

Lamis

RISK Assessment

**Risk assessment Plan**

This plan is based on Risk Management

**PRACTICAL APPLICATION ACTIVITY 1**

1. Imagine that you are the Information Security officer of MBI Insurance Company. The company has just embraced the work from home policy due to Covid-19 Where some of the staff members will be working from their homes, using their internet and devices.

Using the knowledge, you have learned and researched, develop a risk assessment plan for the organization stating any assumptions made.

Assess security risks, threats and vulnerabilities to the company and implement appropriate information security protection mechanisms by analyzing requirements following the CIA triad measures.

**STEP 1**: Identify the hazards (threats, vulnerabilities)

**STEP2:** Decide who might be harmed and how (assets, stakeholders)

**STEP3:** Evaluate the Risks and decide on precautions

**STEP4:** Record finding

* + **Start collecting and researching information**
  + **Think creatively.**
  + **Develop the report in Microsoft Word format**
  + **Not more than 2pages**

Step 1: Identifying Threats:

1-Confidentiality Threats :

* Access to confidential information by any unauthorized person
* Intercepted data transfers
* Physical loss of data
* Privileged access of confidential information by employees
* Social engineered methods to gain confidential information
* Unauthorized access to physical records
* Transfer of confidential information to unauthorized third parties
* Compromised machine where attacker is able to access data thought to be secure

2- Avalilability :

* Internet Access absence due to Electricity down or Data limitations.

Step 2: Decide who might be Harmed and How :

* Confidentiality & availability threats can harm The assets [Data , Hardware ,Software ]

**3.0 Stakeholders in Risk Management Plan**

Assets:

**4.0 Risk Identification**

Hardware – I/o devices, communication devices, processors ,All tangible parts of a computer system.

Software- All programs, OS and utilities

Data- which is stored, used, printed, archived update logs and Auditrecords.

People- skilled or mere users.

Documentation- of programs, hardware and software, system

The supplies – paper, ink, media, magnetic tapes

**5.0 Assessing Potential Risk**

Step 3:

Once risks are identified, they are evaluated on a two (2) dimensional matrix using a qualitative rating of the likelihood of the event occurring and the scale of the possible consequences. When risks have been identified, they are analysed by combining the consequences and likelihood to produce a level of risk. This form of evaluation provides a good graphical representation of how serious the risk is or where it lies within a group of risks. The risk analysis provides information critical to determining what risks need to be treated and what risks are accepted.

### Likelihood

|  |  |  |
| --- | --- | --- |
| **Level** | **Descriptor** | **Description** |
| A | Almost certain | Almost certain Expected to occur in most circumstances |
| B | Likely | Will probably occur in most circumstances |
| C | Moderate | Should occur at some time |
| D | Unlikely | Could occur at some time |
| E | Rare | may occur only in exceptional circumstances |
| F | Never | It is not foreseeable that this will occur |

**Consequence**

|  |  |
| --- | --- |
| **Level** | **Descriptor** |
| 1 | Insignificant |
| 2 | Minor |
| 3 | Moderate |
| 4 | Major |

|  |  |
| --- | --- |
|  |  |
| 5 | Catastrophic |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Likelihood** | **Consequences** | | | | |
|  | **1** | **2** | **3** | **4** | **5** |
| **A** | S | S | **H** | **H** | **H** |
| **B** | M | S | S | **H** | **H** |
| **C** | L | M | S | **H** | **H** |
| **D** | L | L | M | S | **H** |
| **E** | L | L | M | S | S |

Legend:

**H** High risk; detailed research and management planning required at senior levels

**S** Significant risk; senior management attention needed

**M** Moderate risk; management responsibility must be specified

**L** Low risk; manage by routine procedures

**Step 4: Risk Register**

Compiled by: Lamis GabAllah Date: 21 /5/2021

Reviewed by: Rhoda Date: 21/5/2021

Function / Activity: Risk Assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Risk – what and**  **how can it happen** | **Consequence** | **Likelihood** | **Existing Controls** | **Consequence**  **Rating** | **Likelihood**  **Rating** | **Level of**  **Risk** | **Risk**  **Priority** |
| Confidentiality | Access to confidential information by any unauthorized person | Leak of Data , Loss of Privacy | Moderate | Encryption , VPN | 5 | D | High | 1 |
| Availability | Internet Access absence due to Electricity down or Data limitations | No Production & unmeet deadlines | Moderate | provide Extra Data Bundles using WiFi to avoid also the internet cut due to electricity outage | 4 | C | High | 1 |

# Appendix 1 TEMPLATE OF RISK REGISTER

Risk Treatment: Compiled by: Date:

Reviewed by: Date:

Function / Activity:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Risk What & how**  **can it happen** | **Consequence** | **Likelihood** | **Existing Controls** | **Consequence**  **Rating** | **Likelihood Rating** | **Level of Risk** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |