**ASSIGNMENT FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 5: Security** | | |
| **Submission date** | 1/10/2021 | **Date Received 1st submission** |  |
| **Re-submission Date** | 1/21/2021 | **Date Received 2nd submission** |  |
| **Student Name** | Nguyen Dong Anh | **Student ID** | GCC19072 |
| **Class** | [GCC0801-1623](https://cms.greenwich.edu.vn/course/view.php?id=2585) | **Assessor name** | [Lê Huỳnh Quốc Bảo](https://cms.greenwich.edu.vn/user/view.php?id=5515&course=1) |
| **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** | Anh |

**Grading grid**

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

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

|  |
| --- |
| **Submission Format** |
| **Part 1**  The submission is in the form of an individual written report. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs, subsections and illustrations as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system. The recommended word limit is 2,000–2,500 words, although you will not be penalised for exceeding the total word limit.  **Part 2**  The submission is in the form of a policy document (please see details in Part 1 above).  **Part 3**  The submission is in the form of an individual written reflection. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system. The recommended word limit is 250–500 words, although you will not be penalised for exceeding the total word limit. |

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

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO3** Review mechanisms to control organisational IT security | | **D2** Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment. |
| **P5** Discuss risk assessment procedures.  **P6** Explain data protection processes and regulations as applicable to an organisation. | **M3** Summarise the ISO 31000 risk management methodology and its application in IT security.  **M4** Discuss possible impacts to organisational security resulting from an IT security audit. |
| **LO4** Manage organisational security | | **D3** Evaluate the suitability of the tools used in an organisational policy. |
| **P7** Design and implement a security policy for an organisation.  **P8** List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion. | **M5** Discuss the roles of stakeholders in the organisation to implement security audit recommendations. |

**TABLE OF CONTENTS**

[**P5 Discuss risk assessment procedures. 7**](#_Toc15768)

[What is risk in security? 7](#_Toc6153)

[What is risk identification? 7](#_Toc1228)

[Identify the threats to those assets. 8](#_Toc29489)

[Identify your vulnerabilities to those threats. 9](#_Toc20259)

[What is risk assessment? 9](#_Toc13914)

[The purpose of risk assessment 10](#_Toc32321)

[Risk Assessment procedure: 11](#_Toc8664)

[**P6 Explain data protection processes and regulations as applicable to an organization. 15**](#_Toc10594)

[What is data protection? 15](#_Toc20297)

[Purpose 16](#_Toc11698)

[Scope 16](#_Toc20745)

[Why are data protection and regulations  so important?  16](#_Toc24189)

[Data Processing under The Data Processing Laws 18](#_Toc30253)

[**P7 Design and implement a security policy for an organization. 24**](#_Toc15274)

[What is Security Policy? 24](#_Toc8056)

[The importance of security policies 25](#_Toc2412)

[Security Policy Circle 25](#_Toc13548)

[Common elements of Security Policy 26](#_Toc14853)

[Security Policy frameworks 26](#_Toc421)

[Basic steps for designing security policies: 28](#_Toc18057)

[Scope 30](#_Toc13139)

[Responsibilities 31](#_Toc18243)

[Policies 31](#_Toc2744)

[**P8 List the main components of an organizational disaster recovery plan, justifying the reasons for inclusion. 36**](#_Toc28242)

[What is Business Continuity? 36](#_Toc10025)

[Policies and procedures that are required for business continuity 36](#_Toc31887)

[Scope of the policies 36](#_Toc16719)

[Objectives of Business Continuity System 36](#_Toc5670)

[Type of events that business continuity planning guard against 37](#_Toc6290)

[The main components of an organizational disaster recovery plan 37](#_Toc4071)

[Steps needed for recovery planning 39](#_Toc27079)

[**References 41**](#_Toc10621)

#### P5 Discuss risk assessment procedures.

#### What is risk in security?

A security risk is something that could result in the compromise, loss, unavailability or damage to information or assets, or cause harm to people. Security risk is the effect of uncertainty on objectives and is often measured in terms of its likelihood and consequences. And order to know what kind of risk we are dealing with, we need to identify it.

#### What is risk identification?

Risk identification is the first step in the risk assessment process and focuses on identifying the source of risk and potential events that could impact an organization's objectives. Risk identification also provides insight in the interaction between risk and threat.

