Security Statement

About this Security Statement

This AmBank Group Web Portal Security Statement ('**Security Statement**') applies to the AmBank Group website www.ambankgroup.com ("**AmBank Group Web Portal**"). Through links provided by AmBank Group Web Portal, you may be brought to other websites operated by AmBank Group entities, including online internet banking services, provided by AmBank Group entities. For the Security Statement of these websites, please refer to the Security Statements available in the websites of the relevant AmBank Group entities.

This Security Statement explains:

Security of your personal information collected and/or processed through AmBank Group Web Portal; and Your Obligations as a User of AmBank Group Web Portal

AmBank Group aims to maintain strict procedures and standards and take all reasonable care to prevent unauthorised access to your personal information, and to protect the security of your personal information during transmission. AmBank Group constantly monitors developments in security and encryption technology and will review and update its processes in line with industry standards.

AmBank Group has taken several security initiatives such as deploying technological hardware and software, policies and procedures, and addressing operational security issues.

1. Security of Personal Information

Personal information supplied by you to AmBank Group shall be used in providing AmBank Group's services under the AmBank Group Web Portal.
To ensure security, transmission of personal information over the Internet between the browser and the servers in the AmBank Group Web Portal is encrypted using the proven Secure Socket Layer ("SSL") technology, an industry standard security measure available through your browser. Encryption is a mechanism of transmitting data in a secure manner, where the data is encrypted using a key (this key is provided by a recognised Certificate Authority (CA))
All your personal information collected and/or processed by the AmBank Group Web Portal are stored in secured repositories in our secured data centre. Only authorised personnel have access to the data repositories in limited circumstances and they are prohibited from making any unauthorised disclosure of your personal data. Backups are performed to ensure that your personal information is safe against system failures. These backups are stored in a secured location.

AmBank Group, in its goal to protect your information, has implemented various security features, including:

1.1. Firewalls & Intrusion Prevention Systems
1.2. Anti-Virus Software
1.3. Internal Policies & Guidelines
1.4. Security Assessments and Surveillance
1.5. Server side Authentication through Digital Certificates

Where relevant, such as in linked online services, additional security features are implemented including:

1.6. Login ID and Password Verification
1.7. Encryption of Passwords
1.8. Account Locking
1.9. Automatic Log out

1.1. Firewalls & Intrusion Prevention Systems

Firewalls act as filters that control and monitor information flowing in or out of a protected network. AmBank Group also has an industry standard Intrusion Prevention System to automatically block known attacks from hackers. The Intrusion Prevention System alerts AmBank Group's security personnel about possible attacks-in-progress and AmBank Group keeps audit logs to provide a trail of information.

1.2. Anti-Virus / Anti-Malware Software

With the outbreak of viruses over the internet, it is critical for AmBank Group to have anti-virus / anti-malware software. AmBank Group has implemented industry standard anti-virus / anti-malware software to ensure its systems are safe from viruses and malwares.

1.3. Internal Policies & Guidelines

AmBank Group adopts various policies and procedures for managing system access, system back-ups and other operations management to safeguard access to AmBank Group's systems. Several guidelines and procedures have been put in place to minimise potential security breaches and to ensure and protect the data integrity of AmBank Group's network.

1.4. Security Assessments and Surveillance

AmBank Group engages security consultants to perform independent regular periodic security assessments on our security infrastructure to detect and to immediately address any currently known high risk vulnerabilities. AmBank Group also engages security consultants for continuous security surveillance to detect and immediately address any abnormal activities.

1.5. Server side Authentication through Digital Certificates

AmBank Group’s transaction systems are secured with a digital certificate to enable safe communications with our customers. Such a feature ensures message privacy, web site authentication, and message integrity. You will be able to verify the website identity by clicking on the closed padlock icon located either at the top or bottom of your browser window.

1.6. Login ID and Password Verification

Your Login ID and Password will be used to authenticate you during logins to online services. To ensure the integrity of your Login ID and Password, AmBank Group advises you to periodically change your Password and to keep it secret.
Where appropriate an additional layer of security, for example in the form of a Transaction Authorisation Code (TAC) via SMS, is required as a second level of authentication before you are allowed to perform specific transactions.

1.7. Encryption of Password

Passwords are treated with the highest level of security. AmBank Group makes use of industry standard technologies to encrypt and protect your Password.

1.8. Account Locking

Invalid login attempts are logged and the account is locked by AmBank Group's system after the allowed login / sign-on attempts are exceeded. Once your account is locked you need to call our Contact Centre to reactivate your access.

1.9. Automatic Log Out

If there is prolonged inactivity during your logged in online session, AmBank Group's system will automatically log you out of the system. You are then required to re-login.

2. Your Obligations as User of AmBank Group Portal

As a user, you play an important role in ensuring the security of your online sessions when using the AmBank Group Web Portal and AmBank Group's online services provided through links in the AmBank Group Web Portal. The following are the minimal security options you can enforce.

2.1. Review your Account Activities

You are advised to regularly review your account activities. If you suspect any unusual account activity, immediately contact AmBank using the contact information provided below.

2.2. Maintaining the secrecy of your Login ID and Password

You are responsible for maintaining the secrecy of your Login ID and Password. AmBank Group will not be able to secure your information if you reveal your Login ID and Password to any third party. AmBank Group's personnel are not authorised to ask you for your Password.

2.3. Use strong password

When selecting a password do not associate your selected password with anything personal such as names, birth dates, phone numbers or other familiar words. Do use a combination of numbers, lower and upper case alphabets and special characters, for example *, %, #, ^, &, and a minimum length of 8 characters for your password.

2.4. Log Off / Log Out

Never leave your computing device unattended during your online transaction session. Always remember to log off or log out after you have completed your online transaction. You are advised to check your last login date and time immediately after you have login / sign-on. If you suspect any unusual account activity, please contact AmBank Group immediately using the contact information provided below.

2.5. Keep your computing device's Operating System (OS) and browser up-to-date

To secure the information transmitted between your computing devices (e.g. a Personal Computer) and the AmBank Group's systems, you will need to use a current version of a reputable browser and ensure the security fixes for the computing device and the browser are up-to-date.

2.6. Install Internet security cum anti-virus / anti-malware software

For you to have safe and secure online transaction sessions, you should ensure that you have installed internet security cum anti-virus / anti-malware software on your computing devices for added protection.

2.7. Clearing your browser

After the completion of your online transaction, to protect the privacy of your information, you are advised to clear the browser's cache by taking such steps as may be required by your internet browser.

3. Enquiries / Complaints / Communication

Should you have any query / concerns / complaints, in relation to this Security Statement, kindly contact us at:

Phone: 1300 80 8888 (Domestic) or (603) 2178 8888 (Overseas) [24 hours]
AmBank Contact Centre
Mail: P.O. Box No. 12617
50784 Kuala Lumpur
E-mail: customercare@ambankgroup.com