ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date	23/05/2021	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	PHAM CAO NGUYEN	**Student ID**	GCC18074
Class	GCC0803	**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	CAONGUYEN

Grading grid

P5	P6	P7	P8	M3	M4	M5	D2	D3

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			

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		
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.	**D2** Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.
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

Introduction [1]

As the Internet's popularity grows, more businesses are opening up their information systems to their partners and suppliers. As a result, it's critical to understand which of the company's tools ought to be safeguarded, as well as to manage device access and user privileges in the information system. The same is true when it comes to gaining Internet access to your business.

Security is the most indispensable thing to a business. Small companies, on the whole, seem to overlook defense. Since they believed their business was not at risk of failure or attacks. However, this way of thinking puts the organization at risk, and it can be avoided. Wheelie Good was hired by a security firm to conduct an audit and develop a security strategy for their business.

Is it necessary for all users to have equal access to the data and functionality offered by your applications? Is there a subset of users that want privileged functions? Is it true that certain records are only accessible to those types of users? Answers to questions like this will help you provide the foundation for your application's security specifications. (Fischer, Edward Halibozek, M.B.A, Walters, 2012)

Discuss risk assessment procedures.

1. **What is risk in security? [2]**

   A security risk is something that may cause information or asset breach, destruction, unavailability, or injury, as well as harm to people. The effect of uncertainty on targets is known as a security risk, and it is often calculated in terms of its probability and implications. And we need to recognize the kind of danger we're working with in order to realize what we're up against. (Amoore, 2013)

2. **What is risk identification? [3]**

   The first phase in the risk management process is risk analysis, which works on determining the root of risk and future incidents that may have an effect on an organization's goals. Risk identification also provides insight into the interaction between risk and threat. (Carr, Konda, Monarch, Ulrich, Walker, 1993)

   Nevertheless, a basic approach has evolved over time that all risk identification methodologies tend to follow:

   Identify your assets.
   In order to determine your cyber risk exposure, you need to first decide what your assets are. This is not as easy as it may seem: you can't protect everything, so you need to identify the assets that must be protected, and their priorities. A series of questions can help to clarify the situation:

   - What kind of data do you store in your organization?
   - Whose data is it? Yours? Or from somebody else?
   - What would be the consequences if something happened to this data?

That last question leads us into the fundamental triangle of cybersecurity: Confidentiality, Integrity, and Availability.

The CIA triangle guides you in asking these fundamental security-related questions about your data assets:

- What would happen if the data were revealed or became public (confidentiality)?
- What would happen if the data were incorrect or falsified (integrity)?
- What would happen if the data could no longer be accessed (availability)?

Some examples:
You're a credit card firm, and the customers' credit card numbers and PIN codes have been stolen and leaked (confidentiality);

You are a bank, and a hacker adds a zero to the amounts in bank transfers (integrity);

You are a hospital, and a ransomware attack makes it impossible to access your medical records (availability).

The CIA triangle will help you define the things you need to secure by letting you know what sort of harm they could do if they are compromised. But compromised by whom? Or is that anything else? This brings us to the next subject.

3. Identify the threats to those assets. [4]

Threat analysis involves the identification of potential sources of harm to the assets (information, data) that you need to protect.

The planet is full of dangers, and the line between what distinguishes relevant "cyber hazards" and other types of dangers will still be blurry. While hacking is obviously a cyber challenge, natural disasters such as floods and fire can still put the data at risk. You'll have to determine whether or not they're important to your case.

Business-related threats constitute an even grayer area regarding their relevance to cybersecurity. Equipment failure like broken disks could threaten your data. An emerging source of much preoccupation is supply-chain security: can you be confident that your vendors aren't sending ransomware to you, either deliberately or unintentionally? Insider attacks, such as those posed by dissatisfied or idealistic workers (or former employees) who steal or publish the info, are becoming an increasing source of concern.

Some of these types of threats may not always seem related to cybersecurity, but the connection can be subtle. As always, experience is the key to recognizing threats and correctly prioritizing them.

And if the risks are clearly linked to cybersecurity, you'll need to fine-tune the threat detection. Hacking by a remote malicious user, for example, is clearly a cybersecurity threat. So what kind of

hacking are we talking about? A "denial of service" attack will prevent the data from being accessed (making it unavailable). A malware assault will do the same thing (and make you pay in the process). A malware attack could install a program that reads your typing and steals your personal data. Professional analysts' expertise is important for good recognition in this case as well. (Moteff, 2005)

4. **Identify your vulnerabilities to those threats. [5]**

Once threats have been identified, your next task is to identify weaknesses in your overall cybersecurity environment that could make you vulnerable to those threats.

It may not always be simple to identify weaknesses and their sources and remedies. For example, how might you be vulnerable to insider threats? Certainly, by firing or losing an employee who was in charge of sensitive data. But you might also be vulnerable because of insufficient employee cybersecurity awareness: perhaps your employees innocently choose weak passwords (recall that this is how the famous Enigma code was broken in World War II) or are not sufficiently aware of the dangers of opening attachments to electronic mail messages. (Pfleeger, Pfleeger, 2012)

5. **What is risk assessment? [6]**

Risk assessment is the process of identifying and evaluating risks for assets that could be affected by cyber-attacks. Basically, you identify both internal and external threats, evaluate their potential impact on things like data availability, confidentiality, and integrity, and estimate the costs of suffering a cyber-security incident. With this information, you can tailor your cyber-security and data protection controls to match your organization's actual level of risk tolerance. After you have identified the risks, the next thing you need to do is assess them.

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 on 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. (Rausand, 2013)

6. **What does a risk assessment include? [7]**

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. (Faustman, Omenn, 2008)

7. 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.

8. The purpose of risk assessment. [8]

The goal of the risk assessment process is to evaluate hazards, then remove that hazard or minimize the level of its risk by adding control measures, as necessary, to create a safer and healthier workplace.

The Risk Equation

We can understand risk using the following equation:

Risk = Threat x Vulnerability x Asset

Although the risk is represented here as a mathematical formula, it is not about numbers. It's a rational structure. As an example, suppose you want to determine the possibility of hackers breaching a specific device. Your danger is high if your network is really weak (perhaps because you don't have a firewall or antivirus solution) and the asset is important. However, if you have good perimeter defenses and your vulnerability is low, and even though the asset is still critical, your risk will be medium

This isn't a statistical formula in the strictest sense. It's a blueprint for deciphering the connections between the factors that go into deciding risk:

The threat is short for "threat frequency," or how often an adverse event is expected to occur.

Vulnerability is shorthand for "the likelihood that a vulnerability will be exploited and a threat will succeed against an organization's defenses." What is the organization's security climate like? When a breach occurs, how easily can catastrophe be mitigated?

Cost is a measure of the total financial impact of a security incident. It includes hard costs, like damage to hardware, and soft costs, such as lost business and consumer confidence.

Other costs can include:

Data loss: Theft of trade secrets could cause you to lose business to your competitors. Theft of customer information could result in loss of trust and customer attrition.