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 are a credit card company, and the numbers and personal identification codes of your customers are hacked and published (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 helps you to identify the assets you need to protect, by understanding the kind of damage that could occur if they are compromised. But: compromised by whom? Or what? That leads to the next topic.

#### Identify the threats to those assets.

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

The world is full of threats, and the boundaries between what constitute relevant “cyber threats” and other kinds of threats will always be unclear. For example, although hacking is clearly a cyber threat, environmental factors such as flooding and fire could also threaten your data. You will have to decide how relevant they are to your situation.

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 sure that your suppliers are not delivering malware to you, intentionally or otherwise? Insider threats, e.g. from disgruntled or idealistic employees (or former employees) who decide to steal or publish your data constitute another growing cause for 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.

Even when threats are clearly related to cybersecurity, you will need to refine your identification of the threats. For example, hacking by a remote malicious user is obviously a cybersecurity threat. But what kind of hacking? A “denial of service” hack will block access to your data (making it unavailable). A ransomware attack will do the same (and make you pay in the process). A malware attack might install a program to read what you type and steal your confidential information. Here, too, the experience of professional analysts is key to successful identification.

#### Identify your vulnerabilities to those threats.

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.

#### What is risk assessment?

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 (Rausand, 2013) After you have identified the risks, the next thing you need to do is assess it.

To get started with IT security risk assessment, you need to answer three important questions:

* What are your organization’s critical information technology assets — that is, the data whose loss or exposure would have a major impact on your business operations?
* What are the key business processes that utilize or require this information?
* What threats could affect the ability of those business functions to operate?

Once you know what you need to protect, you can begin developing strategies. However, before you spend a dollar of your budget or an hour of your time implementing a solution to reduce risk, be sure to consider which risk you are addressing, how high its priority is, and whether you are approaching it in the most cost-effective way.

#### The purpose of risk assessment

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 created a safer and healthier workplace.

**The Risk Equation**

We can understand risk using the following equation:

**Risk = Threat x Vulnerability x Asset**



Although risk is represented here as a mathematical formula, it is not about numbers. it is a logical construct. For example, suppose you want to assess the risk associated with the threat of hackers compromising a particular system. If your network is very vulnerable (perhaps because you have no firewall and no antivirus solution), and the asset is critical, your risk is high. 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(Rausand, 2013)

This isn’t strictly a mathematical formula. it’s a model for understanding the relationships among the components that feed into determining risk:

**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 security environment in the organization? How quickly can disaster be mitigated if a breach does occur?

**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:** If somebody steals data from one of your databases, even if that data is not particularly valuable, you can incur fines and other legal costs because you failed to comply with the data protection security requirements of HIPAA, PCI DSS or other compliance

#### Risk Assessment procedure:

**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. While hackers and malware probably leap to mind, there are many other types of threats:

**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 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. People can accidentally delete important files, click on a malicious link in an email or spill coffee on a piece of equipment that hosts critical systems.

**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 controls that are either in place or in the planning stage to minimize or eliminate the probability that a threat will exploit a vulnerability. Technical controls include encryption, intrusion detection mechanisms, and identification and authentication solutions. Nontechnical controls include security policies, administrative actions, and physical and environmental mechanisms.

Both technical and nontechnical controls can further be classified as preventive or detective. As the name implies, preventive controls attempt to anticipate and stop attacks. examples include encryption and authentication devices. Detective controls are used to discover threats that have occurred or are in process. they include audit trails and intrusion detection systems.

**Step 5: Determine the Likelihood of an Incident**

Assess the probability that a vulnerability might actually be exploited, taking into account the type of vulnerability, the capability and motivation of the threat source, and the existence and effectiveness of your controls. Rather than a numerical score, many organizations use the categories high, medium and low to assess the likelihood of an attack or other adverse event.

**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**

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

* The likelihood that the threat will exploit the vulnerability.
* The 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 50, and a low impact level 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**

Using the risk level as a basis, determine the actions needed to mitigate the risk. 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.

