AXADRA VENTURES

CHECKLIST FOR KEEPING OUR PARTNERS AND CLIENTS DATA SECURE

WHAT IS DATA PRIVACY AND SECURITY?

Collecting data and information about our Partners and Clients allows us to analyze important information, make informed decisions and gain access to web-based tools among others. **It also comes with a responsibility.**

We have to ensure we practice safe, ethical, and effective management of personal and non-personal data that we use for operational purposes.

When we safeguard our partner's and clients' data, we protect our organization.
In particular, we need to protect Personal Identifiable Information or PIIs and credentials. Which are part of our day-to-day operations.

☐ PERSONAL IDENTIFIABLE INFORMATION OR PIIS.

These are information that directly identifies an individual

- Name
- Address
- Social Security Number
- Telephone Number
- Email address

These are information that intends to identify specific individuals in conjunction with other data elements

- Gender
- Race
- Birth Date
- Geographic Indicator

☐ CREDENTIALS

- Username
- Emails
- Passwords
- Multi-factor authentication details like security questions and phone numbers

USE THE CHECKLIST BELOW AND BECOME A BETTER STEWARD OF OUR CLIENTS' AND PARTNERS' DATA:

DATA SECURITY CHECKLIST

- [ ] **1. I have identified all sensitive data and classified it.**

  You need to know precisely what types of data you have access to. Being aware that you have this information allows you to protect them effectively. Examples of sensitive data are personal information, credit card details, website credentials, web-based software credentials.

- [ ] **2. I monitor access to sensitive data**

  We need to offer the right access control to the right user. This will ensure that the right user is using data. An example of this is access to the data stored in Google Sheets, Google Docs, Google Slides, Google Drives, and other cloud storage. Only share access with authorized team members. The most common levels of access we have are Editor, View, and Comment access. Avoid putting the sharing settings to 'Anyone Can View' or 'Anyone that has a Link'

- [ ] **3. I Keep my Devices Secure**

  Physical security is often overlooked when discussing data security best practices. You can start by locking down your workstations -- even at home. This also applies to the gadgets that you use for work. Always keep your smartphones, tablets, or laptops in a secure place when not in use. Minimize the usage of these gadgets in a public place and avoid using public wifi. Never leave your laptops unattended while in a public place like coffee shops, co-working spaces, or lounges. Theft or loss of these gadgets can lead to serious data breaches

- [ ] **4. I use end-point security systems to protect my data.**

  It is a must to install anti-virus software, anti-spyware, anti-malware, pop-up blockers, and firewalls (place the items in bullets/list, accompanied by simple icons). If these are installed, see if they are regularly updated.

DATA SECURITY CHECKLIST

- [ ] **1. I have enabled multi-factor authentication**

  It is considered one of the most advanced and proven forms of data protection strategies. If available, enable two-factor authentication on your credentials and tools. This means that even if our passwords are compromised, we have another layer of security such as one-time passwords on mobile phones, fingerprints, or security questions.

- [ ] **2. I have Free Security Tools Installed like VPNs and Password Managers**

  This includes encrypted storage solutions, password managers, and VPNs. These small tools can dramatically decrease your vulnerability to attack and are easy to use and install. Instead of keeping your username and passwords on a notepad, word document, or sticky note, consider using password managers

- [ ] **3. I Have Strong Passwords.**

  Strong passwords are at least 12 characters long and contain a combination of upper and lower case letters, numbers, and if possible, symbols.

- [ ] **4. I use end-point security systems to protect my data.**

  Refrain from sharing PIIs and Credentials to people that are not members of your unit, brand, or organization.

- [ ] **5. I never tamper with Partners' and Clients' Data.**

  Never carry out unauthorized changes, edits or deletion of our partners' and clients' data. As responsible stewards of data, we must preserve its integrity. Make sure that the information we have access to is correct and accurate at all times.

- [ ] **6. I only visit websites that are secure (HTTPS)**

  The S after the HTTP stands for "Secure," which means the data being sent between your browser and the site you are on is encrypte

7. I don’t click on pop-ups or virus warnings.

These warnings are now called “scareware,” which are fake security alerts telling you to click a link to download software to remove the virus in your computer. The links, however, contain viruses.

8. I have a backup of my files and data.

The threat of ransomware has been growing through phishing e-mails and pop-up ads. Ransomware is when a hacker locks your computer down and threatens to wipe out your data if you don’t pay up. The backup should be placed in company-approved hardware, software, or cloud location.

9. My software is up-to-date.

Software updates are critical for everything from brand new iPhones to ancient PCs because these updates fix security and privacy flaws that leave you vulnerable to hackers.

10. My Firewall is Enabled

Firewalls are network security systems that monitor incoming and outgoing network traffic based on predetermined security rules. Make sure yours is up, and that they stay up.

11. I Share Online Files to Authorized People Securely.

Securely share files with anyone on the web by password protecting them. With a password protecting your PDF or any other file, you can rest assured that the intended recipient only views it.

It is our responsibility as the individual user to protect data to which we have access -- especially personal data.

GREAT JOB! YOU HAVE FINISHED THE CHECKLIST. THE INFORMATION THAT YOU PROCESS IS NOW SAFE AND SECURE.