Cyber Security Policy

Policy brief & purpose

Our Cyber Security Policy outlines our business' guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store, transfer and manage information, the more vulnerable we become to security breaches. Human error, hacker attacks and system vulnerabilities and malfunctions can cause great financial damage and may jeopardise our business' reputation and client data security.

For these reasons, we have created this policy to implement various security measures and create guiding principles/rules for us all to follow to help mitigate cyber security risks.

Scope

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

In addition to general guidelines, other relevant policies include:

- Data Protection Policy
- Social Media Policy
- Email Usage Policy
- Internet Usage Policy.

Policy elements

Personally identifiable information

Personally identifiable information is valuable. Types of personal information that we aim to protect, and which is more likely to cause an individual serious harm if compromised, includes:

- Sensitive information such as information about an individual's health.
- Documents commonly used for identity fraud, such as driver's licence or Medicare card details
- Financial information.

Common examples are:

- Information relating to clients/partners/vendors.
- Client lists (existing and prospective).
- Unpublished financial information.

Anyone with access to this information is obliged to protect it. In this policy, we detail how we seek to avoid security breaches.

When to use password protection

The following documents (and potentially others) will contain personal client information, which is either financial, sensitive or identifying in nature and therefore must be password protected before sending electronically:

- Statements of Advice (SoAs).
- Recommendations of Advice (RoAs).
- Fact Finds.
- Application forms (prefilled, signed).
- Client statements.

- Client identification documents used for certification.
- Medical or underwriting information.
- Any other document or record that contains a client's bank account, Tax File Number, Date of Birth or other identifying material.

Documents that **do not** need to be password protected unless they contain personal client information, which is either financial, sensitive or identifying in nature.

Protect personal and business-issued devices

When digital devices are used to access business emails or accounts, they introduce a security risk. You are required to keep both your personal and business-issued computers, tablets and mobile phones secure. To do this you should:

- Keep all devices password protected. Use of **two-factor authentication** on systems and applications (including XPLAN) and a **password manager** (such as Lastpass) is to be current on all devices.
- Choose and upgrade to a competent, market-renowned antivirus with auto-update enabled. Antivirus or security applications endorsed by our business must not be deactivated at any time.
- Ensure you do not leave devices exposed or unattended. Lock the screen when you walk away from the device and apply a password reset timer after a MINIMUM of 10 minutes.
- Install security updates on browsers and systems monthly, or as soon as updates are available.
- Log into business accounts and systems through secure and private networks only. Do not use public Wi-Fi or computers to access business emails or to access the business network. Instead, use approved devices and personal hotspots / VPNs from your mobile.
- Avoid accessing internal systems and accounts from other people's devices or lending your devices to others.

Keep emails safe

The preferred business email account tool is **Microsoft Outlook,** which is to be protected by two-factor authentication. Emails often host scams and malicious software (e.g. worms).

To avoid virus infection or data theft, we recommend you:

- 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 addresses and names of people you receive a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, an excessive number of exclamation marks).
- Delete emails which contain personal information and save them to XPLAN, an approved cloud storage solution (i.e. Microsoft OneDrive/SharePoint.Dropbox).
- Delete emails received in error and contact the sender to ensure the correct email address is used in the future.
- Never access work emails through a personal email system such as Gmail, Hotmail or Yahoo. Business or enterprise versions of email gateways are acceptable.

If you are not sure that an email you have received is safe, you should stop and seek guidance before opening it or clicking on any links.

Our preferred method of accessing documentation

Our preference is to access all information directly via an adviser's system, for which we have been provided with a login that is protected by two-factor authentication. This may include **Microsoft OneDrive/ SharePoint/GoogleDrive/Dropbox (**depending on the business that we are working with). It may also include

access directly into an adviser's CRM (such as XPLAN, AdviserLogic, MidWinter, Xeppo, etc), for which we have also been provided with a login that is protected by two-factor authentication.

Sending documents by email

We should very rarely send documents to an adviser or service provider via email. When sending documents by email:

- Any documents containing sensitive information are to be protected using the preferred program of **7-Zip**. The password is to be consistently generated for the client and will be the initials of the client followed by the month and year (e.g. Gary Smith's review in October 2020 would be sent a password of gs1020). This password must only be communicated to the recipient via text message and then via a phone call if necessary (never via email).
- **Unencrypted copies** of the files are to be held in XPLAN for auditing and record-keeping requirements (i.e. you should not password protect files held in XPLAN).
- The **body of the email and/or subject line** must not contain personal client information, which is either financial, sensitive or of an identifying nature.

If personal client information is received by error, that information should be destroyed and/or the email should be deleted. The recipient should contact the email sender so they can correct the email address to send future emails to.

Capacity Connection **does not accept or implement transaction requests**. They will be ignored and a phone call place to alert that such a request has been received.