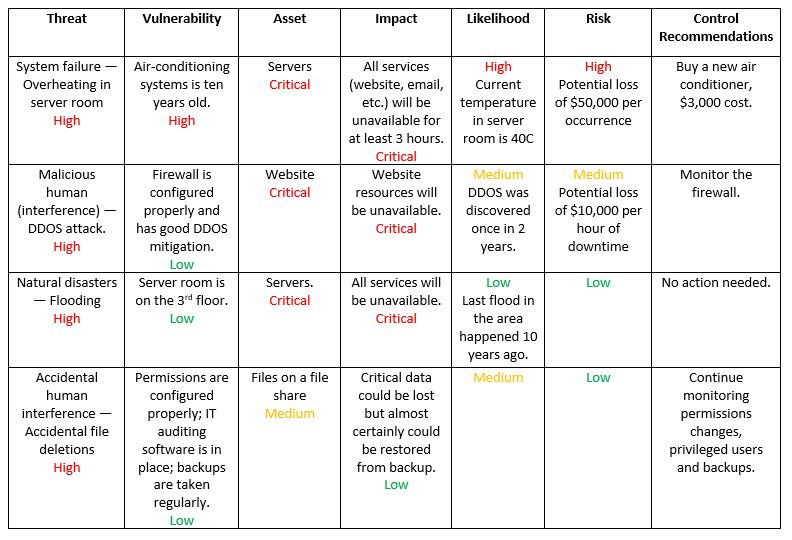
**Low** — The team must decide whether to accept the risk or implement corrective actions.

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 to 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 (Rausand, 2013)

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

#### What is data protection?

General Data Protection Regulation (GDPR) focuses on the protection of [“personal data”](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-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.”

Achieving data protection takes a combination of administrative and technical measures. Administrative measures include legal aspects (privacy policies, terms and conditions, …)

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 little tolerance for downtime that can make it impossible to access important information (Voigt, 2017)

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 being accessible to only those that have access privilege to it (Voigt, 2017)

The context of data protection varies and the methods and extent also vary for each; there is data protection on the personal level, that of business or public entities, and that of data so highly classified that it should never fall into the hands of others aside from its owners, or in other words, top secret.

For example, in the United States data privacy is not highly regulated, so by extension there are no strict data protection laws that apply, although that is quickly changing as people become aware of the value of privacy and data protection. In the United Kingdom however, the legislative body passed the Data Protection Act of 1998, a revision of the very basic Act of 1984 which stated rules for data users and defined individuals' rights in regard to data that is directly related 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. The Act gives guidelines, eight principles, which a data controller must observe when handling personal data in the course of doing business, in the name of protection. These principles go along the lines of having being obtained fairly and lawfully, to it not leaving the country or territory unless under certain conditions of protection. Not all countries have data protection laws, however.

#### 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.

#### 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?](https://www.fsb.org.uk/resources-page/why-is-data-protection-so-important.html)

The purpose of personal data protection isn’t to just protect person’s data, but to protect the fundamental rights and freedoms of persons that are related to that data. 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 current job.

Not complying with the personal data protection regulations can lead to even harsher situations, where it’s possible to extract all the money from a person’s bank account or even cause a life-threatening situation by manipulating health information.

Data protection regulations are necessary for ensuring and fair and consumer friendly commerce and provision of services. Personal data protection regulations cause a situation, where, for example, personal data can’t be sold freely which means that people have a 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 person data protection regulations.

To ensure that personal data is secure, it’s important to know what data is being processed, why it’s being processed and on what grounds. In addition, it’s important to identify which safety and security measures are in use. All of this is possible through a thorough data protection audit, which identifies the data flow and whether the data protection regulations are being followed. The audit can be carried out by answering a set of specific questions that have been prepared for that purpose. The results will give a clear overview of the procedures and possible data leaks, which can then be stopped.

**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 a 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 analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**‘pseudonymisation’** 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 which is responsible for monitoring the application of data protection. In the UK the supervisory authority is [the Information Commissioner’s Office](https://ico.org.uk/) (ICO).

**‘filling system’** refers to personal data that is organized, resumably for ease of access and use, and could include anything from and alphabetized set of papers in a cabinet through to an enormous, searchable database. A number of papers in a box in a back room is 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(Voigt, 2017) These require that personal data is:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. 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.
5. Kept for no longer than is necessary for the purposes for which the personal data are processed.
6. 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
7. The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.
8. **Legal bases for processing**

The Company will only process personal data where it has a legal basis for doing so (see Annex). Where the Company does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.

