**SIMIYU JOY ABIGAEL – ID.NO: WT/21/120**

**joy.simiyu@womentechsters.org**

**PRACTICAL APPLICATION ACTIVITY 1**

Risk assessment plan for an organization.

1. Identify the hazards (threats, vulnerabilities)

Unencrypted File sharing – this involves companies not encrypting their data and files when it is in transit from a remote location to another through a personal/home network. Most companies ensure that their data is protected within their network which forms a threat or vulnerability of working from home.

Remote access via an insecure home/personal Wi-Fi – Wi-Fi networks of employees who work from home can pose a risk to a company’s data by not being secure or by lacking protective malware that would otherwise be used on the company’s network like firewalls which would aid in monitoring the network traffic and in blocking malicious activity.

Use of personal devices like flash drives for printing/ sharing data/ sending data can cause vulnerability to the security and privacy of company data since employees cannot bring home technology such as printers and desk phones from the office that are set to the company’s network and protection protocols.

Phishing Schemes which involves a person or entity posing as a legitimate source, to trick a victim into providing personal login credentials or data, which is then used to hack into accounts, steal more sensitive information and more.

1. Who might be harmed and how (assets, stakeholders)

Customers /users can lose their information or data through phishing schemes or hackers.

Software developers can be slowed down by threats or attacks that affect a system’s productivity which can also lead to increased cost of development in the handling of vulnerabilities or threats.

Project manager

Business people, investors can be affected by having to deploy more resources for the handling of the risks or hazards. It can also affect the work relationship between the developers, the customers and the investing team.

Employers can be affected by losing their jobs when a breach in the network or data security is traced back to an individual employee who could have unknowingly exposed the company systems to a vulnerability or hack.

1. Evaluate the Risks and decide on precautions.

 Provide cyber security training to the company’s staff on the threats and possible vulnerabilities of working from home and on the most effective way of handling it.

Deploy antivirus software for each work-issued device that is administered to every employee.

Validation of security effectiveness of any and every service provider, supplier and partner which involves ensuring that there are no weaknesses in the supply chain.

Effectively encrypting sensitive data when it's sent over email or phone.

|  |  |
| --- | --- |
| RISK (THREAT, VULNERABILITY & HARZARD) | INFORMATION SECURITY PROTECTION MECHANISMS. |
| Unencrypted File sharing | Provide cyber security training to the company’s staff on the threats and possible vulnerabilities of working from home and on the most effective way of handling it. |
| Remote access via an insecure home/personal Wi-Fi | Providing each employee who works with a lot of sensitive data, with a firewall to secure their home's Wi-Fi. |
| Use of personal devices like flash drives for printing/ sharing data/ sending data | Deploying an antivirus software for each work-issued device that is administered to every employee. |
| Phishing Schemes | Effectively encrypting sensitive data when it's sent over email or phone. |
| Human error which can be in several different forms like employees using poor/weak passwords to protect data despite having secure VPNs and firewalls in the network. | The company can impose Password policies to help ensure that each employee has strong passwords which cannot be easily hacked or create a vulnerability in the access to data. |