# MBI INSURANCE COMPANY WORKING FROM HOME RISK ASSESSMENT PLAN

Due to Covid-19 some workers will be working from home as of 21/05/2021 and will be using their devices and internet. As the Information System Department we have assessed the risks and vulnerabilities that will come with and we have looked at ways to mitigate these and this is what this report is based on.

## HAZARDS

* Since workers are taking work home, specifically on their own devices, workers devices might have viruses thus placing the information **confidentiality** at stake.
* Workers have been physically working with files and departments were physically divided by floors so only people in certain floors had access to certain information but since we are going online, division will be made by resources and their tags so no personnel from a different department interferes with information of another ensuring information **integrity.**
* Workers are using their own internet which could result in latency or sometimes not having data and thus the **availability** of the information to stakeholders and customers will not be 100%.

## IMPACT AND PRECAUTIONS

* If information **confidentiality** is at risk this impacts our clients whose information might be sold or use maliciously which then affects stakeholders as the company’s reputation will go down the drain with lawsuits and trying to counteract the damage.

As a precautionary measure a system should be put into place where workers will login in to do their work and this system will be handled by the I.T team for security, mitigation and overall maintenance.

* Information **integrity** is key and the loss of it means loosing assets and costing the company recuperation money.

A precautionary measure to this is to use tags to isolate and group resources according to departments and to add authorisations to these resource groups.

* With weak or no information **availability**, departments will not be able to access information as needed and this will affect how and when their do their work which ultimately affects how the company runs.

As a precaution a VPN will be put into place into the system created to mitigate confidentiality and we will delegate to the necessary department to ensure workers have Wi-Fi to do their work.

## CONCLUSION

All of the precautionary measures will be deployed and maintained using Microsoft Azure. We will record videos so workers can familiarise themselves with the system and any help they need can be e-mailed to the Support Desk.

We hope everyone stays safe.

Information Security Team