[YOUR BUSINESS NAME] IT SECURITY POLICY

Spark Lab has created this template with smaller businesses in mind. It can also be used as a base for conversation in medium to large businesses.

To see how Spark can help with your IT Security, call us on 0800 110 062.

Writing policies can be very useful, but only if they are ‘owned’, maintained and most importantly, enforced by people in your business to ensure its success.

# Contents.

[Introduction. 3](#_Toc526931941)

[Responsibilities. 3](#_Toc526931942)

[Review Process. 3](#_Toc526931943)

[Managing Our Information. 4](#_Toc526931944)

[Public. 4](#_Toc526931945)

[Employee Confidential. 4](#_Toc526931946)

[Business Confidential. 4](#_Toc526931947)

[Customer Confidential. 4](#_Toc526931948)

[Access Controls. 5](#_Toc526931949)

[Security Software. 5](#_Toc526931950)

[Employees Joining [Your Business Name]. 5](#_Toc526931951)

[Employees Leaving [Your Business Name]. 6](#_Toc526931952)

[Your Responsibilities. 6](#_Toc526931953)

[Protecting Your Own Device(s). 6](#_Toc526931954)

[Password Guidelines. 7](#_Toc526931955)

[Be Alert to Other Security Risks. 7](#_Toc526931956)

[Backup, Disaster Recovery and Continuity. 8](#_Toc526931957)

# Introduction.

At [Your Business Name], we recognise that cyber security is a global issue and a very real threat to Kiwi businesses, with many unable to recover from cyber-attacks due to the cost and time involved. We have created this IT Security Policy to assist us in reducing the risk to ourselves and, more importantly, our customers and their data.

**Important: It is compulsory for all our people to read and acknowledge they will uphold the requirements of this policy.**

The intention of this policy is to:

1. Reduce the risk of a cyber attack
2. Meet our professional obligations towards customers
3. Protect our customer, employee and business data
4. Prepare for cyber threats and deal with them when they happen
5. Continue working if something does go wrong
6. Keep our company information and intellectual property confidential
7. Meet our legal obligations under New Zealand law

# Responsibilities.

The table below lists the names and roles of those who are responsible for maintaining and implementing this Policy.

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Responsibilities** |
| [Name] | [Owner/Director] | Managing IT Security Strategy |
| [Name] | [Operations Manager] | Implementing this Policy day-to-day |
| [Name] | [IT Manager or Partner] | Assist with IT Security planning and support |
| [Name] | [Legal support] | Advise on data protection laws and best practices |

# Review Process.

We will review this policy [frequency].

The next review date is [dd-mmm-yyyy].

In the meantime, if you have any questions, or feedback, please contact our [Role], [Name] at [email] or [phone].

# Managing Our Information.

At [Your Business Name], we only collect information necessary to serve our customers and carry out our business responsibilities. Disclosing any confidential information - whether intentional or not - has the potential to seriously harm [Your Business Name].

**Important: You should assume information is confidential unless you are sure it is not and act accordingly.**

If unsure, please reach out to [Role], [Name]. We expect all our people to take responsibility and exercise extreme care when dealing with confidential information.

We manage information using these four groups so we can protect it as best as we can:

|  |  |
| --- | --- |
| Public. This is information that can be made public without any implications for the company, such as information that is already in the public domain. | Employee Confidential. This includes but is not limited to:   * Payroll and salary information * leave allowances * [HR matters] |
| Business Confidential. This includes but is not limited to:   * contracts/agreements * any documents * business plans * passwords for all [Your Business Name]’s software and systems * customer contact records * accounts | Customer Confidential. This includes but is not limited to:   * any personally identifiable information such as   + name   + address (email or physical)   + account information * passwords to customer systems * customer business plans * new product information * market sensitive information |

We have grouped the information we keep as follows:

|  |  |  |
| --- | --- | --- |
| **Information Type** | **Systems Involved** | **Category** |
| [e.g. Customer records] | [CRM software] | [Customer Confidential] |
| [e.g. Account Information] | [Accounting software] | [Business Confidential] |
| [e.g. Salary information] | [Payroll software] | [Employee Confidential] |

# Access Controls.

At [Your Business Name], we try and take a practical and pragmatic approach to the way we control access levels to our data and information. Generally, we have structured our data access as follows:

|  |  |  |
| --- | --- | --- |
| **Control measures** | **Sensitive Systems** | **Trusted Admin Users** |
| **Customer Confidential** | | |
| [Measure] | [system name/s] | [Role/s and name/s] |
| **Employee Confidential** | | |
| [Measure] | [system name/s] | [Role/s and name/s] |
| **Business Confidential** | | |
| [Measure] | [system name/s] | [Role/s and name/s] |

