

## IT acceptable use policy

### Purpose

The purpose of the IT Acceptable Use Policy is to ensure that all IT Resources such as systems, networks, and any equipment owned or managed by Vector are operated in an effective, safe, ethical, and lawful manner.

### Who does this policy apply to?

This policy applies to all Vector people, employees, directors, contractors, consultants, temporaries, and other workers at Vector, including all personnel affiliated with third parties that use IT Resources that are owned or leased by Vector.

Vector expects all Vector people to:

1. Utilise IT Resources responsibly and ethically, respecting the rights of other users, our customers and Vector's contractual, legal, regulatory and ethical obligations.
2. Engage in activities that do not intentionally disrupt, damage or allow unauthorised access to Vector systems or data.
3. Use Vector systems and data in accordance with Vector's policies, values and Strategic Pillars.
4. Report any potential misuse, data loss or compromise, or unusual activity to appropriate managers or teams ([Cyber Security](#), [Enterprise Information Management](#), or the [Privacy Officer](#)).

More detailed guidance is provided in the sections below.



## 1. Access control

- 1.1 Rights are granted based on business need and access to IT Resources is provided by the appropriate system administrator. Any other access is considered unauthorised and is in breach of this requirement.
- 1.2 Damaging, altering, or disrupting the operations of Vector IT Resources is not permitted. Users must not carry out any activity with the intention of capturing or obtaining passwords, encryption keys, or anything that could facilitate unauthorised access by themselves or anyone else.
- 1.3 Access to any Vector IT Resources must be through an authorised Vector user account.
- 1.4 Unauthorised persons must not be permitted to access Vector's buildings or premises.
- 1.5 All visitors to Vector must be signed in through the sign-in process established at each of its physical locations. Anyone not wearing visible identification such as a visitor's badge or pass, or anyone not appearing to be part of Vector, should be challenged for identification.

## 2. Passwords and authentication

- 2.1 User IDs and passwords must not be disclosed to anyone or shared with anyone.
- 2.2 Passwords must comply with [Vector's Password Standard](#).
- 2.3 Group or generic user IDs and passwords are prohibited as a rule, but in special circumstances may be approved by the Cyber Security team ([cybersecurity@vector.co.nz](mailto:cybersecurity@vector.co.nz)) who will keep a written record of the exceptions.
- 2.4 Passwords must not be written down and left in a place where unauthorised persons might discover them or saved in plain text. Only a Vector approved password management application may be used to store passwords.
- 2.5 Anyone that uses a personal computer at home should use different login credentials for their work and home accounts.
- 2.6 Users are responsible for all activity performed with their personal user IDs and passwords. Users must not allow others to perform any activity with their user IDs and are not permitted to perform any activity with IDs belonging to other users.



2.7 Users are responsible for locking their computer screen whenever they leave their computer unattended – even for just a short period of time.

### 3. Mobile devices and bring your own device

3.1 Vector supports Bring Your Own Device (BYOD) on its wireless network. However, the use of any personal devices such as mobile phones, tablets, portable computers, laptops, etc must comply with the requirements of this policy.

3.2 Mobile devices supplied by Vector must not be altered or added to in any way including:

- Unauthorised upgrades.
- Addition of components.
- Removal of components.
- Altering configuration or security settings.
- Installation of non-approved applications.

3.3 All Vector-owned and BYOD devices must have Vector's Mobile Device Management solution installed. Any changes or maintenance will be carried out by the Digital Workplace Service (DWS) Team.

3.4 Use of public Wi-Fi or charging stations to access Vector systems or data or charging Vector-owned devices should be with care. Do not connect to an unknown or unrecognised wireless access point and verify that it is a legitimate wireless connection.

3.5 Data and voice services are available on the SIM card(s) mainly for business purpose, Vector also allows a reasonable personal usage (usually three times the average usage) of data and voice services. As over usage incurs in extra costs for Vector, if you exceed the reasonable usage limit you will be contacted with alternatives and options going forward.

