| Name of Procedure | Cyber Security Protection Procedure |
|---|---|
| Policy Statement | This process covers the security of internal and external IP for devices and cloud-based information. |
| Frequency of Use | Ongoing |

## Purpose

Statement of purpose:

- To ensure that all intellectual property, both internal and external is protected against loss, fraud and cyber attacks.

## Policy:

- It is our policy to have a system in place whereby each contractor takes the steps in this process to protect their devices and subsequent intellectual property.
- This is necessary to minimize the risk to both our clients, Your VA as a company, and contractors as individuals.

## Responsibility

Each individual contractor is responsible for their own cyber security and that of clients' they are responsible for.

---

- **Step 1 Secure Password Vault**
- **Step 2 You and Your Devices**
- **Step 3 Cloud Systems**
- **Step 4 Monthly Checklist**
- **Step 5 Accountability**
- **Step 6 Client Authorisation**

---

## Procedure

- **Step 1 Secure Password Vault**

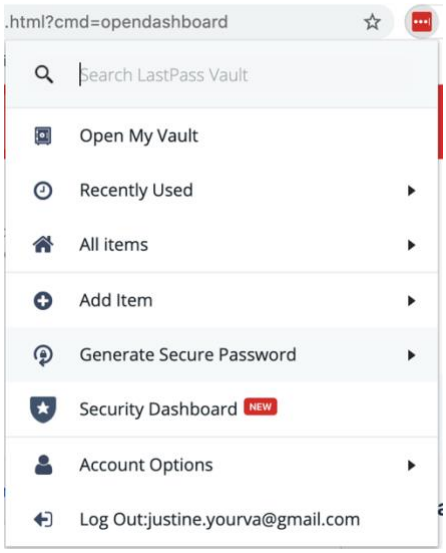
  Use a secure password vault for all online logins, this applies to internal (Your VA) and external (client) logins. We use LastPass for all internal logins however a client may use a different tool in which case we'd also create an account in the same tool for sharing logins specific to that client. Follow the steps below to ensure best practice. Where you are using an application different to LastPass, follow their recommendations for maintenance.

1. Where sharing login with a team member or client, check the 'allow recipient to view password' box. Where sharing to an external contact leave this box unselected.

2. No logins (client or Your VA) will be saved in any browser.

3. Don't use variations of the same password for your logins.

4. Generate a secure password for your LastPass account by accessing their *generate secure password* option from the Chrome extension (or your LastPass Vault). See screenshot using the Chrome Extension.




5. *At least monthly*, perform *the Security Dashboard* audit to ensure your score is over 80%.

6. Turn on Two-Factor Authentication:
Protect your account with two-factor authentication. Even if your master password were somehow stolen, the thief would still need the two-factor authentication data to access your account.

7. Enable a Security Email Address:
With the security email address feature in LastPass, you can enable a secondary email address solely for LastPass security alerts. Depending on your settings, these alerts may occasionally be sent with details of password or username changes, and important account updates. If you're worried about your primary email address ever being compromised, the secondary email address ensures you have a dedicated inbox for LastPass that no one else should know about.

8. Link a Personal Account:
A password manager like LastPass can help protect you both at home and in the workplace. But if you're using LastPass at work, it's a good idea to keep personal and business separate. For LastPass business accounts, an admin can delete an account at any time, which would also delete any passwords stored in the vault.

That's why we recommend always creating a separate, personal LastPass vault. You can then link the personal vault to the business vault, giving you convenient access to both throughout the workday. They remain separate and private, though, and the admin can't see what's in your personal vault (though what you do on company devices, including the sites you access, is likely still being monitored).

9. Relating to point 8 above, we recommend setting up a Your VA gmail account (i.e. justine.yourva@gmail.com). You can use this gmail for your LastPass account as well as other online tools you use as a contractor. This also makes it easy for us as a team to share access to Google Drive, Dropbox and other cloud based tools.

- **Step 2 You and Your Devices**

1. You must have an antivirus protection installed on your computer. AVG has a free version and works on all platforms.
2. Keep all operating systems, software and apps updated by turning on auto-updates. This ensures your applications have the latest security protection possible.
3. Shut down your laptop/desktop at the end of the day.
4. Don't click on a link in a suspicious email, if you have concerns contact justine@yourva.co.nz with a screenshot of the email.
5. If you should lose or sell a device, erase information on the device as follows:
   a. iPhone
   b. Andriod
   c. PC
   d. Mac

- **Step 3 Cloud Systems**

1. Once a month log out of *all devices* for:
   a. Google
   b. Facebook
   c. Gmail
   d. Dropbox (profile pic – settings – security)
   e. OneDrive
2. Check that two-factor authentication is configured for all accounts where possible.
3. All documents and information must be stored either in Dropbox, Drive or SharePoint (depending on the client) and shared via LastPass with Justine.yourva@gmail.com so we have a 'master' access to all our client's IP. No IP is to be saved on personal computers.

- **Step 4 Monthly Checklist**
  Each month perform the following tasks *for yourself, and clients* you are responsible for:

  - Change your LastPass (or similar) master password
  - Perform the Security Dashboard Audit in LastPass (or similar, see step 1)
  - Log out of all devices (see step 3)
  - Change passwords for apps or software you use most often (using LastPass to suggest password)
  - Ensure *find my phone* is turned on (if applicable)
  - Ensure you have logins for your (as applicable) iCloud, Google, Microsoft, LastPass and/or other critical logins stored somewhere other than your devices in case of emergency.

- **Step 5 Accountability**
  Each contractor is responsible for adhering to this SOP both on their own devices, and performing the same steps above for clients they are responsible for.

  This SOP is signed by each contractor agreeing to this process:
  - During onboarding
  - When accepted as a permanent contractor (month 2)
  - Annually

  These signed SOP's are filed in Google Drive – Contractors – [Contractor Name]

- **Step 6 Client Authorisation**
  Because this process directly affects our clients, in order to protect their IP they will sign this SOP agreeing to our execution of the monthly checklist (step 4) on their behalf. *If a client has their own policy in place, please follow that where it differs from this document.*

## Authorisation

| Contractor Name | Date | Signed |
|---|---|---|
| | [onboarded] | |
| | [permanent – mth 2] | |
| | [annual]<br>29-11-2020 | |

## Version Control

| | | | |
|---|---|---|---|
| Author: | | Approved: | |
| Version: | | Date | |