**NAME : FANNY VIRTUOUS**

**EMAIL: virtuous.fanny@womentechsters.org**

**SUBJECT: PRACTICAL APPLICATION ACTIVITY 1**

**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**

MBI Insurance Company is an insurance company, an insurance company needs topmost protection of details.

Assuming there are 10 staff members, who work from the office, it is assumed that they are connected to the same internet and most likely have a master device that connects all devices in the same room together.

Working from home will imply staff members connected to different internet , some may connect to a ‘free’ wifi which is often targeted at extracting details from systems.

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

1. Hackers can manipulate VPNs without a view of the whole: Virtual private networks, or VPNs, have become the new lifeline for many businesses, extending encrypted networks to our homes. However, many home networks are already infected with malware or compromised hardware that can be exploited for staging attacks through machines with VPN termini
2. Information can be weaponized: Often times, attackers can paint a decoy link or a decoy landing page. An unattentive user can go ahead and fill insensitive details thinking he is in the right place.
3. **Online work increases cyber security risks:** Without the security protections that office systems afford us – such as firewalls and blacklisted IP addresses – and increased reliance on technology, we are far more vulnerable to cyber-attacks. The most obvious risk is that most of our tasks are conducted online. After all, if something’s on the Internet, then there’s always the possibility of a cyber-criminal compromising it

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

1. MBI Insurance Company - useful data can be exposed to unauthorized individuals
2. The insured - useful data can be exposed to unauthorized individuals
3. The stakeholders – if the system is affected, they get to lose investments from the company.

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

1. Hackers can manipulate VPNs. To solve this, hardware or software providers are ro be contacted to ensure configurations and policies are in order, starting with the VPN, endpoint and identity solutions.
2. Information can be weaponized: Always ensure to click on the right links at all the time
3. **Online work increases cyber security risks:** To protect against this risk, all work where possible should be done on a corporate laptop subject to remote access security controls. It will also gives the IT team oversight of the organisation’s IT infrastructure and allows it to monitor any malicious activity, such as malware and unauthorised logins.