**Mechanical Breakdown Insurance Risk Assessment Report**

1. Introduction

Due to the new policy that has allowed employees to work from home, this report details the cyber risks that are posed to the organization, how they can impact the organization and our customers and how we can best approach these risks.

2. What are the risks posed by the Work from Home policy?

* **Theft of sensitive information**
* **Hardware damage**
* **Compromised credentials**
* **Malware and viruses**

3. How do these risks affect the organization?

**Theft of sensitive information**

As an insurance organization, we store highly valuable and confidential information such as banking details and identification information. If an employee’s device happens to get hacked or they install phishing software, a data breach can occur resulting in competitors gaining our knowledge and contacting customers which would lead to loss of profit. Also in the case of a hacker gaining access to sensitive information, they could hold the company at ransom in order to release the information which can be very costly. Customers would lose trust in us and withdraw from the organization. Some may sue the organization for breach of private information.

**Hardware damage**

If an employee happens to damage a work device, it would cost the organization to replace/repair the device. It would also mean less productivity from the employee for a duration of the time taken to replace the device hence disrupting the workflow in a certain department. That would result in inefficient delivery times for in demand services which could result in customer dissatisfaction.

**Compromised credentials**

If an employee signs in to the work portal and a person happens to see their login credentials, if the person has malicious intent, they can sign in to the portal and gain access to highly sensitive and confidential information. The bigger threat is the fact that they can go undetected for a long period of time causing immeasurable amounts of damage to the organization. This can increase the probability of data breaches from hackers who can decide to hold the organization at ransom or sell the information to competitors.

**Malware and viruses**

If the employee downloads third party software, the software may contain viruses that could damage the device resulting in complete data wipes which can be very detrimental to productivity or leaked information which can lead to legal issues, customer dissatisfaction and loss of business.

4. How to mitigate these risks

* Ensure all employees strictly use their work devices to access the work portal.
* Create authorization roles of who can access certain information and restrict access to highly valuable information stores.
* Create a VPN server that only the work devices can access.
* Change the login credentials used to access the work portal daily.
* Regular audits of where and how employees access the work portal.
* Constantly back up information to secure servers.
* Restrict access to other websites that are not relevant to the organization.
* Consider insuring work devices in the event of damage.
* Educating employees on security awareness.
* Constantly ensuring the servers are properly encrypted from unauthorized access.
* Regular work portal updates to ensure up to date security patches
* Create a cyber breach response plan that is transparent to customers and reassures them that their security is always a priority to the organization.