System or application downtime: If a system fails to perform its primary function, customers may be unable to place orders, employees may be unable to do their jobs or communicate, and so on.

Legal consequences: And if the data stolen from one of your databases isn't especially useful, you might face penalties and other court expenses if you don't follow the data privacy enforcement provisions of HIPAA, PCI DSS, or other regulatory standards.

9. **Risk Assessment procedure: [9]**

Step 1: Identify and Prioritize Assets:

Assets include servers, client contact information, sensitive partner documents, trade secrets, and so on. Remember, what you as a technician think is valuable might not be what is actually most valuable for the business. Therefore, you need to work with business users and management to create a list of all valuable assets. For each asset, gather the following information, as applicable:

- Software and Hardware
- Data
- Users and Interfaces
- Mission or purpose
- Criticality
- Functional requirements
- IT security policies
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security environment
- Environmental security

Because most organizations have a limited budget for risk assessment, you will likely have to limit the scope of the remaining steps to mission-critical assets. Accordingly, you need to define a standard for determining the importance of each asset. Common criteria include the asset's monetary value, legal standing, and importance to the organization. Once the standard has been approved by management and formally incorporated into the risk assessment security policy, use it to classify each asset as critical, major, or minor.

Step 2: Identify Threats.

A threat is anything that could cause harm to your organization. Although hackers and ransomware come to mind first, there are a variety of other risks to consider:

Natural disasters: floods, hurricanes, earthquakes, fire, and other natural disasters can destroy not just data, but servers and appliances as well. When deciding where to house your servers, think about the chances of different types of natural disasters. For instance, your area might have a high risk of floods but a low likelihood of tornadoes.

Hardware failure: The likelihood of hardware failure depends on the quality and age of the server or other machine. For relatively new, high-quality equipment, the chance of failure is low. But if the equipment is old or from a "no-name" vendor, the chance of failure is much higher.

Malicious behavior: There are three types of malicious behavior.

- Interference is when somebody causes damage to your business by deleting data, engineering a distributed denial of service (DDOS) against your website, physically stealing a computer or server, and so on.
- Interception is theft of your data.
- Impersonation is a misuse of someone else's credentials, which are often acquired through social engineering attacks or brute-force attacks, or purchased on the dark web.

This threat should be on your list, no matter what business you are in. Accidentally deleting sensitive data or important files, clicking on a malicious connection in an email, or spilling coffee on machinery that hosts vital systems are all possibilities.

Step 3: Identify Vulnerabilities

A vulnerability is a weakness that could enable a threat to harm your organization. Vulnerabilities can be identified through analysis, audit reports, the NIST vulnerability database, vendor data, information security test and evaluation (ST&E) procedures, penetration testing, and automated vulnerability scanning tools.

Don't limit your thinking to software vulnerabilities. there are also physical and human vulnerabilities. For example, having your server room in the basement increases your vulnerability

to the threat of flooding, and failure to educate your employees about the danger of clicking on email links increases your vulnerability to the threat of malware.

Step 4: Analyze Controls.

Analyze the safeguards in place or in the planning stages to reduce or remove the likelihood of a danger exploiting a weakness. Encryption, intrusion prevention systems, and recognition and authentication solutions are examples of technical controls. Security procedures, executive decisions, and physical and environmental processes are examples of non-technical controls.

Both technical and non-technical controls can further be classified as preventive or detective. Preventive controls aim to detect and deter threats, as the name suggests. Encryption and authentication systems are two examples. Threats that have arisen or are in the pipeline are discovered using detective controls. Audit trails and intrusion prevention devices are among them.

Step 5: Determine the Likelihood of an Incident.

Assess the likelihood of a weakness being abused, taking into account the type of vulnerability, the threat source's capabilities and motivation, and the presence and efficacy of the controls. Often organizations use the ratings high, medium, and low to measure the risk of an attack or other adverse occurrence rather than a numerical ranking.

Step 6: Assess the Impact a Threat Could Have.

Analyze the impact that an incident would have on the asset that is lost or damaged, including the following factors:

- The mission of the asset and any processes that depend upon it.
- The value of the asset to the organization.
- The sensitivity of the asset.

To get this information, start with a business impact analysis (BIA) or mission impact analysis report. This document uses either quantitative or qualitative means to determine the impact of harm to the organization’s information assets, such as loss of confidentiality, integrity, and availability. The impact on the system can be qualitatively assessed as high, medium, or low.

Step 7: Prioritize the Information Security Risks.

Determine the level of risk to the IT system for each hazard and vulnerability pair using the following criteria:

- The likelihood that the threat will exploit the vulnerability.
- The approximate cost of each of these occurrences.
- The adequacy of the existing or planned information system security controls for eliminating or reducing the risk.

A useful tool for estimating risk in this manner is the risk-level matrix. A high likelihood that the threat will occur is given a value of 1.0. a medium likelihood is assigned a value of 0.5. and a low likelihood of occurrence is given a rating of 0.1. Similarly, a high impact level is assigned a value of 100, a medium impact level of 50, and a low impact level of 10. Risk is calculated by multiplying the threat likelihood value by the impact value, and the risks are categorized as high, medium, or low based on the result.

Step 8: Recommend Controls.

Determine the steps required to minimize the danger using the risk level as a guide. Here are some general guidelines for each level of risk:

High: A plan for corrective measures should be developed as soon as possible.

Medium: A plan for corrective measures should be developed within a reasonable period of time.

Low: The team must decide whether to accept the risk or implement corrective actions.

- As you evaluate controls to mitigate each risk, be sure to consider:
- Organizational policies
- Cost-benefit analysis
- Operational impact
- Feasibility
- Applicable regulations
- The overall effectiveness of the recommended controls
- Safety and reliability

Step 9: Document the Results.

- The final step in the risk assessment process is to develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures, and so on. For each threat, the report should describe the corresponding vulnerabilities, the assets at risk, the impact on your IT infrastructure, the likelihood of occurrence, and the control recommendations. Here's an example for a risk assessment matrix:
- As you work through this process, you will get a better idea of how the company and its infrastructure operates and how it can operate better. Then you can create a risk assessment policy that defines what the organization must do periodically (annually in many cases), how risk is to be addressed and mitigated (for example, a minimum acceptable vulnerability window), and how the organization must carry out subsequent enterprise risk assessments for its IT infrastructure components and other assets.

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
System failure — Overheating in server room High	Air-conditioning systems is ten years old. High	Servers Critical	All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost.
Malicious human (interference) — DDOS attack. High	Firewall is configured properly and has good DDOS mitigation. Low	Website Critical	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years.	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall.
Natural disasters — Flooding High	Server room is on the 3rd floor. Low	Servers. Critical	All services will be unavailable. Critical	Low Last flood in the area happened 10 years ago.	Low	No action needed.
Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup. Low	Medium	Low	Continue monitoring permissions changes, privileged users and backups.

