AmAccess Corporate Security Statement

1. Introduction

This Security Statement applies to AmAccess Corporate, owned and operated by AmBank (M) Berhad (Company No, 8515-D) & AmBank Islamic Berhad Company No 295576-U) (hereinafter collectively referred to as "the Bank"). The Bank is committed to protect the privacy of your personal, company and financial information.

This statement is to be read with the Master Services Agreement and all relevant Terms and Conditions. By you accepting the terms contained in this statement, it is deemed that you have accepted the terms of the Master Agreement.

For the purposes herein, all words and expressions shall have the same meaning as in the Master Services Agreement (hereinafter referred to as `Master Agreement'), except where otherwise expressly stated.

The Bank reserves the right to add, delete, edit or modify the terms contained within this statement at any time without notice to the customer.

2. Security Statement

The Bank aims to maintain strict procedures and standards and takes all reasonable care to prevent unauthorized access to your information, and to protect the security of your information during data transmission.

The Bank has taken several security initiatives such as deploying technological hardware and software, policies and procedures, to address operational security issues.

AmAccess Corporate is secured with a digital certificate to enable safe communication between the Bank and their corporate customers. Such a feature ensures message privacy, web site authentication, and message integrity. You will be able to verify the identity of the website by clicking on the closed padlock icon located at the browser window.

3. Your Obligations

As a user, you play an important role in ensuring the security of your Internet banking sessions.

To secure the information transmitted between your personal computer and AmAccess Corporate, you will need minimum Microsoft Internet Explorer 7.0 or higher with 256-bit encryption. Encryption is a mechanism of transmitting data in a secure way, where the data is encrypted using a key (this key is provided by a Certificate Authority (CA)). The Bank is not responsible for any losses or damages incurred by you if you are not using the recommended minimum system requirements.

To protect the privacy of your information, you are advised to remove the cache information using the steps provided in the Security Tips.

4. Authentication

AmAccess Corporate caters for 2 types of authentication – depending on Channel Services rendered by customer i.e. AmAccess Corporate Inquiry or AmAccess Corporate Payment.

The standard Login ID and Password authentication will provide you access to AmAccess Corporate inquiry functions only. To ensure the integrity of your Login ID and Password, the Bank advises you to periodically change your Password and under no circumstances should you reveal your Password to anyone. You should not disclose your Password to the Bank's personnel even if requested to do

so. When selecting a Password, do not associate your selected Password with anything personal such as names, birth dates, phone numbers or other familiar words.

All transactions can only be performed by Token Based Users i.e. AmAccess Corporate Payment Customers.

Token Based Users are authenticated using a Two-Factor Authentication token such as Vasco®, which is activated by a Personal Identification Number (PIN), in addition to your Login ID. Each time you enter your Login ID, a Challenge will be provided. A Response to the Challenge has to be generated from a Vasco® token device that is assigned to your Login ID. A new Challenge Code is required after 50 seconds to prevent fraudulent use of expired Response.

After three (3) incorrect sign-on attempts, the user will be blocked by the Bank System.

5. Automatic Log Out

If there is inactivity of Twenty (20) minutes during your AmAccess Corporate session, the Bank's system will automatically log you out of the system. You are then required to re-login. You are advised not to leave your PC unattended whilst logged onto AmAccess Corporate.

To ensure that no unauthorized persons gain access to an active AmAccess Corporate session, the Bank advises you to logout of the system by clicking the Logout button before leaving your workstation.

6. Data Security & Confidentiality

AmAccess Corporate is designed to give you control over your financial information. The Bank uses the industry standard security measures available through your browser that is known as Secure Socket Layer (SSL) encryption. To ensure that your financial information is kept secure, the Bank stores it on a data repository in a secured data centre.

The Bank, in its commitment to protect the privacy and security of your information, has implemented the following security features:

a) Login ID and Password Verification for AmAccess Corporate Inquiry Customers only
b) Two-Factor Authentication for AmAccess Corporate Payment Customers only (Token Based Users)
c) Firewalls & Intrusion Detection Systems
d) Anti-Virus software
e) Internal Policies & Guidelines
f) Server side Authentication through Digital Certificates

a) Login ID and Password Verification for AmAccess Corporate Inquiry Customers only

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, AmAccess Corporate advises you to periodically change your Password and to keep it secret.

A Transaction Authorisation Code (TAC) via SMS is required for first time users logging into system for AmAccess Corporate Inquiry Functions.

b) Two-Factor Authentication for AmAccess Corporate Payment Customers only (Token Based Users)

To ensure provision of Token user is correct & authorised by customer, Token Acknowledgment & Activation is required before first time login.

c) Firewalls & Intrusion Detection Systems

Firewalls act as filters that prevent information from getting in or out of a protected network. This protects the network against unauthenticated access to the server and permit-selected traffic based on functions available at AmAccess Corporate.

The Bank also has an intrusion detection system to automatically disable attacks from hackers. The intrusion detection system alerts the Bank's security personnel about possible attacks-in-progress and the Bank keeps audit logs to provide a trail of information.

d) Anti-Virus Software

With the outbreak of viruses over the Internet, it is critical for the Bank to have anti-virus applications. The Bank has implemented industry standard anti-virus applications to ensure its systems are safe from viruses. For you to have safe and secure Internet banking sessions, you should ensure that you have implemented anti-virus software on your personal computer for added protection.

As a user, you are strongly advised to have anti-virus and anti-spyware applications installed in your PC, laptop or mobile devices. The Bank uses digital certificates (see below) to guard against Trojan horses, spyware or other malicious software from infiltrating its systems.

e) Internal Policies & Guidelines

The Bank adopts various policies and procedures for managing system access, system back-ups and other operations management to safeguard access to the Bank’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 the Bank’s network.

f) Server side Authentication through Digital Certificates

Digital Certificates are used to verify the authenticity of a website and provides an encrypted communication. Internet banking sessions between you and AmAccess Corporate are encrypted to prevent Interlopers, Eavesdroppers, Vandals or Imposters, through the use of 256-bit Secure Socket Layer (SSL) from a reputable Certificate Authority such as DigiCert and Verisign, a protocol designated to provide privacy and reliability, and Integrity.

7. Queries, Concerns or Complaints

Any queries, concerns or complaints regarding this privacy policy, please address to us. Click here for AmAccess Corporate contact information.