Security Statement

About this Security Statement

This AmFIRST Real Estate Investment Trust's ("AmFIRST REIT") Web Portal Security Statement ("Security Statement") applies to AmFIRST REIT's website at www.amfirstreit.com.my. Through links provided by AmFIRST REIT's Web Portal, you may be brought to other websites. For the Security Statement of these websites, please refer to the Security Statements available in the said websites.

This Security Statement explains:

1. Security of your personal information collected and/or processed through AmFIRST REIT's Web Portal; and

2. Your Obligations as a User of AmFIRST REIT's Web Portal.

AmFIRST REIT 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. AmFIRST REIT constantly monitors developments in security and encryption technology and will review and update its processes in line with industry standards.

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

1.0 Security of Personal Information

Personal information supplied by you to AmFIRST REIT shall be used in providing AmFIRST REIT's services under the AmFIRST REIT's Web Portal.

To ensure security, transmission of personal information over the Internet between the browser and the servers in the AmFIRST REIT's 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 recognized Certificate Authority (CA)).

All your personal information collected and/or processed by the AmFIRST REIT's 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.

About this Security Statement – Contd.

1.0 Security of Personal Information – contd.

AmFIRST REIT, 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; and
1.5 Server side Authentication through Digital Certificates.

1.1 Firewalls & Intrusion Prevention Systems

Firewalls act as filters that control and monitor information flowing in or out of a protected network. AmFIRST REIT also has an industry standard Intrusion Prevention System to automatically block known attacks from hackers. The Intrusion Prevention System alerts AmFIRST REIT's security personnel about possible attacks-in-progress and AmFIRST REIT 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 AmFIRST REIT to have anti-virus/anti-malware software. AmFIRST REIT has implemented industry standard anti-virus/anti-malware software to ensure its systems are safe from viruses and malwares.

1.3 Internal Policies & Guidelines

AmFIRST REIT adopts various policies and procedures for managing system access, system back-ups and other operations management to safeguard access to AmFIRST REIT'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 AmFIRST REIT's network.

1.4 Security Assessments and Surveillance

AmFIRST REIT 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. AmFIRST REIT also engages security consultants for continuous security surveillance to detect and immediately address any abnormal activities.

1.0 Security of Personal Information – contd.

1.5 Server side Authentication through Digital Certificates

AmFIRST REIT'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, where applicable. To ensure the integrity of your Login ID and Password, AmFIRST REIT 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. AmFIRST REIT makes use of industry standard technologies to encrypt and protect your Password.

1.8 Account Locking

Where logins are required, invalid login attempts are logged and the account is locked 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 of Logged-In Sessions

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

About this Security Statement – Contd.

2.0 Your Obligations as User of AmFIRST REIT Web Portal

As a user, you play an important role in ensuring the security of your online sessions when using the AmFIRST REIT 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 AmFIRST REIT 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. AmFIRST REIT will not be able to secure your information if you reveal your Login ID and Password to any third party. AmFIRST REIT's personnel are not authorized 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 AmFIRST REIT 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 AmFIRST REIT’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.

About this Security Statement – Contd.

2.0 Your Obligations as User of AmFIRST REIT Web Portal – contd.

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.

3.0 Enquiries/Complaints/Communication

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

Telephone No. : 03 – 7955 8780/8782

Address : AmREIT Managers Sdn Bhd (730964-X)
(formerly known as Am ARA REIT Managers Sdn Bhd)
Penthouse, Menara AmFIRST
No. 1, Jalan 19/3
46300 Petaling Jaya
Selangor

E-mail : rahman-joned@ambankgroup.com

Note: By using or accessing the AmFIRST REIT's Web Portal, you shall be deemed to have read this Security Statement. If you are not agreeable to any of the terms mentioned in this Security Statement, please immediately discontinue your use of AmFIRST REIT's WebPortal.

Updated as at 13th February 2018.