**PRACTICAL APPLICATION ACTIVITY 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

# Risk Management Plan for MBI Insurance Company.

A risk management plan is a report that contains details of the organization's risk management procedures.

Working from home is a process that was embraced when the Covid-19 hit the country. This mode of working can greatly affect the organization’s security in terms of customers' credentials, the insurance policies and IT services will deteriorate because of some challenges like data breaches.

**Some Risks, Threats, and Vulnerabilities Which Are Likely to be Experienced**

* Phishing: This is the act of sending malicious links to the employee’s email, once the link is accidentally opened it either releases malware or key logs. This induces the individual to reveal personal information like passwords and credit information which could later be used to access the company’s databases
* Most of the home networks are very insecure thus gives cybercriminals an advantage over them. This way malicious actors nearby can easily spy on the connection and collect confidential information.

In an unmonitored network, attackers can barely be identified

* Social Engineering: With the change of workplace the company is likely to suffer some major loss of data confidentiality with its customers. In a scenario where a cybercriminal can pose one of the company’s employees, he/she can easier call one of the company’s customers and will able to acquire some sensitive information from the customer without his/her knowledge. In this case, the customer will have trusted the caller without actually knowing it’s a cybercriminal posing as one of the insurance company employees.

This is bound to happen because communication between the customer and the company happens on mobile phones instead of highly secure and monitored call centers.

**Appropriate Information Security Protection Mechanisms**

* Use of VPN: Virtual Private Networks gives the employees online privacy while working. They also create anonymity by creating a private network from a public internet connection, this makes working from home much safe since employees' IP addresses will be masked (untraceable).
* Ensuring that the company has firewalls in working devices: This will monitor incoming and outgoing traffic based on certain set security rules. Firewalls prevent malicious programs from entering the device being used and can maintain data from unauthorized personnel
* Training the employees on cybersecurity awareness: The company security team should also make a point of educating the employees on the basic cybersecurity measures they should always be aware of to avoid any human errors.
* Use of encrypted emails: This is the use of private keys to encrypt and decrypt work-related emails to avoid interception. Considering that the company shares lots of sensitive data, the use of private keys and public keys only shared with the company employees creates a digital signature that assures the recipient that the sender is who they claim to be.