3.6 If a Vector-owned mobile device is lost or stolen, contact the DWS Team via TechConnect.

3.7 Vector maintains the right to conduct inspections of any mobile device that it owns or manages without prior notice to the user or custodian. The device must be returned to the DWS Team upon request for maintenance and when the user ceases to provide services to Vector.

3.8 Except for purchases made from an approved online application store (e.g. Apple's App Store or Google's Google Play Store), games, freeware, shareware, video or



music may not be downloaded onto any Vector mobile device unless its use is legal (does not breach copyright law). Videos taken with the device for work purposes are exempt from this requirement.

- 3.9 Any purchase that incurs in a cost must be approved and performed by a systems administrator or covered by the user.

## 4. IT resources use

4.1 Users of IT Resources owned or managed by Vector shall not use these IT Resources to engage in any activity which contravenes human rights legislation, or which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user for any reason or on any grounds, including on any prohibited grounds.

4.2 Vector IT Resources are primarily for business use and must not be used for illegal or unethical purposes in any circumstances.

4.3 Personal use of Vector IT Resources must be reasonable and appropriate and not impact on staff productivity, operating costs, system performance or bring Vector into disrepute.

4.4 Only voice and video communication systems approved by Vector shall be used. Any other voice and video communication system must be approved by the Cyber Security team ([cybersecurity@vector.co.nz](mailto:cybersecurity@vector.co.nz)) before being used.

4.5 USB sticks, key fobs or any other storage devices allocated by Vector are only for business use. Extra care is required when storing information on these devices due to their size and portability. Users should be aware of the following:

- Loss of keys and data is a problem due to the small size of these devices.
- Increased chances of introducing a virus as such devices can be used on multiple computers.
- Such devices should not be inserted into any computer that does not have up-to-date security patches and anti-virus software.
- Such devices must be stored and transported in a safe manner to reduce the chances of loss.
- Data on such devices should be encrypted and/or protected by a password that complies with [Vector's Password Standard](#).
- Such devices found at random should not be used at all and handed into DWS Team immediately.

4.6 IT Resources supplied by Vector must not be altered or added to by users any way including:

- Unauthorised upgrades.
- Addition of components.
- Removal of components.



- Altering configuration or security settings.
  - Installation of non-approved applications.
- 4.7 All changes to the configuration or maintenance of IT Resources must be carried out by the DWS Team.
- 4.8 Users should not lend IT Resources that have been allocated to them by Vector for business activities to anyone. This includes, co-workers, friends, and family.
- 4.9 Any actions or activities, whether intended or accidental which cause, or could cause the computer systems, information or networks of Vector to be compromised in any way is considered serious misconduct including (but not limited to):
- Security breaches or disruptions of network communications. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
  - Port scanning or security scanning. These activities are expressly prohibited unless sanctioned by the Cyber Security team ([cybersecurity@vector.co.nz](mailto:cybersecurity@vector.co.nz)) for the purposes of testing network security.
  - Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal duties or has been duly authorised.
  - Circumventing user authentication or security of any host, network or account or running password cracking programs.
  - Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
  - Using any program/script/command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally.
  - Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data.
  - Copying or altering configuration or system files for unauthorised personal use or to provide to other people or users for unauthorised use.
  - Creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with Vector's or another organisation's email service.
  - Downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by Vector or not.
  - Providing or selling Vector information without approval and for personal gain.
  - Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using Vector resources that would bring Vector into disrepute.



- 4.10 Users must use the standard applications for which Vector is licensed. Users are not permitted to install any software program, application, script or executable code on Vector

IT Resources in their care. Only software approved by the DWS and Cyber Teams may be installed.

- 4.11 Devices provided by Vector have been configured to connect to network resources (including the Internet) using approved wired or wireless mechanisms. Users working in Vector's premises are not permitted to connect to the Internet using mobile USB modems, personal hotspots, USB mobile wireless devices, mobile broadband cards or any other mechanism that bypass official corporate systems.
- 4.12 If printing confidential or potentially sensitive information the printouts must be protected from being viewed by unauthorised persons.

