Cyber Security Policy

Karen Barclay Virtual PA is aware of the risk that cyber-attack poses to its business, and to the businesses of our clients. In particular, the risk of confidential or sensitive client information, both in hard copy and stored electronically. All team members, including employees and contractors, are required to adhere to this Cyber Security Policy. Questions about the Policy should be directed to Karen Barclay, kbarclay@karenbarclay-vpa.com or 0432 015 716.

Your Responsibilities

Effective security is a team effort requiring the participation and support of every team member. It is your responsibility to know and follow these guidelines.

Anti-Virus Software

We use industry-standard anti-virus software to protect devices used to record and store confidential and private information.

Current protection is with BitDefender Zero Gravity Zone. Settings must be configured by our IT Contractor, TechSeek, to help prevent successful hacks and ransomware attacks.

All team members are to use only the IT equipment provided by Karen Barclay Virtual PA.

Password Policy

Strong passwords are key to ensuring security on devices, networks, and software. We enforce a strict Cryptographic password protocol with compulsory password manager use.

The current protocol is a minimum of eight (8) characters, including at least one upper case letter, lower case letter, number, and symbol. No use of dictionary words, including compound words or combinations. No use of names, locations, or addresses. Avoid patterns, eg. sequential numbers or letters.

All team members need to be aware of their personal responsibilities for following the password policy.

Wherever possible, systems must be configured to enforce the password policy, eg. computer user accounts, Office 365, etc. and to enforce an account lockout policy, eg. three (3) failed attempts that will cause a user account to be locked.

Passwords must be changed immediately if a compromise is suspected.

Password sharing must be kept to an absolute minimum. Karen Barclay Virtual PA uses password management software, Keeper Vault, to share passwords, where required. All team members will have their own accounts. Passwords will only be shared using the authorised software, never by email or other insecure methods, such as via text message. Passwords must only be stored in the authorised management software and must never be written down or recorded elsewhere, such as in a hard copy document, such as a notebook, post-it-note, a Word document, or in an email.

Team members may choose to use a secure password generator within Keeper Vault to generate passwords that meet the protocol.

Email Filtering

Karen Barclay Virtual PA uses Microsoft Office 365 email client, which incorporates multiple spam filters.

To maximise these protections, our IT Contractor, TechSeek will configure the protection settings to best meet the needs of Karen Barclay Virtual PA.

Web Traffic Filtering

Web traffic filtering is turned on for the office network.

Staff should ensure that web filtering is turned on if they are using a shared connection, such as a coworking space.

Bank Details

Where any bank details are provided by email in text format, ie. not PDF, such as an invoice or on a website, these are to be confirmed with the payee by phone before payments are made.

Two-Factor Authentication

Two-factor authentication, where available, is turned on for software programs used by Karen Barclay Virtual PA and its clients.

Users need an authentication app such as Google Authenticator or Microsoft Authenticator to sign in.

Software Updates

Karen Barclay Virtual PA use Windows 10 computers. It is essential that all software updates are performed in a timely manner, to minimise vulnerability to cyber-attack. All devices should be configured to automatically install updates, except over metered connections. If you are using a metered connection for an extended period, manually check and perform updates every week.

All staff must ensure that their devices and software are updated regularly to protect against the risk of cyber-attack.

Removeable Hardware

Karen Barclay Virtual PA does not use removable media to store or transfer information. We use OneDrive, Google Drive, or DropBox as file storage for the business. Files are stored on these cloud-based servers. Information is exchanged using protected mechanisms.

Use of removable hardware such as USB sticks is forbidden as they are vulnerable to being lost or stolen or introducing malware and viruses into the business.

Office Wireless Network

The office wireless network is a private internet connection. Accordingly, other members of the network cannot access your files.

It is preferable when working remotely that staff use a private internet connection.

Public Wi-Fi

A public Wi-Fi hotspot isn't required by law to be secure from potential online threats, so should be treated as unsecured, unless the operator of the hotspot states otherwise. Users

can normally find this information in the security clause of the 'terms of use' that they typically must agree to before using a public Wi-Fi hotspot.

A public Wi-Fi hotspot that is password protected and uses Wi-Fi Protected Access 2 (WPA2) encryption and the 802.1x Standard for authentication, which is currently regarded as industry best practice, is considered secure.

Staff should avoid the use of public Wi-Fi hotspots. The office wireless network should be always used in the office, or if the network is unavailable, the staff member's personal hotspot may be used, and only if it is password protected. The next best alternative is to use a secured public hotspot.

Staff should avoid using an unsecured public Wi-Fi hotspot unless absolutely necessary and, in that case, any use should be limited to minimise the amount of confidential information exposed to the unsecured network, eg. turn off file sharing and location services.

Laptop Security

Work-related files should never be stored locally, except for syncing purposes. All work-related files are stored in the cloud-based storage provider, either the client's or Karen Barclay Virtual PA.

Back-Up

As all data is stored in the cloud-based storage provider of either the client or Karen Barclay Virtual PA, which has adequate protocols for data encryption in transit and at rest, it is not considered necessary at this point to add further back-up protocols. To do so may expose the business to additional data breach risk, eg. hacking of hard drive devices.

Karen Barclay Virtual PA has two SharePoint sites which are backed up to a Melbourne-based third-party data centre, AFI. Automated and fully encrypted backups are performed three times per day.

Training and Awareness

As part of the onboarding process, new staff are required to complete mandatory cyber security training.

Cyber Insurance

Karen Barclay Virtual PA has purchased a Cyber Risk Insurance Policy that provides us with cyber risk cover. This Cyber Risk Policy provides protection from losses to a limit of $250,000 for each claim. It provides cover for Network Security Liability, Privacy Liability, and Management Liability.

Cyber Risk Assessment

At the end of every financial year, Karen Barclay will review this policy, in collaboration with TechSeek, assess the business' exposure to cyber risk and update our policies and practices to address any change.

Changes to this Policy

Karen Barclay Virtual PA may update this policy from time to time to record our updated security procedures. This Cyber Security Policy was last updated in August 2022.