1. **Privacy by design and by default**

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

**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  
The Company shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual(Voigt, 2017)

1. **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.

1. **Subject access requests**

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

1. **Rectification**

The individual or another data controller at the individual’s request, has the right to ask the Company to rectify any inaccurate or incomplete personal data concerning an 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 rectify 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. [

1. **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 receives a request to erase it will ask the individual if s/he wants his personal data to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise).  The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual’s personal data at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data to erase the personal data, taking into account available technology and the cost of implementation.

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.

1. **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 defence of legal claims. or
* The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification 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.

1. **Data portability**

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller in circumstances where:

* The processing is based on the individual’s consent or a contract. and
* The processing is carried out by automated means.

1. **Object to processing**

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest.

The Company shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual’s interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

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

1. **Enforcement of rights**

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request’s repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

1. **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 authorised 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.

1. **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 effected jurisdiction.

1. **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.

1. **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 authorised 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:**

1. Consent of the individual for one or more specific purposes.
2. 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.
3. Processing is necessary for compliance with a legal obligation that the controller is subject to.
4. Processing is necessary to protect the vital interests of the individual or another person.
5. 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.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

**The lawfulness of processing conditions for sensitive personal data are:**

1. Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.
2. Processing is necessary for carrying out data controller’s obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. 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.
4. In the course of its legitimate activities, 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.
5. Processing relates to personal data which are manifestly made public by the individual.
6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7. Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
8. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee [NOTE 21], 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.
9. 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.
10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

#### P7 Design and implement a security policy for an organization.

#### What is Security Policy?

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. Company employees need to be kept updated on the company's security policies. The policies themselves should be updated regularly as well (Cooper, 2003)

A security policy contains pre-approved organizational procedures that tell you exactly what you need to do in order to prevent security problems and 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

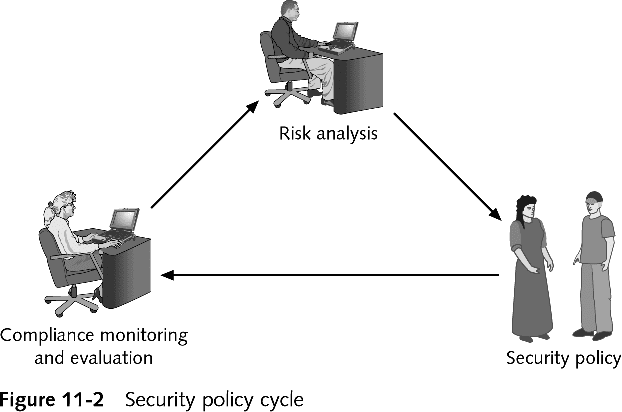
Availability – information not being available when it is required or being available to more users than is appropriate

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.

#### The importance of security policies

The aim of IT security policies is to address security threats and implement strategies to mitigate IT security vulnerabilities, as well as defining how to recover when a network intrusion occurs. Furthermore, the policies provide guidelines to employees on what to do and what not to do. It should also have an exception system in place to accommodate requirements and urgencies that arise from different parts of the organization.

#### Security Policy Circle



First step in security policy cycle is to identify risks. Risk identification seeks to determine the risks that an organization faces against its information assets. That information becomes the basis of developing a security policy.

The next step is designing a security policy in the cycle

After the risks are identified, the organization must decides which risks are needed to be dealt with the msot so that a security policy can be created to mitigate those risks. 

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 respond to the initial attack and reexamine security policies as soon as possible to determine what changes need to be made to prevent the reoccurrence.

#### 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. Which means that one person’s work serves as a complementary check on another person’s, and no more than one person should have complete control over any action from initialization to completion.

#### Need to know

One of the best methods to keep information confidential is to restrict who has access to that information. Only that employee whose job function depends on knowing the information is provided access.

#### Security Policy frameworks

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(Knapp, 2009)

#### 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 which manages security separately may not be in the scope of the policy)(Knapp, 2009)

#### Information security objectives

Guide your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives:

* Confidentiality—only individuals with authorization canshould 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 may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee. The policy should outline the level of authority over data and IT systems for each organizational role.
* Network security policy—users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts.

