SECURITY POLICY

1- WHAT PRECAUTIONS SHOULD YOU TAKE BEFORE ENTERING YOUR USER NAME OR TOKEN PASSWORD ON THE INTERNET?

Just as you take precautions when using an ATM it is in your best interest to take precautions when using Electronic Banking. Regardless of whether you are accessing the Internet from an Internet Café, a home or work PC, we suggest the following:

- It is important to ensure that you are at the Alrajhi website. This you do by checking the Alrajhi Security Certificate
- Always ensure the secrecy of your Token device and do not lend it to work colleagues as you will be hold accountable.
- Never lend your Token to anyone this includes bank staff members. A bank staff member will never ask your Token and you must ensure if a bank employee requests you to logon to your system that you are allowed complete privacy before you do so.
- Be especially vigilant of security cameras pointing on your PC

2- HOW DO YOU KNOW THAT YOU ARE ON THE SECURE LOCAL BANKING WEBSITE?

Check to make sure that the URL begins with "https" rather than "http" and that the complete url: https://www.almubasher.com.sa/NewECorporate/p/login/companyUser.do is viewable in your browser address field. The login screen, where the user Name and password are entered is secured using SSL (Secure Sockets Layer) encryption technology.

3- WHAT IS "SPOOFING" AND HOW DO YOU ENSURE THAT YOU ARE NOT AT A "SPOOFED" SITE?

"Spoofing" is a practice that criminals undertake to lure you to their site, with the express purpose of defrauding Internet bankers and shoppers. A "spoofed" website looks like the real website, but with a few checks it is easy to establish if you are at the correct site.

4- WHAT IS A "CERTIFICATE"?

The certificate is a digital ID book that authenticates a website. A certificate itself is a small-encrypted file that contains certain information that has been verified to be true by VeriSign. This certificate can be verified by the built in capability of any Microsoft or Firefox or Google browser to be a real VeriSign certificate. The digital certificate is thus a tamper proof repository of information that will verify the identity of the holder, be that a person or a web server.

5- WHO OR WHAT IS "VERISIGN"?

VeriSign was founded in 1995 and is the world's foremost Certificate Authority providing public and enterprise trust services in order to secure electronic transactions of any kind.

6- WHAT ADDITIONAL SECURITY FEATURES DOES ALRAJHI INTERNET BANKING EMPLOY?

Alrajhi Bank has instituted the following security measures in order to protect you and the bank:

7- ADVANCED ENCRYPTION SOFTWARE

Alrajhi uses the most advanced internationally accepted standards of encryption technology. At present this is 128-bit encryption built into the browsers and it is continuously upgraded.
Therefore, it is always in your best interest to update your browser to the latest released version.
Please note: Alrajhi Bank does not advise the use of Beta versions of browsers for access to Internet banking - only the commercially released browser. (Beta in the IT world refers to software that is still under user testing)

8- USER NAME AND TOKEN

You can only make use of the Electronic Banking service if you are registered as a user and have an user Token device.

9- SECURITY VIOLATION

You have three opportunities to enter your password correctly on the website. After the third

unsuccessful attempt, you will be denied access to the service. You will then be required to call the Alrajhi Helpdesk to have the password reset.

10- TIME OUT

If you have logged on and have not used the service for 15 minutes, you will be logged off. To access your accounts again you will need to LOGON.

11- SECURITY

11.1 It is the Client's responsibility to control and restrict access to the Electronic Banking platform. Accordingly, the Client should acquaint itself with all aspects relating to the security of Electronic Banking, including, but not limited to, the use of the Tokens referred to in clause 11.2 below.

11.2 Upon installation of Electronic Banking, the Bank will provide each system manager nominated by the Client, with an access Token and a Pin providing operating abilities as agreed with the Client.

11.3 Each system manager or operator may change the Pin, but is entirely responsible for the secrecy of such a Pin.

11.4 If this agreement is terminated for whatever reason, the Client must return to the Bank all software, hardware, manuals, forms, instructions and other documentation and writings including copies, relating to Electronic Banking supplied by the Bank to the Client, unless the Client purchased them from the Bank.

12- RIGHT TO CHANGE THIS PRIVACY AND SECURITY STATEMENT

We may always change this privacy and security statement. We will put all changes on our website. The latest version of our privacy and security statement will replace all earlier versions of it, unless it says differently.

Email us on ecorporate@alrajhibank.com.sa if you have any questions about this privacy and security statement.