10. How to use a risk assessment matrix. [10]

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. (Ristić, 2013)

11. 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 complete risk analysis.

12. Hardware and software.

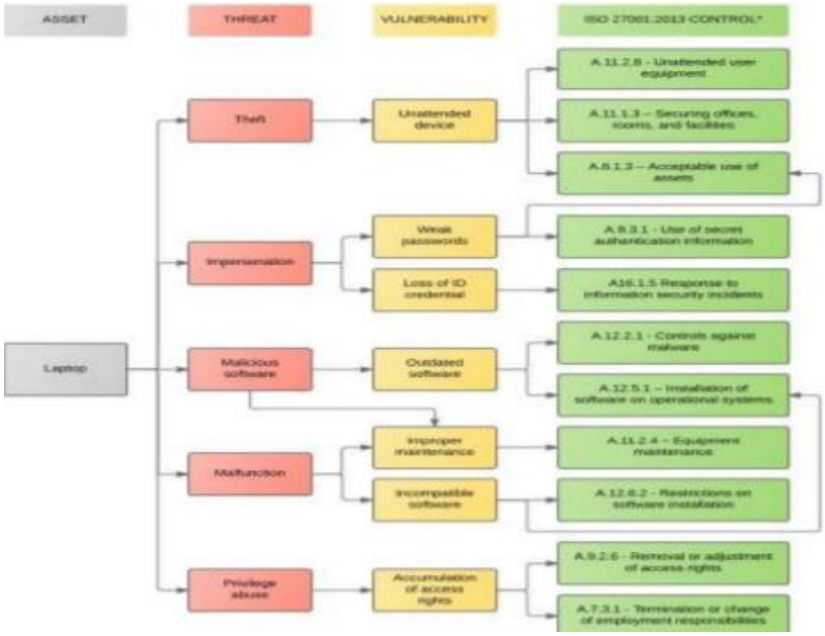
The risk may be considered as a potential opportunity that could be eventually exploited resulting in undesired consequences or negative impact on the operations.

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 suites are not so effective and come with multiple ways in which they could be exploited.

Risk symptoms are known as triggers.



- **Hardware Security Risks:**

  Computers with conventional BIOS

  Computers with PBA (Preboot authentication) or TPM (TrustedPlatform Module)

  Routers that run on outdated hardware

  Drives that don’t encrypt or decrypt automatically

- **Software Security Risks:**

  Unpatched and outdated Operating systems

  Unpatched or outdated office automation and productivity suite ie MS office

  Unpatched web browser

  Legacy custom applications

Out of date plug-ins

Old Mobile OS

Explain data protection processes and regulations as applicable to an organisation. [11]

What is data protection?

General Data Protection Regulation (GDPR) focuses on the protection of "personal data", defined as:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Data security is achieved by a mix of administrative and technological safeguards. Legal concerns (privacy policies, terms and conditions, etc.) are included in administrative measures.

One of the most important aspects of GDPR is the legal basis for processing a subject's data. In many cases, the basis will be "informed consent", which can be withdrawn at any time. However, there are several other legal bases, some of which may well apply in a healthcare context.

The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also minimal tolerance for downtime, which might prevent crucial information from being accessed.

Data protection should always be applied to all forms of data, whether it be personal or corporate. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it is accessible to only those that have access privilege to it.

The context of data protection varies and the methods and extent also vary for each; there is data protection for individuals, businesses, and public institutions, as well as data that is so highly classified that it should never enter into the hands of anyone other than its owners, or top-secret data, or in other words, top secret.

In the United States, for example, data privacy is not strictly controlled, therefore there are no stringent data protection laws in place, however, this is rapidly changing as people become more conscious of the need for privacy and data protection. However, in the United Kingdom, the legislative body approved the Data Protection Act of 1998, which was a reform of the 1984 Act, which set forth standards for data users and established individuals' rights in relation to data that is directly connected to them. The Act became effective on March 1, 2000. The law itself strives to

balance the individual rights to privacy and the ability of more public organizations to use this data in the process of conducting business. In the interest of protection, the Act establishes standards, or eight principles, that a data controller must follow while managing personal data in the course of business. These principles include having been gained honestly and legitimately, as well as not leaving the nation or territory unless specific safeguards are in place. However, data protection rules may not exist in every country. (Bygrave, 2002)

Purpose.

The Data Protection Act contains a set of principles that organizations, government, and businesses have to adhere to in order to keep someone's data accurate, safe, secure, and lawful. These principles ensure data is: Only used in specifically stated ways. Not stored for longer than necessary. (Bygrave, 2002)

Scope.

In its broadest sense, it applies to:

The processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which forms part of a filling system. Why are data protection and regulations so important?

Why are data protection and regulations so important?

The goal of personal data protection is to safeguard not just a person's data, but also the basic rights and freedoms of others who are affected by it. Whilst protecting personal data it is possible to ensure that persons' rights and freedoms aren't being violated. For example, incorrect processing of personal data, might bring about a situation where a person is overlooked for a job opportunity or, even worse, loses their current job.

Not complying with the personal data protection regulations can lead to even harsher situations, such as the theft of all funds from a person's bank account or even the creation of a life-threatening scenario by tampering with health information.

Data protection regulations are necessary for ensuring and fair and consumer-friendly commerce and the provision of services. Personal data protection legislation creates a system in which personal data, for example, personal data can't be sold freely which means that people have greater control over who makes them offers and what kind of offers they make.

If personal data is leaked, it can cause companies significant damage to their reputation and also bring along penalties, which is why it's important to comply with the personal data protection regulations.

To protect the security of personal data, it's critical to understand what data is being processed, why it's being handled, and why it's being processed on what grounds. It's also crucial to figure out what

safety and security measures are in place. All of this is achievable thanks to a complete data protection audit, which determines data flow and compliance with data protection standards. The audit can be completed by answering a set of questions that have been designed specifically for that purpose. The results will give a clear overview of the procedures and possible data leaks, which can then be stopped. (Bygrave, 2002)

Regulations Definitions

In this policy the following terms have the following meanings:

consent means any freely given, specific, informed, and unambiguous indication of an individual's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of persona data relating to him or her.

data controller means an individual or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

data processor means an individual or organization which processes personal data on behalf of the data controller.

personal data means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

processing means any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

sensitive personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,

biometric data, data concerning health, an individual's sex life or sexual orientation, and an individual's criminal convictions.

Supervisory authority means an independent public authority that is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

filling system refers to personal data that is organized, presumably for ease of access and use, and could include anything from an alphabetized set of papers in a cabinet through to an enormous, searchable database. A number of papers in a box in a back room are unlikely to qualify, although emails in an inbox will.

Data Processing under The Data Processing Laws.

The Company processes personal data in relation to its own staff, work-seekers, and individual client contacts and is a data controller for the purposes of the Data Protection Laws.

