General Guidelines: Cyber Security Do's and Don'ts

This document is created to help educate customers on our platform on the latest Cyber Security best practices to ensure security, confidentiality and integrity of your data.

1. PIN / password security

- Use strong passwords (min 8 alphanumeric characters including a combination of uppercase, lowercase letters and special characters)
- Keep passwords secret, don't write them down
- Change passwords regularly
- Never share passwords or user IDs with anyone

Example of a Good password (for company SESAMi (Singapore) Pte Ltd)

- *SeMi@SG72874*

Example of a Bad password (for company SESAMi (Singapore) Pte Ltd)

- *sesamisingapore*

2. Client browser security

- Clear browser cache often to flush potentially damaging information
- Purge cookies periodically
- Avoid saving login credentials in your browser
- Turn off autofill for any confidential or personal details such as credit card information, etc
- Analyze your browser settings frequently to further protect your privacy

3. Detecting phishing / malicious emails

- Observe proper email usage. Do not send or forward chain emails
- Beware of suspicious emails and attachments. Do not open emails from unknown persons or attachments
- Delete unwanted emails
- Never give personal information via e-mails
- Do not forward company emails to public email services

4. Endpoint security

- Install antivirus solutions and keep the software up to date with the latest anti-virus databases
- Keep OS patches updated
- Ensure firewall is always activated
- Remote access to the company's network has to be encrypted (VPN)