#### Data classification

The policy should classify data into categories, which may include “top secret”, “secret”, “confidential” and “public”. Your objective in classifying data is:

* 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. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection.
* Data backup—encrypt data backup according to industry best practices. Securely store backup media, or move backup to secure cloud storage.
* Movement of data—only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

1. **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(Knapp, 2009)

* 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.

1. **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(Knapp, 2009)

#### Basic steps for designing security policies:

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 (Flowerday, 2016)

1. **Identify your risks**

A good way to identify your risks can be through the use of monitoring or reporting tools. Many vendors of firewalls and Internet security products allow evaluation periods for their products. If those products provide reporting information, it can be helpful to use these evaluation periods to assess your risks. However, it's important to ensure that your employees are aware that you will be recording their activity for the purposes of risk assessment.

1. **Learn from others**

There are many types of security policies, so it's important to see what other organizations like yours are doing. Also, talk to the sales reps from various security software vendors. They are always happy to give out information.

1. **Make sure the policy conforms to legal requirements**

Depending on your data holdings, jurisdiction and location, you may be required to conform to certain minimum standards to ensure the privacy and integrity of your data, especially if your company holds personal information. Having a viable security policy documented and in place is one way of mitigating any liabilities you might incur in the event of a security breach.

1. **The level of security is equal the level of risk**

Don't be overzealous. Too much security can be as bad as too little. You might find that, apart from keeping the bad guys out, you don't have any problems with appropriate use because you have a mature, dedicated staff. Excessive security can be a hindrance to smooth business operations, so make sure you don't overprotect yourself.

1. **Include staff in policy development**

No one wants a policy dictated from above. Involve staff in the process of defining appropriate use. Keep staff informed as the rules are developed and tools are implemented. If people understand the need for a responsible security policy, they will be much more inclined to comply.

1. **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.

1. **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.

1. **Set clear penalties and enforce them**

Network security is no joke. Your security policy isn't a set of voluntary guidelines but a condition of employment. Have a clear set of procedures in place that spell out the penalties for breaches in the security policy. Then enforce them. A security policy with haphazard compliance is almost as bad as no policy at all.

1. **Update your staff**

A security policy is a dynamic document because the network itself is always evolving. People come and go. Databases are created and destroyed. New security threats pop up. Keeping the security policy updated is hard enough, but keeping staffers aware of any changes that might affect their day-to-day operations is even more difficult.

1. **Install the tools you need**

Having a policy is one thing, enforcing it is another. Internet and e-mail content security products with customizable rule sets can ensure that your policy, no matter how complex, is adhered to.

#### Scope

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 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 apply to technology administered in individual departments, the resources administered by central administrative departments (such as the Wheelie office and Computing and Information Services), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the Wheelie’s network services.

#### 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.

#### Policies

#### 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 protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing company’s network and computing resources.
* You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
* You must not use company computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

#### 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.

#### 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.

* To help prevent identity theft, personal or fiscally useful information such as credit card numbers must never be used as a user ID or a password.
* Passwords should not be inserted into email messages or other forms of electronic communication.
* 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 password owner will be required to change it immediately.
* 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 regularly inspect these logs and any irregularities such as suspected attacks should be reported.

#### Privacy Policy

* All users of the company’s network and computing resources are expected to respect the privacy and personal rights of others.
* Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to company discipline as well as legal action by those who are the recipient of these actions.
* Personal data may be required if you use our services, and the information needed may vary with the services. When required to provide personal information, we will inform you about respective collections conditions, regulations and purposes. We will only use and disclose your personal information for the purpose for which it was collected.
* 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.

#### 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.
* Where information is held on IT equipment, it is the policy of the company that such equipment will be assumed to hold sensitive information and that all information residing on such equipment must be disposed of securely.
* 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.

#### Service-Level Agreement Policy (SLA)

* Customer should provide all necessary information and assistance related to service performance that allows the company to meet the performance standards as outlined in document.
* 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.