- The Company may hold personal data on individuals for the following purposes:
- Staff administration.
- Advertising, marketing, and public Accounts and records.
- Administration and processing of work-seekers personal data for the purposes of providing work-finding services, including processing using software solution providers and back-office support
- Administration and processing of clients' personal data for the purposes of supplying/introducing work-seekers.

1. **The data protection principles.**

The Data Protection Laws require the Company acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is:

Processed lawfully, fairly, and in a transparent manner.

Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Accurate and kept up to date. every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Kept for no longer than is necessary for the purposes for which the personal data are processed.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures. and that

The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Legal bases for processing.

Personal data will only be processed by the Company if it has a legal basis to do so. Any processing of personal data by the Company without a legal cause would be a violation of the Data Protection Laws.

The Company will assess the personal data it possesses on a regular basis to verify that it is being handled lawfully and that it is correct, relevant, and up to date, and those specified in the Appendix will be in charge of doing so.

The Company will show that it has a legal purpose for sending personal data to any third party (such as previous, current, or potential employees, suppliers, customers, and clients, intermediaries such as umbrella companies, anyone filing an inquiry or complaint, and any other third party (such as software solutions providers and back-office support) before doing so.

3. Privacy by design and by default.

The Company has put in place methods and processes to guarantee that individual privacy is appropriately protected and that data protection is included in all processing operations. Implementation measures include things like:

Data Minimization:

Under Article 5 of the GDPR, principle (c) advises that data should be limited to what is necessary, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes, and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimization enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes:

Electronic collection (i.e. forms, website, surveys, etc) only have the fields that are relevant to the purpose of collection and subsequent processing

Physical collection (i.e. face-to-face, telephone, etc) is only that which is relevant and necessary

Where we have SLA's and bespoke agreements in place with third-party controllers who send us personal information only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out

Forms, contact pages, and any documents used to collect personal information are reviewed every 6-months to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

Rights of the individual.

Any information on data processing that the Company provides to a person must be in a succinct, transparent, comprehensible, and easily available manner, using clear and simple language. The information must be delivered in writing or by other methods, including, where applicable, electronic means. If the individual requests it, the Company may disclose this information orally.

Privacy notices.

Where the Company collects personal data from the individual, the Company will give the individual a privacy notice at the time when it first obtains the personal data.

Where the Company collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month. If the Company intends to disclose the personal data to a third party then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner).

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

Subject access requests.

The individual is entitled to access their personal data on request from the data controller.

Rectification.

The individual, or another data controller acting on their behalf, has the right to request that the Company correct any erroneous or incomplete personal data on them.

If the Company has supplied the personal data to any third parties, the Company will inform such third parties that a request to correct the personal data has been received, unless doing so is impracticable or requires excessive effort. Those third parties should likewise correct the

personal data they retain; however, the Company will not be able to audit those third parties to guarantee that this has happened.

Erasure.

The individual or another data controller at the individual's request has the right to ask the Company to erase an individual's personal data.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however, the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

If the Company has made the data public, it must take reasonable efforts to notify other data controllers and data processors that the personal data has been made public, taking into account available technology and implementation costs.

If the Company receives a request to erase, it will ask the individual whether he or she wants his or her personal data completely erased or if he or she is okay with his or her information being maintained on a list of people who don't want to be contacted in the future (for a specified period or otherwise). The Company is unable to preserve a record of individuals whose data it has deleted in order to contact them again if the Company comes into possession of the individual's personal data at a later period.

Restriction of processing.

The individual or a data controller at the individual's request, has the right to ask the Company to restrict its processing of an individual's personal data where:

- The individual challenges the accuracy of the personal data.
- The processing is unlawful and the individual opposes its erasure.
- The Company no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise, or defense of legal claims. or
- The individual has objected to the processing (on the grounds of public interest or legitimate interest) pending the verification of whether the legitimate grounds of the Company override those of the individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however, the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

Data portability.

Individuals have the right to receive personal data about themselves that they have supplied to the Company in a structured, frequently used, and machine-readable format, as well as the right to transmit such data to another data controller in the following circumstances:

- The processing is based on the individual's consent or a contract
- The processing is carried out by automated means.

Object to processing

Individuals have the right to object to their personal data being processed in the public interest or in the pursuit of a legitimate interest. Individuals will be entitled to object to their data being profiled for reasons of public interest or genuine interest.

The Company must stop processing personal data unless it has compelling legitimate grounds to do so that outweigh the individual's interests, rights, and freedoms, or unless it is necessary for the establishment, exercise, or defense of legal claims.

The individual has the right to object to their personal data for direct marketing.

Enforcement of rights.

Any subject access request, as well as requests for correction, deletion, limitation, data portability or objection, automated decision-making processes, or profiling, must be responded to within one month of receipt. If required, the Company may extend this period for another two months, depending on the complexity and quantity of requests.

If the Company believes a request under this section is plainly baseless or disproportionate because of its recurring character, the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

Automated decision making.

The Company will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the data controller and the individual.
- Is authorized by law.
- The individual has given their explicit consent.

Reporting personal data breaches.

All data breaches should be referred to the persons whose details are listed in the Appendix.

Personal data breaches where the Company is the data controller:

Where the Company establishes that a personal data breach has taken place, the Company will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the personal data breach happens outside the UK, the Company shall alert the relevant supervisory authority for data breaches in the affected jurisdiction.

Personal data breaches where the Company is the data processor:

The Company will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach.

Communicating personal data breaches to individuals:

Where the Company has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the personal data breach where:

- The Company has implemented appropriate technical and organizational protection measures to the personal data affected by the breach, in particular, to make the personal data unintelligible to any person who is not authorized to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialize.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

If you have a complaint or suggestion about the Company's handling of personal data then please contact the person whose details are listed in the Appendix to this policy.

The lawfulness of processing conditions for personal data are:

- Consent of the individual for one or more specific purposes.
- Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
- Processing is necessary for compliance with a legal obligation that the controller is subject to.
- Processing is necessary to protect the vital interests of the individual or another person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- Processing is essential for the controller's or a third party's legitimate interests unless those interests are outweighed by the individual's interests or basic rights or freedoms that need personal data protection, particularly if the subject is a minor.

The lawfulness of processing conditions for sensitive personal data are:

Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.

Processing is required to fulfill the data controller's duties under employment, social security, or social protection law, or a collective bargaining agreement that includes suitable protections for an individual's basic rights and interests.

Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.

In the course of its legitimate activities, the processing is carried out with appropriate safeguards by a foundation, association, or any other not-for-profit body, with a political, philosophical, religious, or trade union aim and on condition that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.

Processing relates to personal data which are manifestly made public by the individual.

Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Processing is required for reasons of substantial public interest under EU or Member State legislation, which must be proportionate to the goal sought, respect the essence of the right to data privacy, and allow for appropriate and particular safeguards to protect the individual's fundamental rights and interests.

Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.

Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.

Processing is required for public interest archiving, scientific or historical research, or statistical reasons, which must be proportionate to the goal sought, respect the core of the right

to data privacy, and include appropriate and specific safeguards to protect the individual's fundamental rights and interests.

