**NAME: Edith Njoki Wangui**

**Email address:** [**edith.wangui@womentechsters.org**](mailto:edith.wangui@womentechsters.org)

**Risk Assessment Plan (risks, threats, vulnerabilities and security protection mechanisms) of MBI Insurance Company**

|  |  |  |  |
| --- | --- | --- | --- |
| **Hazard (threats, risks, vulnerabilities)** | **Who is at risk** | **Risks** | **Protection**  **Mechanisms** |
| Unsafe network connections e.g. use of home or public insecure Wi-Fi | Data i.e.  organizations data  clients data  employees data | Leaking of sensitive information to cyber criminals  Legal sue due to leakage of clients data | Use of encrypted communication tools like virtual private network when accessing the company’s data or files. |
| Insider threats | Organizations data that includes employees clients data  Software  Documentation | Data leaks  Loss of data in case of deletion or loss of documents | Provide security training to employees regularly  Employees to report on security breaches such as deletion or modification of data on their end  No access to sensitive information by unauthorized users including employees  Enforce use of antivirus software in their devices that are recommended by the organization  Monitor devices regularly |
| System failures | Hardware  Software  Organizations data | Loss of data | Backup data on organizations cloud servers  Regular update of software used by employees  Reporting of any system failures by employees  Reporting of any system failures by employees so that other systems can be made available to them |
| Use of third party software | Software’s  Organizations data | Leakage of data through hacking or malicious software’s designed to steal information on systems | Use third party software’s recommended by the organization  Enforce the use of anti-virus software on employees devices  Access files emails from secured company servers |
| Natural disasters  e.g. fires, floods, power outages | Hardware  Organizations data  Documentation  Employees | Loss of data  Loss of hardware(computers)  Loss of documentation | Transfer the risk to third party  Backup data on cloud servers by all employees  Employees should report on disasters |
| Personal devices | Organizations data  Software’s  Hardware(employees computers) | Unauthorized access to sensitive information by unauthorized users  Data leaks  Opening emails containing malware | Avoid data sharing  Use only devices authorized by the organization when working  Update software’s regularly  Report in case of theft of devices  Access files and emails from secure company servers  Avoid use of public Wi-Fi and use encrypted communication tools when sending files  Report on cases such as data deletion due to human errors and any modification of data and also the loss of devices. |