## 5. Email

- 5.1 Vector's email system is predominantly for business use. Personal use must be reasonable and appropriate and not impact on staff productivity, system performance or bring Vector into disrepute.
- 5.2 All use of email must be consistent with Vector policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- 5.3 Users are prohibited from using third-party email systems such as Google, Yahoo, and MSN Hotmail etc. to conduct Vector business, or to store or retain email on behalf of Vector and must never email any work-related documents to their personal email accounts.
- 5.4 Email attachments and embedded links should be treated with caution. If a message does appear to be not genuine and/or the sender unknown, it should be reported using the "Report Message" add-in in the Microsoft Outlook toolbar. Under no circumstances should attachments or links from suspicious emails be opened, or any personal or security information disclosed if prompted.

## 6. Information management

- 6.1 Subject to any third-party agreement, any document, data and/or information created modified saved, transmitted or archived using the corporate systems of Vector, or otherwise located within a computer system owned or managed by Vector, remains the property of Vector. For the avoidance of doubt, this includes any personal documents and emails.
- 6.2 All corporate information and data must be stored in approved corporate information repositories. This includes the appropriate information repository, corporate applications and other approved shared repositories. Information is not to be stored on local drives of



PCs or workstations, USB devices, laptops or copied onto portable media such as CDs or DVDs unless these copies are made in addition to saving it in an approved corporate file system.

Filesharing services that are not approved by Vector are not permitted to be used to store and exchange corporate data. Examples include (but are not limited to) Dropbox, iCloud, GoogleDrive, and personal OneDrive accounts, etc.

The following filesharing services are approved:

Service	For filesharing with external parties?	For filesharing with internal parties?
Accellion	Yes	No
Microsoft Teams	Yes	Yes
Vector OneDrive	No	Yes
SharePoint	Subject to approval by <a href="#">Cyber Security</a> and <a href="#">Enterprise Information Management</a>	Yes

6.3 Electronic information must be protected based on its sensitivity, value and criticality regardless of the type of media that holds the information, its location, the systems used to process it or the processes it is subjected to, as described in the Group Data and Information Policy.

6.4 Users must not delete or dispose of potentially important Vector electronic records or information without the approval of the Enterprise Information Management team ([InformationManagement@vector.co.nz](mailto:InformationManagement@vector.co.nz)) and the data owner, and without following standard document management procedures for disposing of information. Deleting Vector's records without following the proper procedures is considered a serious breach of this requirement particularly if the records cannot be recovered.

6.5 It should be noted that document retention should be in accordance with Group Data and Information Policy.

## 7. Internet use

7.1 The internet is primarily available for business use. Personal use must be reasonable and appropriate, not impact on staff productivity, operational costs, system performance or bring Vector into disrepute.

7.2 Users of the internet connection managed by Vector shall not use the connection to visit, interact with, or download content from websites that are offensive, obscene, contain indecent material (such as pornography and violence), contravene human rights legislation or which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user for any reason or on any grounds, including on any prohibited grounds.



7.3 The internet connection must not be used for any illegal or unethical activity or personal business activity and must not be used to compromise the security of any computer system or network whether owned or managed by Vector or not.

7.4 Examples of unacceptable internet use include (but are not limited to):

- Computer hacking (accessing another's electronic data or computer without permission).
- Providing access to unauthorised persons.
- Impersonation.
- File downloads (except for work related reasons).
- Use of the internet for personal gain.
- Gaming, wagering or betting.
- Playing online games.
- The intentional transmission in any way of viruses or files that cause a negative impact on computer systems (e.g. unauthorised email attachments such as video, audio and executable files).
- Downloading or distributing information subject to copyright requirements (such as licensed software or protected internet applications).
- Disclosing private or confidential information including passwords or other information that may compromise the security of the computer systems.
- Engaging in any illegal activity, including dissemination of material in breach of legislation.
- Bypassing Vector's security, firewalls, and authentication mechanisms.
- Peer to peer file sharing or downloading of movies, music, eBooks, applications, games and so forth is not permitted.

