BEST PRACTICE GUIDE FOR PROTECTING YOUR INFORMATION

WHEN OUTSOURCING TASKS TO VIRTUAL ASSISTANTS IN THE PHILIPPINES

Social Friends™

When working with a Virtual Assistant (VA) in the Philippines from Australia, it's crucial to consider online security measures to protect your business and personal information. Here are some key aspects to focus on:

1. Data Security and Access Control:

There are two primary types of data to consider – commercially sensitive data, which pertains to confidential business information, and personally identifiable data, which includes sensitive information which may be subject to sovereignty regulations.

- **Limit Access:** Provide your VA with access only to the specific systems, applications, and data they need to perform their tasks. Avoid granting them blanket access to all your systems or sensitive information.

- **Use Strong Passwords and Two-Factor Authentication (2FA):** Implement strong, unique passwords for all accounts accessed by you and your VA. Enable 2FA wherever possible to add an extra layer of security.

- **Share Passwords Securely with a Password Manager:** Access to the systems and accounts you need to function properly poses a security risk. To mitigate this risk, use password manager software to safely grant you access to accounts and systems. (Set up 2FA on social platforms – check out the resources the portal on how to do this. All other site access can be managed through password management software like Bitwarden)

- **Secure File Sharing:** Use secure file-sharing platforms that encrypt data transmission and provide access control mechanisms. (Eg: Microsoft OneDrive, Dropbox, GoogleDrive) Avoid sending sensitive information through unencrypted channels like email.

2. Communication Security:

- **Encrypted Communication Channels:** Use encrypted communication channels for all interactions with your VA, such as video conferencing tools or messaging platforms that offer end-to-end encryption. (Eg. Zoom, MS Teams, Google Meet, Whatsapp)

- **Be cautious of Links and Attachments:** Be wary of clicking on suspicious links or opening attachments from unknown senders, including your VA. Verify the sender's authenticity and the legitimacy of the content before interacting.

- **Regular Communication and Awareness:** Maintain regular communication with your VA regarding security protocols and best practices. Educate them about common cyber threats and encourage them to report any suspicious activity promptly.

3. BYOD (BringYour Own Device)Devices:

- **Verify the Virtual Assistant’s Devices Are Secure:** Your VA will use their own computer & mobile devices to access your company system, data, and networks. These devices must be secure, or they are more vulnerable to security threats that could compromise your business's sensitive information. To minimise the risks, it's important to ensure devices are up to date with the latest security patches and use anti-malware software and have the latest Cyber protections enabled where possible.

4. Ongoing Monitoring and Auditing:

- **Regular Password Changes:** Enforce regular password changes for all accounts accessed by you and your VA.

- **Incidence Response:** Security incidents must be reported by your VA immediately so you can assess the risk of data exposure or loss, and how the company will remediate any incidents.

5. Additional Considerations:

- **VPN for RemoteAccess:** If your VA needs remote access to your systems, mandate the use of a company-approved VPN to encrypt their connection and protect data in transit. (Eg. ExpressVPN)

For particularly sensitive business data, you may consider a Virtual System. This solution provides benefits such as restricted website access, prevention of data download to systems outside your country, and activity tracking through tools like Active Track. Social Friends can facilitate the setup and management of this system through our reliable supply partner should you opt for this enhanced security measure.

Both you (the Client) and the Virtual Assistant (VA) have been provided with a comprehensive Best Practices Guide on Data Protection and Cyber Security. It is imperative that each party implements these recommendations diligently to fortify the security of shared information. It's important to note that Social Friends holds no responsibility for the implementation of these measures.

Social Friends
Best Practice Guide for Protecting Your Information When Outsourcing Tasks to Virtual Assistants in the Philippines Version 1
First published & distributed July 2024 by Social Friends
This is proudly a Social Friends Resource

Disclaimer
The content of this workbook is to serve as a general overview of matters of interest and is not intended to be comprehensive, nor does it constitute financial (or other) advice in any way. This workbook is a compilation of one person's ideas, concepts, ideologies, philosophies and opinions. You should carry out your own research and/or seek your own professional advice before acting or relying on any of the information displayed in the resource. The author, and its related entities will not be liable for any loss or damage (financial or otherwise) that may arise out of your improper use, or reliance on, the content in the resource. You accept sole responsibility for the outcomes if you choose to adopt and/or use the ideas, concepts, ideologies, philosophies and opinions within the content of the workbook.