**<<Your business name here>>**

**Cybersecurity Policy**

**Why Cybersecurity is important to us**

In today's modern world, our business depends on computer systems to operate and grow while computer-based attacks are becoming more common. We want to protect our business operations and computer systems from attacks by adopting good computer security practices. If we do not do this, it will be bad for our business because successful computer attacks can cause us to lose valuable income and damage our reputation with new and existing customer/clients. Please support us by reading this policy and sign to show your commitment.

All employees are expected to be responsible when using any of our computer systems and always operate in the best interest of the company.

**How to think about security in our business**

* Every employee is important in supporting good computer security in our business.
* It’s OK to question a computer-related request from anyone that seems suspicious, strange or unethical.
* It is BAD to share any computer access details or private business information with anyone unless approved by your team leader.
* It is GOOD to ask questions, report security concerns, issue, or breach to your team leader. When in doubt about anything always consult your team leader so they can assist you.

**This policy is separated into two (2) sections:**

* Access, Use and Share - What you must do
* Implement and Manage - What we will do

**Access, Using and Sharing**

Get started - Only access computer systems for which you are authorised and never share your access details with anyone.

Understand what we are protecting – We are protecting all digital assets. We consider computer assets to mean both hardware and software which we own and use in our business.

Practise good security habits – Make it a lifestyle habit to practise good security habits, both at work and outside of work.

Be sceptical - do not be afraid to question suspicious or unusual requests for private information.

Identify and report security issues - if at any point you feel there is a security issue, always report it to your team leader so we can investigate and assist.

Keep things basic - To minimise our risk of security breaches, we will aim to give you access only to necessary computer assets.

Sharing - Unless confirmed by your team leader, do not share private business data with anyone outside the business, especially through Social Media or personal messaging applications.

**Implement and Manage**

Identify assets - This business will always try to keep records of which computer systems our business owns.

Blocking harmful software and actions - We will always try to block harmful software and computer functions which may contribute to a security breach.

Setup of new computer systems - We will always try to use good and current security practices when setting up new computer systems to minimise the chance of a security breach.

Improving computer systems - We will continuously review the computer systems we use to identify security weaknesses which we can improve.

Storing/Saving - Store data/information created during work activities.

Internal training and exercises - We will provide you with training periodically to help keep you aware of good security practices.

Monitoring security issues - We will try to keep track of the security issues we have experienced so we can continuously improve.

Review of computer activity - Sometimes we will check the activity records stored on our computer systems to identify security issues we may have missed.

Backup and recovery - We will periodically create a copy of all business data on our computer systems so that in case a system fails we can restore the copy and return to normal.

Independent checks - Sometimes we will ask security professionals to come in and check how well our security practices are working.

|  |  |
| --- | --- |
| **If you have read, understood and will support this policy, then please complete below.** | |
| ……………………………………………………………………….  Full Name | ……………………………………………………………………….  Signature |

**Confidential:** Do NOT share with anyone outside our business.