7.5 The internet shall not be accessed from another employee's computer, unless the user is logged on with their own username and password.

## 8. Remote access

8.1 Citrix is the preferred remote access portal. All staff have access to Citrix by default.

8.2 Users (staff or external users) who require access to the virtual private network (VPN) must log a request with the DWS Team and obtain approval from the Cyber Security team ([cybersecurity@vector.co.nz](mailto:cybersecurity@vector.co.nz)).

8.3 Remote users are only permitted access to applications and systems they have been approved access for the purpose of fulfilling obligations to Vector. All other access is unauthorised.





## 9. Policy compliance

- 9.1 It is the responsibility of every user to understand and to comply with the requirements of this policy and report any non-compliance to their manager, the DWS Team, [Cyber Security](#) or the [Privacy Officer](#).
- 9.2 Vector may conduct internal audits or investigations of IT Resources or may be subject to independent external audits. Auditing may include any stored content, and all aspects of IT Resources use, including emails, chat, web history and usage.
- 9.3 Vector may at any time monitor all aspects of IT Resources, including a user's login sessions, to determine if a user is violating the IT Acceptable Use Policy or any Vector Policy, or for any other reason.
- 9.4 In the course of Vector investigating a suspected breach of the IT Acceptable Use Policy or any other Vector policy, Vector may request permission from a user to audit privately owned equipment or device(s) where, on reasonable grounds, it believes such equipment or devices were involved in the alleged incident.
- 9.5 If you breach any aspect of the IT Acceptable Use Policy, you may be subject to formal disciplinary processes as described in the Vector Code of Conduct and Ethics, and Performance and Conduct Policy.
- 9.6 If as a result of its investigation Vector suspects that you have been involved with, or have been using, viewing or distributing illegal material in any form, or have been involved in an activity which might constitute criminal conduct, Vector may be obliged to report such activities to the relevant legal, law enforcement or regulatory authorities.