Design and implement a security policy for an organisation.

1. **What is Security Policy? [12]**

   A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.

   A security policy must identify all of a company's assets as well as all the potential threats to those assets. Employees must be kept informed of the company's compliance procedures. The policies themselves should be updated regularly as well. (Höne, Eloff, 2002)

   A security policy contains pre-approved organizational procedures that tell you exactly what you need to do in order to prevent security problems and the next steps if you are ever faced with a data breach. Security problems can include:

   - **Confidentiality** - people obtaining or disclosing information inappropriately
   - **Data Integrity** - information being altered or erroneously validated, whether deliberate or accidental
   - **Availability** - information not being available when it is required or being available to more users than is appropriate
   - At the very least, having a security policy will ensure everyone in the IT department is on the same page on security processes and procedures.

2. **The importance of security policies. [13]**

   IT protection measures are intended to counter security risks and enforce techniques to minimize the security flaws, as well as to specify how to recover from a network attack. Employees are often given instructions for what they can and should not do as a result of the policies. It should also have an exception system in place to accommodate requirements and urgencies that arise from different parts of the organization. (Brück, 2007)

3. **Security Policy Circle. [16]**

Figure: Security policy cycle.

Identifying threats is the first step in the security strategy period. Risk assessment is the process of determining the threats that an organization's information assets pose. This data serves as the foundation for creating a security strategy.

The next step is designing a security policy in the cycle.

After the risks are identified, the company must determine which ones need the most attention so that a security strategy can be developed to address them.

The final step is compliance monitoring and evaluation. Some of the most valuable analysis occurs when an attack can get through the security defenses.

A team must be able to react quickly to the original attack and reexamine security measures to decide whether modifications are needed to discourage the attack from happening again. (Hardee, Feranil, Boezwinkle, Clark, 2004)

4. Common elements of Security Policy.

Due care.

Due care is using reasonable care to protect the interests of an organization. For example, due care is developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures.

Separation of duties

Separation of duties (SoD) is a key concept of internal controls and is the most difficult and sometimes the most costly one to achieve. This objective is achieved by disseminating the tasks and associated privileges for a specific security process among multiple people. This ensures that one person's job acts as a supplement to another's, and no more than one person can have full control of any operation from start to finish.

- **Need to know**

One of the most effective ways to keep documents private is to limit who has access to it. Access is granted only to those employees whose job functions depend on learning the details.

5. Security Policy frameworks. [14]

A security policy can be as broad as you want it to be from everything related to IT security and the security of related physical assets, but enforceable in its full scope. The following list offers some important considerations when developing an information security policy. (Friedman, 2011)

- **Purpose**

  First state the purpose of the policy which may be to:

  - Create an overall approach to information security.
  - Detect and preempt information security breaches such as misuse of networks, data, applications, and computer systems.
  - Maintain the reputation of the organization, and uphold ethical and legal responsibilities.
  - Respect customer rights, including how to react to inquiries and complaints about non-compliance.

- **Audience**

Define the audience to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit that manages security separately may not be in the scope of the policy. (Friedman, 2011)

- **Information security objectives**

Guide your management team to agree on well-defined objectives for strategy and security. The three core goals of information management are:

- **Confidentiality** - only individuals with authorization can should access data and information assets
- **Integrity** - data should be intact, accurate, and complete, and IT systems must be kept operational
- **Availability** - users should be able to access information or systems when needed

- **Authority and access control policy**

Hierarchical pattern - A senior manager would be able to determine what data should be exchanged and with whom. A senior manager's security policy can vary from that of a junior employee. Each organizational role's level of authority over data and IT structures should be specified in the regulation.

Network security policy - Users can only reach business networks and servers using one-of-a-kind logins that require authentication, such as passwords, biometrics, ID cards, or tokens. You should keep an eye on all processes and keep track of all login attempts.

- **Data classification**

Data can be classified into groups such as "top secret," "secret," "confidential," and "public," according to the regulation. When it comes to data classification, the goal is to:

- To ensure that sensitive data cannot be accessed by individuals with lower clearance levels.
- To protect highly important data, and avoid needless security measures for unimportant data.

- **Data support and operations**

Data protection regulations - systems that store personal data, or other sensitive data, must be protected according to organizational standards, best practices, industry compliance standards, and relevant regulations. Encryption, a firewall, and anti-malware defenses are all required by most security requirements.

Data backup - encrypt data backup according to industry best practices. Back up to secure cloud storage or securely archive backup media.

Movement of data - only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

- **Security awareness and behavior**

Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification. (Brück, 2007)

- **Social engineering** - place a special emphasis on the dangers of social engineering attacks (such as phishing emails). Make employees responsible for noticing, preventing and reporting such attacks.
- **Clean desk policy** - secure laptops with a cable lock. Shred documents that are no longer needed. Keep printer areas clean so documents do not fall into the wrong hands.
- **Acceptable Internet usage policy** - define how the Internet should be restricted. Do you allow YouTube, social media websites, etc.? Block unwanted websites using a proxy.

- **Responsibilities, rights, and duties of personnel**

Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy. (Brück, 2007)

6. Basic steps for designing security policies: [15]

To secure your network, there are three phases that your organization must go through preparation, prevention, and response. Network security policies begin with risk assessment, followed by the implementation of a security management practice, and lastly, an analysis or a review to modify the existing policies. (Johnson, Easttom, 2020)

- **Identify your risks**

The use of screening or reporting software is a helpful way to classify your threats. Many firewall and Internet protection vendors provide free trial periods for their devices. If those products provide reporting information, it can be helpful to use these evaluation periods to assess your risks. However, make sure that your workers are mindful that you will be monitoring their activities for risk management purposes.

- **Learn from others**

Since there are so many different kinds of compliance strategies, it's crucial to look at what other companies like yours are doing. Often, speaking with sales representatives from different security product vendors. They are still willing to share details.

- **Make sure the policy conforms to legal requirements**

You may be expected to adhere to certain minimum requirements to protect the safety and confidentiality of your data, depending on your data holdings, authority, and location, particularly if your organization keeps personal information. One way to mitigate any risks you might face in the case of a security breach is to have a viable security program recorded and in effect.

- **The level of security is equal the level of risk**

Too much protection can be almost as bad as not having enough. Since you have a mature, committed team, you can find that, aside from keeping the bad guys out, you have no issues with proper use. Excessive protection can make it difficult to run a company smoothly, so be careful not to overprotect yourself.

- **Include staff in policy development**

No one needs a regime that is imposed from on high. Staff should be included in the process of determining acceptable use. Keep the employees updated as the rules and tools are created. People would be far more willing to cooperate once they recognize the importance of a responsible security strategy.

- **Train your employees**

Staff training is commonly overlooked or underappreciated as part of the implementation process. But, in practice, it's probably one of the most useful phases. It not only helps you to inform employees and help them understand the policies, but it also allows you to discuss the practical, real-world implications of the policy.