Other methods of sending documents

You can send documents using share drives like **Microsoft OneDrive/SharePoint/GoogleDrive/Dropbox (**depends on the business that we are working with).

You can send documents via Microsoft OneDrive either with or without password protection:

- Where the document is sent **with** password protection, the password can be shared with the client by calling or texting (not email), so that the client/recipient can open the document.
- Where the document is sent **without** password protection, a code is sent to the client in a separate email. This is the only exception allowable where a password may be sent by email.

If you are sending an email with a protected attachment to a recipient with a **group email address** (e.g. assist@capacityconnection.com.au) you may wish to include a hint in the body of the email or suggest that the recipient call you to obtain the password. Verify the caller before providing the password.

Internally sharing documents must be completed via SharePoint or Dropbox. An email prompt for a work colleague to review the document is permitted.

When submitting client documents to **product providers**, this should be completed via secure e-post portals where available.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they can't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Use the LastPass password manager program to manage passwords for all platforms that belong to Capacity Connection (this is mandatory). You should create a secure password for the tool itself using the guidelines below.
    - We may also be asked to use alternate password managers such as Keeper. This is okay, as long as it is linked to our team inbox and two-factor authentication has been established. Please confirm with the General Manager.

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid using password information that can be easily guessed (e.g. birthdays).
- Remember passwords instead of writing them down. If you need to write down your passwords, you are obliged to keep the paper or digital document confidential and destroy it when your work is done.
- Exchange credentials only when necessary. When exchanging them in person isn't possible, you should use the phone instead of email, and only if you recognise the person you are talking to.
- Change passwords every two months.
- Update all passwords in the password manager program in the event of an employee departing the business.

Two-factor authentication

Two-factor authentication is to be enabled on all data-sensitive applications. This includes email and XPLAN.

- Two-factor on XPLAN is to utilise the Google Authenticator app.
- Two-factor on Outlook is to utilise the Microsoft Authenticator app.
- Two-factor on Lastpass password manager requires an authenticator to be activated.

Transfer data securely

Transferring data introduces security risk. You must:

- Use **Microsoft OneDrive/SharePoint/Dropbox** to transfer documents within the business. Reports must not be transferred via email to reduce the risk of data breaches.
- Avoid transferring sensitive data (e.g. client information, employee records) to other devices or accounts unless absolutely necessary. When a **mass transfer** of such data is needed, ask for help from the General Manager.
- Share confidential data over the **business' network** via Microsoft OneDrive/SharePoint/Dropbox 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 in place.
- Report any **suspected or actual** attacks, suspicious emails or phishing attempts as soon as possible to our General Manager. Our General Manager/IT support team must investigate promptly, resolve the issue and send a business-wide alert when necessary.

Additional measures

To reduce the likelihood of security breaches, you are advised to:

- Turn off your screens and lock your devices when leaving your desk and apply a 10 minute timeout setting. You must manually lock the screen when moving away from your equipment.
- Report stolen or damaged equipment as soon as possible to the General Manager.
- Change all account passwords immediately if a device is lost or stolen.
- Report any perceived threats or possible security weaknesses in business systems.
- Refrain from downloading suspicious, unauthorised or illegal software on business-issued equipment.
- Avoid accessing suspicious websites.

We also expect business employees to comply with our Social Media Usage Policy and Internet Usage Policy.

Our General Manager and/or IT support should:

- Install firewalls, up-to-date antivirus software, anti-malware software and access authentication systems.
- Arrange for cyber security training for all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy's provisions.

Remote employees

Remote employees/external contractors etc. must also follow this policy. As remote users will be accessing our business' accounts and systems externally, they are obliged to use two-factor authentication, follow all data encryption, protection standards and settings, and ensure their private network is secure.

Disciplinary action

We expect all business employees to follow this policy. Employees who don't follow this policy and/or cause security breaches may face disciplinary action, such as:

- 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 may 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 may face disciplinary action, even if their behaviour hasn't resulted in a security breach.

Reporting of incidents

When an employee suspects a cyber incident may have occurred, or an incident is detected, immediate action is required. Please refer to the Adviser Cybersecurity Incident Response Plan for detailed action that must be undertaken as soon as an incident is suspected or detected. A copy can be found on our Licensee's adviser intranet site.

Take security seriously

Everyone, from our clients and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Data Protection Policy

Policy brief & purpose

Our Data Protection Policy covers our commitment to treat the information of our employees, our advisers and their clients and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect for an individual's rights.

Scope

This policy covers all parties (employees, job candidates, clients, suppliers etc.) who provide any amount of information to us.

Who is bound by our Data Protection Policy?