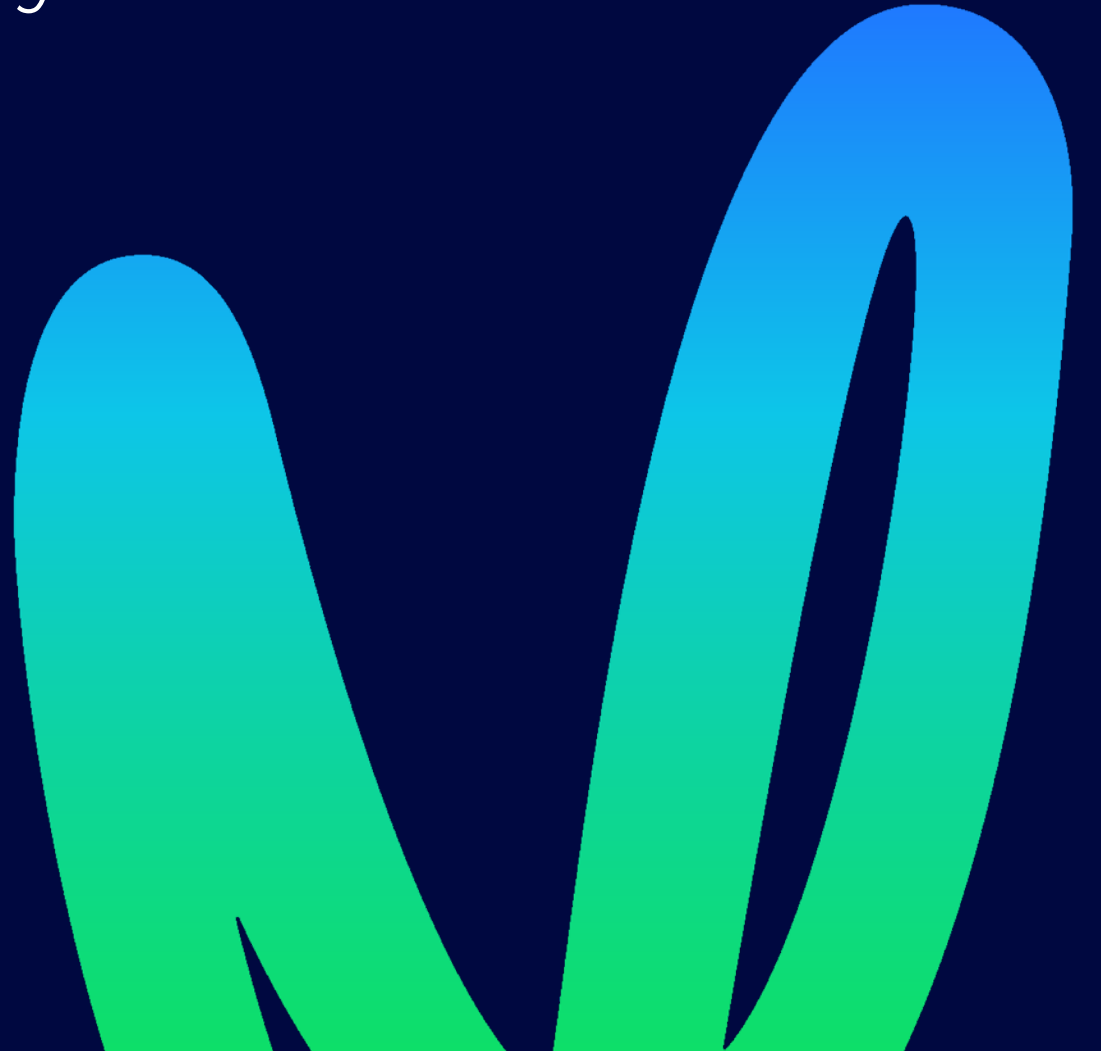
## 10. Associated documents

The following documents are associated with this policy:

- Group Data and Information Policy
- Vector Code of Conduct and Ethics, and Performance and Conduct Policy.

# Introductory Cyber Security Awareness Training for New Starters

**Cyber security is everyone's  
responsibility**



Welcome to the Vector team, we're excited to have you on board.

*The easiest target isn't a system or technology.*

*It's you and me.*

Protecting yourself will protect the business,  
here's how you can help.



# Why cyber security awareness?

Security awareness training encourages Vector people to be responsible for keeping Vector and themselves safe online by developing good habits

## Team Effort

Cyber security is a team effort and everyone's responsibility – yes, it's yours, too



## Good Habits

Better cyber security habits help you keep Vector and yourself safe online



## Fewer Incidents

Report suspicious activity to help prevent security incidents



We need **YOU** in our ongoing effort to reduce cyber security risk and help Vector create a new energy future, securely



# What you need to know



91% of all cyber crimes begin with an email



Resulting in:

- Business disruption
- Financial loss
- Reputational damage

# Avoid getting phished

Mail attachments are a leading source of malware and ransomware

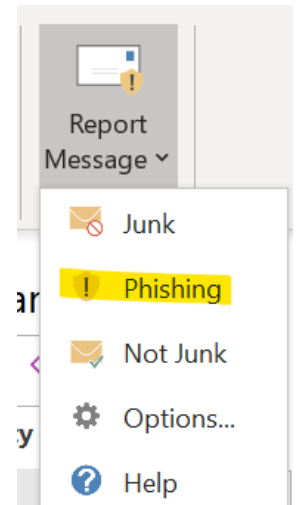
Be suspicious of all unexpected emails or any that seem out of character.



Never click on web links or download any attachments or files you weren't expecting to receive.

If something doesn't look quite right, it's probably not. Report it by using the Report Message tab in Outlook.