- **Get it in writing**

Make sure every member of your staff has read, signed and understood the policy. All new hires should sign the policy when they are brought on board and should be required to reread and reconfirm their understanding of the policy at least annually. For large organizations, use automated tools to help electronically deliver and track signatures of the documents. Some tools even provide quizzing mechanisms to test user's knowledge of the policy.

- **Set clear penalties and enforce them**

Network security is no joke. Your protection policy is a requirement of work, not a series of optional rules. Establish a simple series of protocols that lay out the consequences of violating the security policy. Then put them in place. A security protocol that is followed haphazardly is about as terrible as having no policy at all.

- **Update your staff**

A security policy is a dynamic document because the network itself is always evolving. People come and go. Databases are generated and discarded on a regular basis. New security risks emerge on a regular basis. It's tough enough to keep the security policies up to date, but keeping employees informed of any updates that could impact their day-to-day activities is much more difficult.

- **Install the tools you need**

It's one thing to have a policy; it's another to enforce it. Content protection products for the internet and e-mail with personalized rule sets will guarantee that the protocol, no matter how complicated, is followed.

7. Scope

An information security policy should address all data, programs, systems, facilities, other tech infrastructure, users of technology, and third parties in a given organization, without exception.

This policy applies to all users of computing resources owned or managed by Wheelie good. Individuals covered by the policy include (but are not limited to) Wheelie faculty and visiting faculty, staff, guests or agents of the administration, external individuals, and organizations accessing network services via Wheelie's computing facilities.

Computing resources include all company-owned, licensed, or managed hardware and software, and the use of the company network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies extend to infrastructure managed by individual departments, resources managed by central administrative departments (such as the Wheelie office and Computing and Information Services), privately owned computers and devices linked to the campus network via wired or wireless, and off-campus computers using Wheelie's network services remotely.

8. Responsibilities

As a member of the Wheelie community, the company provides you with the use of work-related tools, including access to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a company employee or a manager), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the company that apply to appropriate use of the Wheelie's technologies and resources. You are responsible for exercising good judgment in the use of the company's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

9. Conclusion

Authorization and access control policy is the most important element and must have while create policy

Because it relates directly with data hierarchy inside organization, by that organization can be clear which information a particular company position can access.

10. Policies.

a. Acceptable Use Policy (AUP)

You may use only the computers, computer accounts, and computer files for which you have authorization.

You may not use another individual's account, or attempt to capture or guess other users' passwords.

You should make a reasonable effort to keep your passwords safe and secure your resources from unwanted access or use. You must set hardware and software in such a way that unauthorized users are unable to gain access to the company's network and computer resources.

Without the permission of the system owner or administrator, you must not attempt to access restricted sections of the network, an operating system, security software, or other administrative applications.

You may not use corporate computing and/or network resources to run programs, software, processes, or automated transaction-based commands that are designed to disturb (or may reasonably be expected to disrupt) other computer or network users, or to damage or impair the performance, software, or hardware components of a system.

b. Human Resource Policy.

Management should ensure that all employees and contractors are aware of and fulfill their information security responsibilities.

All employees will receive security awareness education and training when first employed and at least annually thereafter, in addition to any specific training associated with job responsibilities and employee roles.

Employee disciplinary processes will include applicable provisions to cover any egregious violations of approved information security policies or requirements.

Termination of employment: access to company information resources, work areas, and processing facilities will be revoked, and assets returned upon full termination of employment with company.

c. Password Management Policy.

All passwords must meet the following guidelines, except where technically infeasible:

- Must contain at least eight alphanumeric characters.
- Must contain at least two non-alphabetic characters and least three alphabetic characters.
- At least one alphabetic character must be upper-case and at least one must be lower-case.
- Passwords cannot consist of a single word in any dictionary, language, slang, dialect, jargon, etc.
- Passwords cannot consist of easily guessed or obtained personal information, names of family members, pets, etc.

Personal or economically useful information, such as credit card numbers, should never be used as a user ID or password to help avoid identity theft.

Email messages and other kinds of electronic communication should not contain passwords.

The same password should not be used for access needs external to company.

It is recommended that passwords be changed at least every six months.

Passwords should not be shared with anyone, including administrative assistants or IT administrators.

If a password is suspected of being compromised, it should be changed immediately and the incident

Reported to the company.

Password cracking or guessing may be performed on a periodic or random basis by IT Security or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the owner of the password must replace it right away.

For administrator password: failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days.

Administrators should review these logs on a regular basis, and any anomalies, such as suspected attacks, should be reported.

d. Privacy Policy

When using computing systems to communicate with others, be professional and respectful; utilizing computing resources to libel, slander, or harass another person is not permitted and may result in business discipline as well as legal action by those who are the target of such actions.

Everyone who uses the company's network and computing resources is expected to respect other people's privacy and personal rights.

Personal data may be required if you use our services, and the information needed may vary with the services. When you are asked to contribute personal information, we will inform you of the conditions, restrictions, and purposes of the collection. Your personal information will only be used and disclosed for the purposes for which it was gathered.

All company's administrators shall take appropriate measures to ensure the confidentiality and storing of the data until its usage or storage term come to an end, when the data shall be destroyed or sealed in accordance to what was previously stipulated.

Wheelie uses the collected data for various purposes:

- To provide and maintain the Service.
- To notify you about changes to our Service.
- To allow you to participate in interactive features of our Service when you choose to do so.
- To provide customer care and support.

- To provide analysis or valuable information so that we can improve the Service.
- To monitor the usage of the Service.
- To detect, prevent and address technical issues.

e. Disposal and Destruction Policy.

Physical Print Media shall be disposed of by one (or a combination) of the following methods:

- **Shredding** - Media shall be shredded using issued cross-cut shredders.
- **Shredding Bins** - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor.
- **Incineration** – Materials are physically destroyed using licensed and bonded information disposal contractor.

In particular, it is the company's policy to ensure that all sensitive information which requires disposal is disposed of securely.

When data is stored on IT equipment, the company's policy is that such equipment is assumed to contain sensitive data and that all data stored on such equipment must be securely disposed of.

Copyright: software must be disposed of in line with copyright legislation and software licensing provisions.

The record may be retained for a further period if it has on-going business value or if there is specific legislation which requires it to be held for a further period.

A record should not ordinarily be retained for more than 30 years in aggregate from the date of creation.

f. Service-Level Agreement Policy (SLA).

Customer should provide all essential information and help on service performance so that the company can meet the performance requirements set in the contract.

Customer shall inform company regarding changing business requirements that may necessitate a review, modification, or amendment of the SLA.

The company will act as primary support provider of the services herein identified except when thirdparty vendors are employed who shall assume appropriate service support responsibilities accordingly.

The company will inform customer regarding scheduled and unscheduled service outages due to maintenance, troubleshooting, disruptions or as otherwise necessary.

g. Incidence Response Policy

The IT department detects and investigates security events to determine whether an incident has occurred, and the extent, cause and damage of incidents.