Anyone employed by, or contracted to, our business and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity who has access to our data (i.e AS White Global) are also covered by this policy. Generally, our policy covers anyone we collaborate with, or who acts on our behalf and may need access to data.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that may make a person identifiable, such as:

- Names and addresses
- Usernames and passwords
- Photographs
- Social security numbers
- Financial data etc.

Our business collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

We will ensure our data is:

- Accurate and kept up to date.
- Collected fairly and for lawful purposes only.
- Processed by the business within its legal and moral boundaries.
- Protected against any unauthorised or illegal access by internal or external parties.

We will ensure our data is not:

- Communicated informally.
- Stored for more than a specified amount of time.
- Transferred to organisations, states or countries that do not have adequate data protection policies.
- Distributed to any party other than the ones agreed to by the data's owner (exempting legitimate requests from law enforcement authorities).

In addition to ways of handling the data, our business has direct obligations towards people to whom the data belongs. Specifically, we must:

- Inform people what data of theirs is collected
- Inform people about how we will process their data
- Inform people about who has access to their information
- Have provisions for cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases.

Actions

To exercise data protection, we're committed to:

- Regular / daily data backups by appropriate means.
- Restricting and monitoring access to sensitive data.
- Developing and maintaining transparent data collection procedures.
- Training employees in online privacy and security measures.
- Building secure networks to protect online data from cyber attacks.
- Establishing and maintaining clear procedures for reporting privacy breaches or data misuse.
- Establishing and maintaining data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation procedures/controls etc.).

Business employees must not use public computers or public Wi-Fi to access their work email account. If you are travelling or going out of the office for meetings and require Wi-Fi, use your mobile phone’s personal hotspot or VPN tools.

Two-factor authentication is required for all system access that holds client information, including XPLAN and Microsoft Outlook (as well as the rest of the Office 365 suite, including Sharepoint).

Disciplinary consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines may invoke disciplinary and possible legal action.

Social Media Policy

Policy brief & purpose

Our Social Media Policy provides a framework for using social media. Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether you are handling our business social media account or using one of your own, you should remain productive and avoid damaging our business in any way.

This policy provides practical advice to avoid issues that might arise by the careless use of social media in the workplace. Refer to the IOOF Marketing Standard on the Licensee's adviser intranet site for further guidance.

Scope

We expect all business employees to follow this policy. "Social media" refers to a variety of online communities like blogs, social networks, chat rooms and forums – not just platforms like Facebook or Twitter.

This policy is built around two elements:

1. Using personal social media at work.
2. Representing our business through social media.

Policy elements

Using personal social media

We do not allow our employees to access their personal social media accounts at work using business-issued devices. You may access your personal accounts on breaks during work hours, but we expect you to act responsibly and ensure your productivity isn't affected.

We ask you to be careful when posting on social media. We can't restrict what you post on social media, but we expect you to adhere to our confidentiality policies at all times. We also caution you to avoid violating our anti-harassment policies or posting something that might make your collaboration with other employees more difficult (e.g. hate speech against groups which colleagues belong to).

We advise our employees to:

- **Ensure others know that your personal account or statements don't represent our business.** You shouldn't state or imply that your personal opinions and content are authorised or endorsed by the business. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.
- **Avoid sharing intellectual property** like trademarks on a personal account, without approval as confidentiality policies and laws always apply.
- **Avoid any defamatory, offensive or derogatory content.** It may be considered as a violation of our business' anti-harassment policy, if directed towards colleagues, clients or partners.

Representing our business

Some employees may represent our business by handling our social media accounts or speaking on our behalf. When you're utilising our social media account, we expect you to act carefully and responsibly to protect our image and reputation. You should:

- **Be respectful, polite and patient,** when engaging in conversations on our business' behalf. You should be extra careful when making declarations or promises towards clients and stakeholders.

- **Avoid speaking on matters outside your field of expertise** when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility.
- **Follow our** confidentiality and data protection policies and observe laws on copyright, trademarks, plagiarism, and fair use.
- **Inform our business** when you're about to share any major-impact content.
- **Avoid deleting or ignoring comments** for no reason. We should listen and reply to criticism.
- **Never post discriminatory, offensive or libellous** content or commentary.
- **Correct or remove** any misleading or false content as quickly as possible.

Disciplinary consequences

We will monitor all social media postings on our business accounts. We may have to take disciplinary action leading up to and including termination if business employees do not follow this policy's guidelines. Examples of non-conformity with the social media policy include, but are not limited to:

- Disregarding job responsibilities and deadlines to use social media at work.
- Disclosing confidential information through personal or business accounts.
- Directing offensive comments towards other members of the online community.

If you violate this policy inadvertently, you may receive a reprimand. Following any reprimands, any further violations may result in stricter disciplinary action.

Email Usage Policy

Policy brief & purpose

Our Email Usage Policy helps business employees use their work email addresses appropriately. Our goal is to protect our confidential data from breaches and safeguard our reputation and business property.