If you're unsure about a message you've received, it's a good idea to check it with a colleague, friend or family member.



# Social Engineering

## How can you protect yourself?

- If you suspect someone is trying to trick or fool you, do not communicate with the person.
- Never share sensitive information with anyone you don't know or are not sure is legitimate.
- Don't click on links from unknown senders or use USB sticks that you have found.
- If the attack is related to Vector, be sure to report it to **TechConnect** (Vector's IT Team) and the **Cyber Security team** right away.

### What is social engineering, anyway?

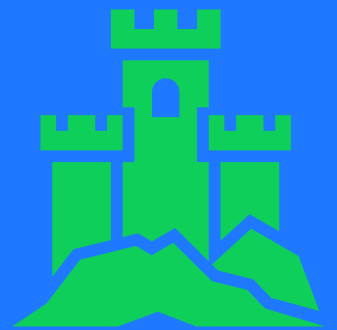
Social engineering is when someone deceives someone else into revealing information that can be exploited.

Social engineers will convince their target to give them crucial information or access, or even send money.



# Passwords are the keys to the kingdom

If an attacker gains access to your password, they are able to log into your account remotely as long as that password remains unchanged



# Passwords

## The top three tips

### NEVER share your password

- Never share your password with anyone and don't write them down

Following these tips means that if you fall victim to a cyber-attack, you'll only need to update the password for the compromised account

### UNIQUE passwords protect your accounts




- Long, strong and unique passwords are much harder for the cyber criminals to crack so try to aim for 15 characters or more
- We know coming up with strong passwords is hard, so trying making passphrases instead. They're easy to remember, but harder for attackers to crack e.g. Nextlevelsecurity!
- [Check out these tips on how to create a good one.](#)

### ALWAYS use two-factor authentication

- Use two factor authentication (2FA) or multi-factor authentication (MFA) if available
- Having MFA / 2FA turned on means even if an attacker gets your login details, they still won't get in
- If you'd like to find out more about MFA/2FA - [check out this article](#)

# Smartphones / Mobile devices

## Attackers have taken notice

-  As smartphone and mobile device ownership has increased attackers have begun targeting these devices because they are **easily lost, stolen and susceptible to cyber attacks** because of their technological vulnerabilities.
-  While Vector supports Bring Your Own Device (BYOD) on its wireless network and requires all Vector-owned and BYOD devices to have Vector's Mobile Device Management solution installed, we still need you to **keep your devices such as mobile phones, tablets, portable computers, laptops, etc. safe**
-  Updates help to keep your apps and devices healthy. It's not just about having the latest features, but they also protect you from any weaknesses that could let attackers in

After your start ensure you read Vector's IT Acceptable Use Policy that provides guidance around the use of mobile devices at Vector and outlines your obligations to help safeguard Vector's information.

# Avoid getting SMiShed or Vished

## SMiShing (SMS phishing) / Vishing (Voice phishing)

Look out for common attacks	Application Stores	Never click on a link in a text	Caller ID is not fool proof
<ul style="list-style-type: none"><li>• Fake security notifications and messages from government agencies are two common forms of SMiShing attacks.</li><li>• Vishers may impersonate government agencies, bill collectors, banks, couriers and others.</li></ul>	<ul style="list-style-type: none"><li>• Watch out for copycat applications from third-party developers.</li><li>• Only download applications from trusted sources such as the Google Play Store or the Apple App Store.</li><li>• Your phone can get malware from these applications or by clicking a link in a text</li></ul>	<ul style="list-style-type: none"><li>• Don't click on links or download any software updates or apps from texts.</li><li>• Updates will never arrive via text message.</li></ul>	<ul style="list-style-type: none"><li>• Never assume a call is legitimate</li><li>• Attackers are capable of spoofing caller ID to fool their targets.</li><li>• Some attackers will use text-to-speech devices or voice filters to sound like the automated calls used by legitimate organisations.</li></ul>

# Keep your mobile devices safe

**Backup your mobile phone or device often.** In the event the device is lost or stolen, restoring your information to a new device will be an easier process.