The IT department directs the recovery, containment and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The IT department coordinates response with external parties when existing agreements place responsibility for incident investigations on the external party.

Information Security Administrators are responsible for unit procedures to train users to recognize and report information security incidents.

The IT department is responsible for responding to High Severity incidents according to procedures established in the company Response Plan.

h. Ethics Policy

Wheelie business, whether domestic or international, must be conducted in compliance with all applicable laws and regulations. Be aware of the legal requirements that apply to your job, and follow those laws strictly. Our company will not tolerate illegal activity conducted for personal gain or on the Company's behalf.

Lack of knowledge of the law will not excuse your non-compliance with this Ethics Policy.

Consider company's reputation and credibility in all your business relationships. Be honest and honorable in all dealings with other employees, the public, the business community, shareholders, customers, suppliers, competitors, and government authorities.

Never accept a gift, entertainment, or other benefit from a person or organization doing business with our company if the gift, entertainment, or benefit could influence your decisions or appear to have impacted your business decision if it were made public. Any present, entertainment, or perk you give a business associate should be small in scale and value. Never give a gift, entertainment, or benefit that violates any applicable law or contract term, or is large enough to sway, or appear to sway, the recipient's business decisions. Ensure that you record (in company's accounts) all expenditures on gifts, entertainment, and other benefits.

The company does not want to dissuade employees from participating in political and related activities. However, you may not make political contributions on behalf of the firm, either directly or indirectly, without the prior written approval of Company's Executive Management.

All reports or other information received regarding alleged violations of this Ethics Policy will be investigated by the Executive Management Team, and the outcomes of material violation investigations will be reported to the Board of Directors.

Anyone found to have broken this Ethics Policy or any associated corporate policy shall face disciplinary action under the company's employee discipline policy, which includes appropriate disciplinary measures for employee misbehavior, up to and including dismissal.

i. Database Credentials Coding Policy.

To maintain the security of company's internal databases, access by software programs must be granted only after authentication with credentials.

The credentials used for this authentication must not reside in the main, executing body of the program.

Database credentials must not be stored in a location that can be accessed through a web server.

Database credentials may not reside in the documents tree of a web server.

Passwords or pass phrases used to access a database must adhere to the Password Management Policy.

Every program must have unique database credentials. Sharing of credentials between programs is not allowed.

Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Management Policy.

j. Acceptable Encryption Policy.

It is strongly recommended to use the Advanced Encryption Standard (AES) for symmetric encryption.

It is strongly recommended to use the RSA (Rivest–Shamir–Adleman) and Elliptic Curve Cryptography (ECC) algorithms for asymmetric encryption.

In general, our company adheres to the NIST (National Institute of Standards and Technology) Policy on Hash Functions.

Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH) Key exchanges must be used.

End points must be authenticated before exchanging the key or derivation of session keys.

Public keys used to establish trust must be authenticated prior to use.

All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

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

1. What is Business Continuity? [17]

Business continuity is an organization's ability to ensure operations and core business functions are not severely impacted by a disaster or unplanned incident that takes critical systems offline. Business continuity planning is the interdepartmental process, often led by information technology, of implementing the tactics used to restore normal business in a set amount of time, define the amount of data loss acceptable to the business, and communicate critical information to organizational stakeholders during and following incidents. (Hiles, 2010)

2. Policies and procedures that are required for business continuity.

Key components of business continuity policy include staffing, metrics, and standard requirements. Internal staffing in a business continuity policy should outline the roles and responsibilities of department heads, corporate management liaisons, and members of the Business Continuity (BC) or Disaster Recovery (DR) team.

Why must an organization define policies for an organization’s business continuity and disaster recovery plans? It is to ensure that the organization is able to efficiently recover from a disaster and resume normal business operations as quickly as possible.

3. Scope of the policies

This Policy is applied to all employees and officers hired under the fixed-term employment contracts, top managers, and members, as well as to all contractors, consultants, distributors, resellers and other representatives acting on behalf of the organization. The policy complies with international and national documents regulating business continuity.

4. Objectives of Business Continuity System

Prevention, identification and elimination of existing and future threats to the organization’s business.

Proactive approach to minimize impact of incidents.

Effective actions taken in the event of business interruption.

Minimization of the periods and consequences of downtimes during incidents.

Reduction of the recovery time.

Preservation of customer and supplier loyalty through demonstration of business sustainability verified by the business continuity system.

5. Type of events that business continuity planning guard against

A variety of events cause digital business disruptions. Just because you're not at risk of one particular cataclysmic disaster doesn't mean many other incidents can't take you offline:

Disasters: Natural and Local

Data loss and system failure can obviously be caused by natural disasters such as floods, earthquakes and fires, but even a simple electronic malfunction could destroy valuable information. When it comes to data, putting all your eggs in one basket is a perilous risk.

Network Disruptions

Third-party internet networks can fail. Fiber can get cut. Your in-house local area network can be disabled. If your business needs continuous connectivity, make sure network availability is a top priority.

Cybersecurity

The prevalence of cyber-security threats is a global phenomenon that no business, large or small, can ignore. New threats such as Ransomware are predicted to be on the rise. Backing up your data with high frequency is crucial to ensuring such attacks don't bring your business down plan against a data breaches is paramount.

Human error

Vulnerability points are often located right in the cubicle next to you. Employees or vendors can cause outages simply out of ignorance, due to innocent mistakes, or even as a result of ill intent.

As organizations rely more on technology and electronic data for their daily operations, the amount of data and information technology infrastructure lost to disasters appears to be increasing. Organizations are estimated to lose revenue and incur expenses every year due to disasters, unpreparedness, and lost productivity. Measures must be taken to protect your organization from disasters. (Hiles, 2010)

6. The main components of an organizational disaster recovery plan

One way your organization can prepare and protect itself from disasters is to create and implement a disaster recovery plan (DRP). Organizations should create a disaster recovery plan that can address any type of disaster. The plan should be easy to follow and understand and be customized to meet the unique needs of the organization. Typical elements in a disaster recovery plan include the following:

6.1. The scope of your plan.

There are multiple types of crises that could affect organizations and multiple dimensions of an organization that need to be protected, so as simple as it seems, the first part of your disaster recovery

plan should define what scope it covers. Ideally, it should cover what to do in the event of a cyber attack and in the event of a natural disaster.

6.2. Identify and assess disaster risks.

Your disaster recovery team should identify and assess the risks to your organization. This step should include items related to natural disasters, man-made emergencies, and technology-related incidents. This will assist the team in identifying the recovery strategies and resources required to recover from disasters within a predetermined and acceptable time frame.

6.3. Determine critical applications, documents, and resources.

The organization must evaluate its business processes to determine which are critical to the operations of the organization. The plan should focus on short-term survivability, such as generating cash flows and revenues, rather than on a long-term solution of restoring the organization's full functioning capacity. However, the organization must recognize that there are some processes that should not be delayed if possible. One example of a critical process is the processing of payroll.