Scope

This policy applies to all business employees, vendors and partners who are assigned (or given access to) a work email address. This email address may be assigned to an individual (e.g. employeename@capacityconnection.com.au)

Policy elements

Employees should use their work email primarily for work-related purposes. However, we want to provide employees with some freedom to use their work email for personal reasons. Below are examples of what constitutes appropriate and inappropriate use.

Inappropriate use of your work email

Whenever you use your work email address you represent our business. You must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services
- Send unauthorised marketing content or solicitation emails
- Register for a competitor's services, unless authorised
- Send insulting or discriminatory messages and content
- Intentionally spam other people's emails, including their co-workers.

Our business has the right to monitor work email accounts.

Appropriate use of work email

Employees are allowed to use their work email for work-related purposes without limitations. For example, you can use your email to:

- Communicate with current or prospective clients and partners.
- Log in to purchased software you have legitimate access to.
- Give your email address to people you meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help you with your job or professional growth.

Personal use

Business employees are allowed to use their work email for some personal reasons. For example, you can use your work email to:

- Register for classes or catchups
- Send emails to friends and family, as long as you don't spam or disclose confidential information.

Business employees must adhere to this policy at all times, in addition to our confidentiality and data protection policies.

Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment. You must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays).
- Remember passwords instead of writing them down and keep them secret.
- Change your email password every two months.

You should always be vigilant to catch emails that carry malware or phishing attempts. You should:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.").
- Be suspicious of clickbait titles.
- Check email addresses and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).
- Delete 'deleted' emails in your deleted folders (trash), if your email account is hacked, cyber-criminals can access not only current emails, but also deleted emails.
- Call clients to confirm bank account changes or unusual account amendment requests such as large withdrawals or out of character requests.
- Keep your anti-malware programs updated.

If you aren't sure that an email you have received is safe, you should check with our General Manager.

Email signature

We encourage Business employees to create an email signature that shows professionalism and represents our Business well. Everyone represents our business to clients and stakeholders and should pay special attention to how they close emails.

Below is a template of an acceptable email signature:
[Employee Name]
[Employee Title]
[Phone number] | [Business Address]

Employees may also include professional images, business logos and work-related videos and links in email signatures. If you are unsure how to do so, you can ask for help from our General Manager. The General Manager may also direct the inclusion of images that reminder our advisers and clients not to click on

suspicious emails and the inclusion of additional images around various holidays to advise of extended due dates.

All email signatures are to include the following text:
This email message and any accompanying attachments may contain information that is confidential. If you are not the intended recipient, do not read, use, distribute or copy this message or attachments. If you have received this message in error, please notify the sender immediately and delete. Capacity Connection does not accept liability for any virus caused by this message.

Disciplinary action

Business employees who don't adhere to the present policy may face disciplinary action up to and including termination. Example reasons for termination are:

- Using a work email address to send confidential data without authorisation.
- Sending offensive or inappropriate emails to our clients, colleagues or partners.
- Using a work email for an illegal activity.

Internet Usage Policy

Policy brief & purpose

Our internet usage policy outlines our guidelines for using our business internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our business' legality and reputation.

Scope

This internet usage policy applies to all our business employees, contractors, volunteers and partners (including AS White) who access our network and computers.

Policy elements

What is appropriate internet usage?

Business employees are advised to use our business internet connection for the following reasons:

- To complete your job duties.
- To seek out information you can use to improve your work.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet.

Any use of our network and connection must follow our confidentiality and data protection policies. You should:

- Keep your passwords secret at all times.
- Log into your work accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

What is inappropriate internet usage?

You must not use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorised recipients
- Invade another person's privacy and sensitive information.

- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorised or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If you are unsure if a file is safe, you should not open it.

We won't assume any responsibility if employees' devices are infected by malicious software, or if your personal data is compromised as a result of inappropriate use.

Business-issued equipment

We expect employees to respect and protect our work equipment including business-issued phones, laptops, tablets and any other electronic equipment that belongs to our business.

We advise our employees that you should lock your offices where your devices reside, when you are not using them. You are responsible for your equipment whenever you take it out of your workplace.

Our business installs antivirus and disk encryption software on business-issued computers. You must not deactivate or configure settings and firewalls.

Work email accounts

You can use your work email account for both work-related and personal purposes, as long as you don't violate this policy's rules. You should not use your work email to:

- Register for illegal, unsafe, disreputable, or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorised advertisements or solicitation emails.
- Sign up for a competitor's services unless authorised.

We have the right to monitor work email accounts. We also have the right to monitor websites employees visit on our equipment and devices.

Disciplinary action

Business employees who don't comply with this internet usage policy may face disciplinary action. Serious violations may provide cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our equipment to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our clients, colleagues or partners.