Network gateways, routers, and switches
    - NAS and shared storage
    - Power supply equipment
- Move on to your endpoints, and go room by room
    - Access points, secondary Ethernet switches
    - Workstations, desktop PCs, monitors, laptops
    - VoIP and phones
    - Printers and peripherals
- When you go to check each room, you must carefully examine the important equipment that is directly related to the school's information materials.

➢ **Rank systems by importance to running the business**

- Identify your critical systems and rate them in order of importance. For example, if you are school equipment, you need to check the data center first because it contains a lot of student information. Systems for inventory and logistics, safety, and security will be of equivalent performance. Environmental and sanitation systems are critical as well.

- If a downed system shuts down a business, or worse, produces more chaos in the absence of proper functioning, the goal is to produce a solution as quickly as possible, and this is the essence of a formal IT disaster recovery plan.
- Before disaster strikes, you should know:
  1. What you need to restore your systems
  2. How long it will take
  3. Who performs each task
- Define the Response Strategy and Recovery Strategy
- Now that you've identified your critical systems, and assigned costs and prioritization, it's time to solve for potential threats using a response strategy

Critical System	Threat	Response Strategy	Response Workflow
E-School website	Server failure	Switch to Backup Server, validate power source	Verify failure Verify backups are present Test backup server Initiate switchover

- You'll want to have response strategies for every critical system.
  - If your security cameras stop functioning, the response strategy might be to call in extra security personnel.
  - If your power goes out, the response strategy might be to check that uninterruptible power source equipment and backup generators have engaged, call the electric company, and base further decisions according to the severity of the outage, allocate power to high priority systems.

Critical System	Threat	Response Strategy	Response Workflow
E-School website	Server failure	Deploy backups onto secondary hardware. Transfer production to that site.	Obtain backups from remote location/cloud provider. Restore/test SQL Server, Exchange Server, SharePoint Server.

- **Understand the role of each employee**
  - If disaster strikes, confusion takes precedence. The quicker you get processes back up and running, the more prepared you are. If time is literally money pace is important. Even with a small staff, one of the best things you can do is assign every point of your Response & Recovery workflow to one specific team member.

  - Most organisations have disaster recovery plans that suit IT within the overall plan. There IT could be required to account for its own properties and to organize its responsibilities and activities as they apply to the whole of the business. Ensure IT has adequate staff resources to restore infrastructure in a timely manner.
  - Make sure that whoever controls IT procurement is aware of the timelines for purchasing and logistics. If you need to purchase computer hardware to restore your systems this should be done with the utmost urgency.

- **Rehearse and update every time systems and personnel change**
  - Organize many fire drills for school or company employees.
  - Organize many security contests about the school or company system to prevent hackers from entering important systems.
  - Additionally, always test any backup systems regularly.

References

Charles, P.P., 2006. Security in computing.

Rausand, M., 2013. *Risk assessment: theory, methods, and applications* (Vol. 115). John Wiley & Sons.

Baloch, R., 2017. *Ethical hacking and penetration testing guide*. CRC Press.

Team, I.G.P., 2020. *EU General Data Protection Regulation (GDPR)–An implementation and compliance guide*. IT Governance Ltd.

Smith, M.E. and Smith, M.E.S., 2004. *Europe's foreign and security policy: the institutionalization of cooperation*. Cambridge University Press.