AVA INSURANCE BROKERS

91 Bencoolen Street #08-03 Sunshine Plaza Singapore 189652
+65 6535 1828
+65 6535 6898 / +65 6535 6878
enquiries@ava-ins.com

SECURITY POLICY

In the following terms of use, "Us", "We", "Our", "AVA" refers to "AVA Insurance Brokers Pte Ltd" and/or any affiliates, related corporations and branches. "You", "Your", "Yours" refers to the person to whom this policy applies to.

AVA is committed to the security of our customer's transactions and the privacy of their personal data. To fulfil this, the following security measures are in place:

- Physical security of our facilities and information stored in those facilities through biometric authentication.
- The data is stored on a secured server.
- Secure Socket Layer (SSL) encryption technology used for transmitting confidential and/or personal data between the platform and the users.
- User passwords are encrypted in our database.
- Additional verification and second level password are implemented to protect more confidential information.
- Multiple levels of firewall between our internal computer systems and the internet.
- Only valid User ID and Password which identifies each unique user will be allowed to log onto our secure platform. This ensures that only authorized users are admitted.
- As an additional security measure, we may log users out of the session if there is no activity after a certain period.

SECURITY GUIDELINES

Although comprehensive security measures have been taken by us, you must take appropriate security measures to protect you own personal data and transactions. Failure to practice these guidelines mentioned below will expose you to the risk of fraud, malicious code and losses.

In addition, AVA shall in no event be liable to you, our customers or any other party for any damages, loss or expense including without limitation, direct, indirect, special, consequential or punitive damages, or economic loss, loss of profits, loss of opportunity, loss of business or goodwill as a result of, arising from or in connection with the following:

- any breach in security measures that are undertaken by us;
- any system, server or connection failure, modification, suspension, discontinuance, error, omission, interruption, delay in transmission, or computer virus;
- your omission or failure to observe the terms and conditions set out in this Security Policy; or
- your negligence or fault.

91 Bencoolen Street #08-03 Sunshine Plaza Singapore 189652
+65 6535 1828
+65 6535 6898 / +65 6535 6878
enquiries@ava-ins.com

Your negligence or fault can consist of, but is not limited to:

- input errors or misuse of its Internet services;
- negligent handling or sharing of Password;
- leaving a computer unattended during an online session;
- failure to report known incidents of unauthorized account access immediately.

CHECKING FOR AUTHENTICITY AND SECURITY OF WEBSITE

Having both the User ID and Password will help ensure that only permitted users can gain entry into online systems but there is also a need to check for authenticity and security of the website.

You should always check to ensure that the website address changes from http:// to https:// and, look out for a security icon in the form of a yellow lock when authentication and encryption is expected.

You should also ensure that the website you are visiting belongs to AVA. You can do so by comparing the URL displayed in your browser with AVA's URL in the digital certificate. The digital certificate can be found by clicking on the yellow lock icon.

If you notice any discrepancy in the SSL certificate or there is a SSL server certificate warning, please terminate your login session and notify us.

MANAGING YOUR USER ID AND PASSWORD

Your User ID and Password identify you whilst using our services. This includes any additional forms of authentication sent to your email or mobile phone. Below are some guidelines on securely managing your User ID and Password:

- Ensure that your Password is not exposed when you log in to our system.
- Keep your Password confidential at all times and do not divulge it to anyone.
- Do not allow anyone to use your User ID and Password, as you are responsible for all transactions undertaken with your User ID and Password.
- Do not use common or easy-to-guess Passwords like your User ID, personal telephone number, birth date or other personal information.
- Memorize your Password and do not write or record it anywhere.
- Do not select the option on browsers for storing or retaining User ID and Password.
- Change your Password regularly.
- Change your Password immediately if you suspect that it has been disclosed to others.
- Never use the same Password for other web-based services such as for email or online services, particularly when they are related to different websites.
- Do not use shared, public or Internet cafe computers to access our online portals.

Note: No staff member or vendor should ever ask you for your Password for whatsoever reasons. You must not reveal your Password under any circumstances.

AVA INSURANCE BROKERS

91 Bencoolen Street #08-03 Sunshine Plaza Singapore 189652
+65 6535 1828
+65 6535 6898 / +65 6535 6878
enquiries@ava-ins.com

PRECAUTIONS AGAINST VIRUSES AND MALICIOUS CODE

Viruses and other forms of malicious code can capture your password keystrokes and access other forms of personal information if they are on your device. Below are some security precautions to follow to minimize your risk:

- Do not use a computer or device which cannot be trusted.
- Install anti-virus, anti-spyware and firewall software in your personal computers especially when you are using broadband connections, digital subscriber lines and cable modem.
- All anti-virus, anti-spyware and firewall software should be updated with the latest security patches or newer versions as soon as possible.
- Do not install or run programs of an unknown origin.
- Do not open any email attachments from unknown sources.
- Delete junk or chain mail.
- Update your operating system patches and service packs.
- Make regular backup of critical data.
- Consider encryption technology to protect highly-sensitive data.
- Remove file and printer sharing in your PCs, especially if they have internet access via cable modems, broadband connections or similar set-ups.
- Do not disclose personal, financial or credit card information to little-known or suspicious websites or platforms.

REMEMBER TO LOG OUT

Always log out after your session and do not leave your computer or device unattended while any sensitive transactions are being processed.

CLEAR YOUR BROWSER CACHE

It is advised to clear your browser's disk cache after every Internet session. Your browser's disk cache can retain images of data sent or received over the internet and are targets for potential system intruders.