Presidio Finance Consulting Pty Ltd ABN 51 128 973 508
Level 1, 32 Logan Rd, Woolloongabba Qld 4102
PO Box 1186, Coorparoo DC Qld 4151
Ph 1800 249 066 | E admin@presidiofc.com.au
W www.presidiogroup.com.au

Cyber Security Policy

Policy brief & purpose

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks, and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors, and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Client Relationship Management (CRM) system data

All employees are obliged to protect this data. We provide our employees instructions on how to avoid security breaches.

Our CRM, Mercury, is provided via our Broking Aggregator, Connective Group Pty Ltd ACN 162 397 060. Connective's Information Technology (IT) Certificate is provided to us annually and attached to our Cyber Security Policy for reference.

Protect personal and company devices

Our employees use their devices to access company emails or accounts, and keep both their personal and company-issued computer, tablet and mobile phones secure. They do this by:

- Keeping all devices password-protected.
- Antivirus software.
- They do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees not to access internal systems and accounts from other people's devices or lending their own devices to others.

We employ professional and independent IT Consultants to monitor and install:

- Managed Cloud Web Protection
- Managed Cloud Spam Filtering
- Managed Cloud Antivirus

Keep emails safe

Emails often host scams and malicious software. To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")

- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they will refer this to Management prior to downloading any links.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Our passwords are secure so that they won't be easily hacked, and they also remain secret. For this reason, we instruct our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords every two months.

We also use the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

Transfer data securely

Transferring data introduces security risk. Employees will:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request the services of our IT Consultants for assistance.
- Share confidential data over the company network system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches, and hacking attempts

Our employees will report perceived attacks, suspicious emails, or phishing attempts as soon as possible to our IT Consultants. Our IT Consultants will investigate promptly and resolve the issue.

Additional measures

To reduce the likelihood of security breaches, we instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to Management.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.

Our IT Consultants:

- Install firewalls, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy provision as other employees do.

Our company will have all physical and digital shields to protect information.

Working remotely

From time to time, our employees may work remotely as part of our Flexibility Program in creating and encouraging a Work-Life Balance. When working remotely, employees must follow this policy's instructions too. Since employees are accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards, and settings; and ensure that their private network is secure.

We encourage them to seek advice from Management.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: we may issue a verbal warning and train the employee on security.
- Intentional, repeated, or large scale breaches (which cause severe financial or other damage): we will invoke more severe disciplinary action up to and including termination.

We will examine each incident on a case-by-case basis.
Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners, to our employees and contractors, should feel that their data is safe. The only way to gain trust is to proactively protect our systems and databases. We will always do our utmost by being vigilant and keeping cyber security at the forefront.

Professional Indemnity (PI) Insurance

Policy Extension

Our PI insurance includes Cyber Liability Endorsement. We may provide Policy information to you upon request.

connective

24 February 2019

Dear Connective member,

RE: IT Security Certificate

As a Credit Licensee, you would be aware that you have an obligation to ensure the integrity of your information systems. Part of this involves an annual review of your system against a number of parameters set out in ASIC Regulatory Guide 205.

As a large part of your information platform may involve Connective's system, Mercury, we wish to assist you in your compliance efforts by providing you with the following certification as to your own system's integrity.

We have performed our system review and determined that:

1. Connective's information security practices remain consistent with world class good practices;
2. Our systems remain current and relevant to the finance broking context;
3. Our disaster recovery and business continuity practices continue to be commensurate with AS/NZS 5050:2010;
4. Hardware continues to be upgraded to support the numbers of users on the system;
5. Such reviews and upgrades include a consideration of system response times and outage history.
6. In reaching this determination, we have also considered the relevance of system-related complaints received through our help desk.

To this end, we certify that you are entitled to rely on our system integrity for the portion of your business platform that relies on our systems to meet your own (Australian Credit Licence) obligations.

Glenn Lees
Connective CEO