Security Statement

Security standards and measures you can take to ensure online safety.

The ASEAN Startup Portal ("**ASP**"), an initiative by Cradle Fund Sdn Bhd and its partner organizations across ASEAN ("**we**", "**us**", "**our**" or "**ours**"), is strongly dedicated to safeguarding the security, safety, and confidentiality of all Personal Data as defined in the Privacy Statement, stored on www.startup-asean.org ("**Website**").

To achieve this, we implement privacy protection control systems aimed at upholding the highest standards of security and confidentiality across the ASEAN region.

Additionally, we believe you play a vital role as well in safeguarding your Personal Data. This security statement ("**Security Statement**") outlines the actions we take and the steps you can take to help maintain security when using this Website.

Username and Password

To prevent unauthorised access to your profile, every user is required to select a username and password, which provides access to their personal information.

To enhance the security of your account, we suggest choosing a more robust and distinctive username. Below are the username guidelines;

- Minimum 6 alphanumeric characters, maximum 16 characters (upper and lower case)
- Use special characters such as . (full stop) and _ (underscore)
- An example of a strong username: ASEAN_Startup_User123

Tips for Maintaining Account Security:

- Avoid selecting a password that can be easily guessed by others.
- Refrain from using simple words, such as your name, birth date, telephone number, or common dictionary words.
- Commit your password to memory and avoid writing it down.
- Use passwords or PINs when accessing online accounts to safeguard your personal information.
- Sharing your password equates to granting someone permission to use your identity when accessing an account, and it should not be disclosed even if requested by an authorized party.
- Regularly change your password.

Information Protection

Despite our diligent efforts to provide a safe and secure online experience, we cannot oversee the security of the computer you use to access the Website. As an additional security measure, we have implemented an automatic logout function that activates when no activity is detected within a predetermined time limit.

Nevertheless, it is essential to avoid granting anyone the chance to access your account information:

- Make sure your computer is secure, and your online activities are not monitored by others.
- Logout promptly from the Website after updating your profile and before navigating to other websites.
- Refrain from sharing any account-related information through email.
- Turn off the AutoComplete function in your browser to prevent automatic password completion when entering your email address.

To turn AutoComplete "**On**" or "**Off**" in MS Internet Explorer browser:

- Click the "Tools" menu and select "Internet Options.
- Click "Internet Options" to get the "Content" tab.
- From this tab, click the "AutoComplete" button.
- Uncheck "Email address and passwords on forms".

We gather voluntarily provided Personal Data, including but not limited to your name, email address, and profile details, to facilitate communication and deliver requested services or products. With your consent during the data collection on this Website, we may also share startup perks, newsletters, and information with you. Additionally, we might retain and utilize some or all the collected Personal Data for the Purposes as defined in the Privacy Statement.

Data Confidentiality and Data Integrity

To provide a seamless experience, we may display data that you have previously supplied to any private entities, other government agencies, or that has been gathered from third-party sources, as stated on individual entity profiles. This is done to facilitate the flow of information efficiently. If the data is inaccurate or out-of-date, we kindly request you to contact us or update it with the latest information.

Your Personal Data will be kept for the duration of your status as a user of the Website, following the prevailing legal and regulatory guidelines.

We seek your cooperation to submit updated, complete, and accurate information about your company and any related supporting documents, if applicable. This is to facilitate network building for your company or any other entity that uses this Website to identify or search for companies like yours for networking purposes. Please note that inaccurate data submissions may result in a delay in processing or publishing the information on our Website.

Systems security and monitoring

We adopted a combination of the following systems security and monitoring measures:

- Firewall systems, strong data encryption, anti-virus protection and round-the-clock security surveillance systems to detect and prevent any form of illegitimate activities on our network systems.
- Regular security reviews of our systems by our internal system auditor as well as external security experts.
- This Website may contain links to external sites that do not belong to us; the data protection and privacy practices of these external sites may differ from ours. We are not responsible for the content and privacy practices of these other websites and encourage you to consult the privacy notices of those sites. We also reserve the right to object to or disable any link or frame to or from our website.
- We make diligent efforts to collaborate with prominent vendors and manufacturers, staying updated on advancements in information security technology for potential future implementations.

Additionally, as an added precaution on your end, when you have a broadband connected to the Internet (always-on connection), consider installing a personal firewall. At a minimum, power-off your PC when not in use.

Computer virus protection

Computer viruses pose a genuine threat, leading to potential time loss, information loss, repair expenses, and frustration once your computer is infected. It is crucial to have an anti-virus protection programme installed on your computer to mitigate these risks.

We recommend investing in a programme that offers automatic upgrades for your virus protection regularly. If your current virus protection programme lacks this feature, ensure you manually update your virus detection programme monthly or whenever you learn about a new virus to minimize risks. Visit the website of the software provider for these updates. Additionally, exercise caution when opening attachments from others; only do so if you are certain about the source's trustworthiness, as the sender might be unaware of carrying a virus.

Updating your browser

An internet browser provides access and facilitates navigation through numerous information and service resources on the internet, with most computers equipped with a pre-installed browser.

- Keep your browser up to date by installing new versions, as they frequently incorporate additional security features.
- Examine your browser for included safety features, which you can choose to enable or disable based on your preferences.
- Do not install unnecessary extensions or plugins to the web browser.
- Routinely remove cache, cookies, and temporary files from your browser history.
- It is good practice to always check the site certificate before login.

Security Tips

Enhance Your Online Security and Safeguard Your Information

Please take necessary precautions and be on the alert for suspicious email or phone calls asking for your personal account information. Never reveal your account information to anyone.

8 easy ways to protect yourself

1. Do not share your password with friends, relatives or anyone. Keep your password and PIN confidential, only for your use.
2. Change your password frequently. If you think your password has been compromised, contact us to reset your password.
3. Avoid using the "remember password" function to prevent unauthorized access.
4. Refrain from sharing account details via email or phone.
5. Don't open suspicious email attachments.
6. Avoid downloading free programmes. These may incorporate hacker-friendly software.
7. Always log out of the Website immediately after and before visiting other websites.
8. Clear your cache (information stored in your computer memory) each time you log out.

In case of any conflict or inconsistency between the English version of this Security Statement and the translated version in Malay, the English version shall prevail.

If you have any concerns or suspicions regarding emails from us or potential attempts to obtain your account information under false pretenses, please reach out to us at **contact@startup-asean.org**

Last Update: November 2024