# Security Software.

To protect our data, systems, users and customers we use the following security systems:

|  |  |  |
| --- | --- | --- |
| **System Type** | **Security Software** | **Software Licence Details** |
| [e.g. Laptop/Desktop anti-malware] | [Software Name] | [Licence Details] |
| [e.g.Server anti-malware] | [Software Name] | [Licence Details] |
| [e.g. Cloud-hosted filtering] | [Software Name] | [Licence Details] |
| [e.g. Email archiving] | [Software Name] | [Licence Details] |
| [e.g. Website malware and vulnerability scanning] | [Software Name] | [Licence Details] |
| [e.g. Firewall] | [Software Name] | [Licence Details] |
| [e.g. Intrusion prevention and detection] | [Software Name] | [Licence Details] |

# Employees Joining [Your Business Name].

When a new employee joins us, we will add them to the following systems:

|  |  |  |
| --- | --- | --- |
| **Role Type** | **Systems** | **Access Levels** |
| [Role type 1] | [systems] | [access level 1] |
| [Role type 2] | [systems] | [access level 2] |
| [Role type 3] | [systems] | [access level 3] |

We will also provide training to new staff (including contractors) within [timeframe] of their start-date. This includes:

* An initial introduction to IT security, covering the risks, basic security measures and company policies
* Expected behaviour and where to get help; and
* Training on how to use company systems and security software properly

# Employees Leaving [Your Business Name].

When people leave a project or leave [Your Business Name], we will remove any of their access rights to our business systems **within** **[timeframe]**.

Anyone leaving [Your Business Name] is required to return any company property, transfer any company work-related files back to the company and delete all confidential information from your systems as soon as possible.

# Your Responsibilities.

At [Your Business Name], we encourage a culture of trust and need all our people to support our efforts to operate a secure business. It is your responsibility to know and follow these guidelines.

**Important: You are personally responsible for the secure handling of confidential information that is entrusted to you.**

You may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties. If you become aware of any theft, loss or unauthorised disclosure of protected information or any breach of this policy, we expect you to promptly report this to [Role, Name].

# Protecting Your Own Device(s).

**Important: For our people who use their own devices (e.g. mobile phone, laptop, tablet) it is your responsibility to use these in a secure way.**

[Your Business Name] will provide training and support to help you to do so (see below). At a minimum:

1. Use biometrics (e.g. fingerprint or facial recognition) to log in wherever possible.
2. Make sure your device logs out automatically after 15 minutes and requires a password to log back in.
3. Remove software that you do not use or need from your computer
4. Update your operating system and applications as soon as you are prompted
5. Keep your computer firewall switched on
6. **For Windows users**: Make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date.
7. **For Mac users:** Consider getting anti-malware software.
8. Store files in [Your Business Name] storage locations so that it is backed up properly and available in an emergency.
9. Understand the privacy and security settings on your phone and social media accounts
10. Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers.

# Password Guidelines.

* **Never** share or disclose your password to anyone else
* **Never** write down PINs and passwords
* **Never** use the same password for multiple systems
* **Always** use strong passwords (at least 8 characters, include numbers and symbols)
* **Always** change them every 3 months (set yourself a calendar reminder if you use your own device/s)
* **Always** change default passwords and PINs on computers, phones and all network devices

# Be Alert to Other Security Risks.

While technology can prevent many security incidents, the actions and habits of our people are critical to maintaining secure systems. With this in mind:

Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender.

Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information, including employee, client or company confidential information. Fraudsters and hackers can be extremely persuasive and manipulative.

Be wary of fake websites and phishing emails. Don’t click on links in emails or social media. Don’t disclose passwords and other confidential information unless you are sure you are on a legitimate website.

Use social media, including personal blogs, in a professional and responsible way, without violating company policies or disclosing confidential information.

Where confidential information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and shredded when no longer required.

The following things (among others) are, in general, prohibited on company systems and while carrying out your duties for the company and may result in disciplinary action:

Circumventing user authentication or security of any system, network or account.

Downloading or installing pirated software.

Disclosure of confidential information at any time.

# Backup, Disaster Recovery and Continuity.

This is how we backup our business-critical systems.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System Name** | **Backup Mechanism** | **Frequency of Backup** | **Recovery Time Target** | **Recovery Point Target** | **Frequency of Test Restores** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

This is how we will respond to potential interruptions to our business:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event** | **Who to Alert** | **Initial Response** | **Recovery Action Steps** | **Where to go for Support /Advice** |
| [e.g. Natural Disaster] |  |  |  |  |
| [e.g. Loss of Power] |  |  |  |  |
| [e.g. Loss of Internet and/or Phone connection] |  |  |  |  |
| [e.g. Loss or theft of critical systems] |  |  |  |  |
| [e.g. Loss or theft of data] |  |  |  |  |

We will test these contingency plans at least once a year.