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

**Security Controls**

**Why these controls are important**

The following are a list of security controls we want to implement to protect our computer systems from attacks and harmful user activity.

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 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.

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.

Please implement the following controls as simply and efficiently as possible using computer-based tools while minimising the security risks to our computer systems.

**Managing Data/Information**

**Identify assets**

We want to create and maintain a record of all computer systems we own and use.

Requirement(s):

For hardware, please record at least the system’s name, model, and serial

For licensed software, please record the name, version, license number and the license owner.

**Block harmful software and actions**

We want to block bad software and computer actions which may contribute to a security breach.

Requirement(s):

* Install a reputable anti-malware software which is licensed to us, and centrally managed to tell us when any of our systems become infected or experience suspicious behaviour.
* Set up automatic daily scans that check all computer systems for malicious software.
* Prevent users from installing software without the team leader using their password approve the installation. i.e. Administrator password.

**Train and educate staff**

We want to train our employees periodically to keep them continually aware of good security practices.

Requirement(s):

* At least every 3 months, give all our employees basic educational guidance on how to use our computer systems and the internet responsibly based on current events.

**Monitor security issues**

We want to keep track of the security issues we have experienced so we can continuously improve.

Requirement(s):

* Implement a basic means of recording security issues that are reported.
* Set all computer systems to record user activity and system activity to show (user ID) who did what (activity/event) and when they did it (date and time).
* At least log critical events such as user login, log off, when a program is opened or installed.
* Set logs to overwrite themselves after 6 months to save on space.

**Review computer logs**

At least once every 3 months we want to periodically check the activity records stored on our computer systems to identify security issues we may have missed.

Requirement(s):

* Check for high numbers of failed login attempts
* Check for malfunctions in programs running
* Check for strange programs that start-up when someone logs in.

**Backup and recover**

We want to 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.

Requirement(s):

* Create a basic and automated backup system which stores backup files on a secure remote location such as an encrypted external drive or cloud storage.
* The backup should require a strong password, only known to team leaders.
* This backup should run at least weekly to save our essential business data.
* Set this automated backup to overwrite itself after at least 3 successful backups, to help us save on space.

**Check independently**

We want someone competent who is not employed by us to come in and assess how well our security practices are working.

Requirement(s):

* Compare our actual computer assets to our electronic records of assets and identify gaps.
* Check for harmful software running on our computers
* Check if we have been making backups of our important computer data
* Check if computer system records show any suspicious activities and perform a quick investigation
* Remove junk software that is not relevant to our business operations. Please confirm with our business owner before removing.

|  |  |
| --- | --- |
| **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.