6.4. Specify backup and off-site storage procedures.

These procedures should identify what to back up, by whom, how to perform the backup, the location of the backup, and how frequently backups should occur. All critical applications, equipment, and documents should be backed up. Documents that you should consider backing up are the latest financial statements, tax returns, a current list of employees and their contact information, inventory records, customer and vendor listings. Critical supplies required for daily operations, such as checks and purchase orders, as well as a copy of the DRP, should be stored at an off-site location.

6.5. A communication plan

If disaster strikes, the last thing you might want to do is address your customers, employees or other stakeholders, but effective communication is key to showing you are in control of the situation and that it will be resolved. Effective communication doesn't just mean communicating everything as soon as possible, but knowing the necessary chain of communication and reporting accurate information. This is why it's important to outline a thorough communication plan that covers these elements.

This plan should include contact lists of those who will need to be communicated to (internally and externally), a protocol for what information can be communicated, and how it should be conveyed, depending on the situation. For example, the communication following a natural disaster will be different from the communication following a data breach, and your plan needs to account for those variations.

6.6. Test and maintain the DRP.

Since the threats of disasters and emergencies are constantly evolving, disaster recovery preparation is a continuous process. The company should test the DRP on a regular basis to ensure that the procedures

recorded in the plan are accurate and acceptable. The recovery team should update the DRP on a regular basis to account for changes in business processes, technology, and disaster risks.

7. Steps needed for recovery planning

Step 1: Set Clear Recovery Objectives

The primary motive to develop a successful disaster recovery plan is to reduce downtime and the cost of data loss. Set RTO (Recovery Time Objective) and RPO (Recovery Point Objective) goals to help you create the best data recovery plan possible. These parameters assist you in determining how quickly you need to recover the data.

An RTO determines the operational downtime within which the system should have its full recovery. An RPO evaluates the maximum limit for manageable data loss that won't lead to a catastrophic impact on business.

Step 2: Identify Involved Professionals

There should be a clear identification of all the included personnel, including internal and external members. The DRP should have written details about how to reach each member and when to contact them. It should also cover their assigned responsibilities in detail.

Also, having a pre-approved budget for resources (recovery tools and services) will help ease the flow and build a successful disaster recovery plan.

Step 3: Draft a Detailed Documentation on Network Infrastructure.

The data recovery process will be aided by a step-by-step guide on network configurations. The proper reconstruction and recovery of the entire system are ensured by a comprehensive blueprint of the existing network infrastructure. The detailed documentation increases the chances of successful reconstruction of corrupted network infrastructure.

It's advisable to keep all the documents offline and in a private cloud. Either way, the document should be easy for all personnel to access.

Step 4: Choose Your Data Recovery Technique

There are many types of data recovery solutions, such as hard drive recovery, RAID recovery, tape recovery, optical recovery, and more. Selecting the right one for your organization is critical. To choose one of these solutions, consider the requirements of the organizations – on-premise, outsourced, or cloud-based DRaaS (Disaster recovery as a service).

Each data recovery approach has its own set of features, which can make it expensive or affordable. Storage space, recovery timetable, and configuration complexity are all factors that influence the cost of recovery solutions.

Step 5: Explicitly Define an Incident Criteria Checklist

Every organization faces temporary outages, but these incidents cannot be used to initiate a disaster recovery procedure. No organization would carry out a recovery procedure for a temporary electricity outage, but if it is due to a natural disaster, then the incident needs to be taken into consideration.

Creating an all-inclusive checklist for identifying a disaster will help the recovery team to execute DRP as quickly as possible.

This checklist will differ for every organization, depending on their goals and budget for data recovery. Even the decision to strictly follow this checklist or not is entirely upon organizations.

Step 6: Document Your Entire Disaster Recovery Procedure

After successful identification of a disaster recovery incident, a recorded collection of protocols can be used to carry out the disaster recovery plan. The DRP should adhere to the RTO and RPO standards that have already been developed. For maximum DRP productivity, both automated and manual processes in the plan should be neatly reported.

It’s important that at the end of the disaster recovery procedure, all the recovered data should be in an operational state.

Step 7: Regularly Test Your DRP

If you don’t test your DRP on a regular basis, it can become obsolete. A thoroughly tested plan is reliable and has a higher chance of giving effective results. All of the included steps in a working DRP should be reviewed on a regular basis.

The entire disaster recovery team should participate in these tests. Simulating data loss and cyberattacks in real-time helps the team remain prepared for the unexpected.

Step 8: Keep Updating Your Recovery Plan

With the growth of the company, the DRP needs to be updated. If you test your DRP on a regular basis, there’s a good chance you'll discover any flaws in your current strategy. Continue to fix these bugs so that the latest updates are in line with the company's needs. Maintain a log for each shift in DRP as well.

As the staff shifts, the list of involved members should change as well. As soon as possible, new members should be trained and assigned responsibilities. This move will aid in the evolution of your DRP over time.

References

[1] Fischer, R., Edward Halibozek, M.B.A. and Walters, D., 2012. *Introduction to security*. Butterworth-Heinemann.

[2] Amoore, L., 2013. *The politics of possibility: Risk and security beyond probability*. Duke University Press.

[3] Carr, M.J., Konda, S.L., Monarch, I., Ulrich, F.C. and Walker, C.F., 1993. *Taxonomy-based risk identification*. carnegie-mellon univ pittsburgh pa software engineering inst.

[4] Moteff, J., 2005, February. Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences. Library of Congress Washington DC Congressional Research Service.

[5] Pfleeger, C.P. and Pfleeger, S.L., 2012. *Analyzing computer security: A threat/vulnerability/countermeasure approach*. Prentice Hall Professional.

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

[7] Faustman, E.M. and Omenn, G.S., 2008. Risk assessment. *Casarett and Doull's toxicology: The basic science of poisons*, pp.107-128.

[8] Landoll, D.J. and Landoll, D., 2005. *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.

[9] Lo, C.C. and Chen, W.J., 2012. A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, *39*(1), pp.247-257.

[10] Ristić, D., 2013. A tool for risk assessment. *safety Engineering*, *3*(7), p.2017.

[11] Bygrave, L.A., 2002. *Data protection law*. Wolters Kluwer Law & Business.

[12] Höne, K. and Eloff, J.H.P., 2002. What makes an effective information security policy?. *Network security*, *2002*(6), pp.14-16.

[13] Brück, T., 2007. *An economic analysis of security policies* (pp. 278-298). Routledge.

[14] Friedman, A., 2011. *Economic and policy frameworks for cybersecurity risks*. Center for Technology Innovation at Brookings.

[15] Johnson, R. and Easttom, C., 2020. *Security policies and implementation issues*. Jones & Bartlett Learning.

[16] Hardee, K., Feranil, I., Boezwinkle, J. and Clark, B., 2004. *The policy circle* (No. 11). London: Policy working paper series.

[17] Hiles, A., 2010. *The definitive handbook of business continuity management*. John Wiley & Sons.