**Protect your devices from unauthorised access** through passwords and/or biometric locks such as fingerprints.

**Turn off connectivity settings when not in use**, like Bluetooth connections or Near Field Connections (NFC).

**Use only known and password-protected networks** and never connect to unknown wireless networks.

**Check privacy settings for apps.** Many applications want you to share your location, account information, or file information stored on your device.

If your Vector-owned mobile device is lost or stolen

contact [TechConnect](#) (Vector's IT team)

# Monitoring / IT Acceptable Use Policy

## Purpose.

The purpose of the IT Acceptable Use Policy is to ensure that all IT Resources such as systems, networks, and any equipment owned or managed by Vector are operated in an effective, safe, ethical, and lawful manner.

This policy applies to all Vector people, employees, directors, contractors, consultants, temporaries, and other workers at Vector, including all personnel affiliated with third parties that use IT Resources that are owned or leased by Vector.

Vector expects all Vector people to:

- Utilise IT Resources responsibly and ethically, respecting the rights of other users, our customers and Vector's contractual, legal, regulatory and ethical obligations.
- Engage in activities that do not intentionally disrupt, damage or allow unauthorised access to Vector systems or data.
- Use Vector systems and data in accordance with Vector's policies, values and Strategic Pillars.
- Report any potential misuse, data loss or compromise, or unusual activity to appropriate managers, **Tech Connect** or teams (Cyber Security, Enterprise Information Management, or the Privacy Officer).



You can view and download Vector's IT Acceptable Use Policy on [VectorConnect \(our employee intranet\)](#).

Thank you for being part of the journey in creating a new energy future, securely.

So what happens next I hear you ask?

- Our priority is to create a culture of security awareness through relevant training, reinforced by both offline and online communications during your time with us at Vector.
- Once you have access to your Vector account you will be assigned a Cyber Security Module in SuccessFactors, to be completed within your first week.
- Vector have partnered with InfosecIQ where you will be enrolled in a security training program focused on identifying and preventing security risks and threats.

For any questions relating to cyber security awareness please contact

[CyberSmart@vector.co.nz](mailto:CyberSmart@vector.co.nz)





## 11. Acceptance form

- 11.1 Please complete, sign, and date below to confirm your agreement to follow the obligations and responsibilities outlined in the IT acceptable use policy.
- 11.2 If you have any queries about the IT acceptable use policy, you are encouraged to discuss them with your Vector contact person/manager before you sign.
- 11.3 Once signed (electronically or scanned copy), return to your Vector contact person/manager to be included in the new user application.
- 11.4 I have read and am aware of the obligations and responsibilities outlined in this IT acceptable use policy, a copy of which I have been provided with and advised to retain for reference. These obligations and responsibilities, which I agree to follow, relate to the Vector work environment and IT Resources.
- 11.5 I also understand that suspected breaches of this IT acceptable use policy will be investigated by Vector, and could result in disciplinary action, and where necessary, referral to legal, law enforcement or regulatory authorities.

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Company: \_\_\_\_\_

Mobile number \_\_\_\_\_

(For Storm Mobile and the  
Gusto Signal Tester App  
users applying through  
Ventia only)

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

I confirm that I've read and understood the Cyber Security Awareness Training included within

## 12. Document control

<b>Document author:</b>	Monique Hogervorst (Cyber Security Governance, Risk and Compliance Manager)
<b>Document owner:</b>	Monique Hogervorst (Cyber Security Governance, Risk and Compliance Manager)
<b>Document approved by:</b>	Aaron McKeown (Chief Information Security Officer)
<b>Document published:</b>	Restricted distribution
<b>Version</b>	3.3
<b>Date of issue:</b>	31/07/2023
<b>Last reviewed/reason:</b>	Updated with condensed Cyber Training
<b>Date for next review:</b>	September 2024