#### 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.

#### 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 any other benefit from an individual or organization doing business with our company if that gift, entertainment or benefit could influence your decisions or, if it were made public, might appear to have influenced your business decision. Any gift, entertainment, or benefit you provide to a business associate must be modest in scope and value. Never provide a gift, entertainment or benefit that contravenes any applicable law or contract term or that is large enough to influence, or appear to influence, the recipient’s business decisions. Ensure that you record (in company’s accounts) all expenditures on gifts, entertainment, and other benefits.
* Company does not wish to discourage the participation of employees in political and related activities. However, you may not make political contributions on company’s behalf, either directly or indirectly, without the prior written approval of Company’s Executive Management.
* The Executive Management Team will investigate all reports or other information received regarding alleged violations of this Ethics Policy, and will report to the Board of Directors on the results of investigations of material violations.
* Any person who is found to have violated this Ethics Policy, or any related corporate policy, will be subject to discipline in accordance with company’s policy on employee discipline, which policy provides for appropriate disciplinary measures for employee misconduct, up to and including dismissal.

#### 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.

#### 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.

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

#### What is Business Continuity?

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 take critical systems offline. [Business continuity planning](https://www.inap.com/disaster-recovery-as-a-service/) 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(Cerullo, 2004)

#### 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.

#### 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.

#### 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.

#### 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 are 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 data breach 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(Cerullo, 2004)

#### 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:

**1. The scope of your plan**

There are [multiple types of crises that could affect organisations](https://www.riskware.com.au/risk-management-blog/6-types-of-crises-you-need-a-business-continuity-plan-for) 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 about what to do in the event of a [cyber attack](https://www.riskware.com.au/risk-management-blog/how-to-protect-your-business-from-cyber-threats) and in the event of a natural disaster.

**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.

**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.

**4. Specify backup and off-site storage procedures.**

These procedures should identify what to back up, by whom, how to perform the backup, location of 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.

**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. Test and maintain the DRP.**

Disaster recovery planning is a continual process as risks of disasters and emergencies are always changing. It is recommended that the organization routinely test the DRP to evaluate the procedures documented in the plan for effectiveness and appropriateness. The recovery team should regularly update the DRP to accommodate for changes in business processes, technology, and evolving disaster risks.

#### 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 key objectives with RTO (Recovery Time Objective) and RPO (Recovery Point Objective), so that you can build an optimal data recovery plan. These parameters help you decide how quickly you need to take steps 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 documented information on how and when to contact each member. 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**

A step-by-step guide on network configurations will help with the execution of the data recovery process. A holistic blueprint of the current network infrastructure ensures proper rebuilding and recovery of the entire system. 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](https://blog.eccouncil.org/redefining-cybersecurity-using-the-cloud/) DRaaS (Disaster recovery as a service).

Each data recovery method has its set of capabilities, making it costly or bringing it within your budget. There are a few factors that affect the cost of recovery solutions – storage capacity, recovery timeline, and configuration complexity.

**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 documented set of procedures help in carrying out the disaster recovery strategy. The DRP should be in accordance with the already established RTO and RPO standards. Both automated to manual processes included in the plan should be neatly documented for maximum efficiency of the DRP.

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**

Your DRP can fall flat if not tested regularly. A thoroughly tested plan is reliable and has a higher chance of giving effective results. For a functional DRP, all the included steps should be routinely tested.

The entire disaster recovery team should participate in these tests. Playing real-time scenarios of data loss and cyberattacks helps the team to stay ready for the unexpected event.

**Step 8: Keep Updating Your Recovery Plan**

With the growth of the company, the DRP needs to be updated. If your DRP goes through regular testing, then there are fair chances that you will come across some limitations in your existing plan. Keep eliminating these flaws so that the new changes will be aligned with your company’s requirements. Also, with every change in DRP, maintain a log for the same.

The list of involved members should chance as the staff changes. The new members should be trained and assigned their responsibilities as soon as possible. This step will help your DRP to evolve with time.

#### References

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

Voigt, P. and Von dem Bussche, A., 2017. The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing.

Cooper, G., Shaw, B., Valente, L. and Sherlock, K., Securify Inc, 2003. System and method for security policy. U.S. Patent Application 09/881,147.

Flowerday, S.V. and Tuyikeze, T., 2016. Information security policy development and implementation: The what, how and who. computers & security, 61, pp.169-183.

Cerullo, V. and Cerullo, M.J., 2004. Business continuity planning: a comprehensive approach. Information Systems Management, 21(3), pp.70-78.

Knapp, K.J., Morris Jr, R.F., Marshall, T.E. and Byrd, T.A., 2009. Information security policy: An organizational-level process model. Computers & security, 28(7), pp.493-508.