J TRUST BANK

SAFETY WAY TO TRANSACTION

For your safety in transactions, please note the following:

USER ID, PASSWORD, TOKEN

1. Change your J TRUST NET INDIVIDUAL & J TRUST MOBILE Password periodically with a unique combination that is difficult to know by others.
2. Do not give your password or PIN to anyone, including Bank officers.
3. Avoid storing J TRUST NET INDIVIDUAL & J TRUST MOBILE Passwords on your computer / Laptop, Smartphone and Tablet.
4. Never send sensitive information via email. Please note that J Trust Bank will not request sensitive information via email or other unsafe electronic means.

COMPUTER/ LAPTOP, SMARTPHONE/TABLET

1. Use a trusted personal computer and network to access J TRUST NET INDIVIDUAL & J TRUST MOBILE services. We recommend avoiding the use of public computers, for example in internet cafes, and / or untrusted networks, such as wifi access points provided by cafes or shops in shopping centers.
2. Always update / update the latest version of the web browser or application that you use to acces J TRUST NET INDIVIDUAL & J TRUST MOBILE.
3. Ensure that the computer / laptop is used safely from the key logger device.

NETWORK

Do not use public Wi-Fi access when making transactions via J TRUST NET INDIVIDUAL & J TRUST MOBILE. Wireless networks available to the public can also be used by criminals to steal information from cellphones, including banking information.

SAFE ZONE

Use the official application specifically issued by J Trust Bank by downloading J TRUST MOBILE application directly from the application store or by accessing the official website of J Trust Bank. Or to find out it's in a safe zone, start with the correct URL, like 'https'. You can also see the padlock in the lower right corner of the monitor screen that shows whether the website is entered safely or not.

VERIFICATION

Before making any transaction, make sure that you are accessing J Trust Bank. Verification of information such as numbers that can be contacted and clear addresses in the event of an error. Also check with the bank by telephone about the intended account number, from the website address to the valid account number.

RENEWAL

Continue to update J TRUST MOBILE application, update the latest version manually or by activating the auto-update function. Always use the latest version of the application on electronic banking services.

OTHERS

1. Some things that need to be considered related to the security of transacting through J Trust Bank Electronics Banking are as follows:
   a. **Phishing**

      Phishing is a fraud by certain parties by creating fake websites that are very similar to the official website of the Bank with the aim of obtaining confidential information belonging to customers such as User ID and Password that can be used to harm the Customer. Security against phishing can be done in the following ways:
      1. Make sure you access J TRUST NET Individual through the official website address at https://www.jtrustnet.com or use the link available on the website www.jtrustbank.co.id, Always double-check the spelling of the website name, do not let a typo, including the use of symbols.
      2. Make a short cut or save address site J TRUST NET Individual in the browser (bookmark) therefore you can use the short cut and the bookmark to minimize typing of J TRUST NET Individual website address.
      3. Be aware of fraudulent attempts from individuals on behalf of J Trust Bank officers by telephone, fax or e-mail asking for personal data including PIN. A J Trust Bank officer will not ask or ask for your Password or PIN number.
      4. Never enter a User ID and Password on a web page that opens automatically (pop up) and / or from suspicious links / links such as from digital advertisements / banners on the website.

b. **Virus**

Viruses are computer software created with certain objectives to damage the operating system, applications, and data on infected computers. Viruses can be spread through many media such as e-mail, CDs, removable storage, programs downloaded from the internet, networks, and also from unsafe websites. Some examples of the effects of viral infections are that computer devices become unstable and often 'hang' (jams), data is erased, and some application programs become unable to function properly. Security against viruses can be done in several ways as follows:

1. Using the latest anti-virus to prevent the infection of your computer with viruses, malware, spyware or other forms of applications that can be detrimental.
2. Be careful downloading email attachments because they can contain viruses that can steal sensitive data. Perform a scan of the attachment first using anti-virus software that was owned before opening.
3. Be careful in downloading and / or installing software.
4. Be careful in connecting removable storage devices to your computer device. Do a scan on removable storage using anti-virus software first before opening the contents.
5. Avoid access to and / or download files from untrusted web addresses.

c. **Spyware**

Spyware is computer software that is made to retrieve important / personal information such as credit card numbers, User ID and PIN / Password, account number, e-mail address, etc. from the infected computer device and will send the information to a specific location for the benefit of the parties who is not responsible. Spyware can be installed via email attachments, programs that are installed from unsafe sources / websites. Viruses can also be programmed to spread spyware. How Spyware works tends to be difficult to detect so it is easier to collect information desired by the maker / spreader. Security against spyware is the same as protecting against viruses.

2. To ensure the security certificate details and the website address https://www.jtrustnet.com/, select View Certificate in the green bar / security icon next to the web address in the browser that you are using. If you leave a warning message about the certificate when accessing J TRUST NET INDIVIDUAL, please do not access the website or double-check the name of the website that has been typed.
3. Make sure there is a lock / lock image in your Internet browser that indicates the page you are accessing is currently encrypted using Security Socket Layer (SSL). If you don't see a lock / lock image, please log out.

4. Never register J TRUST NET INDIVIDUAL & J TRUST MOBILE to get prizes or for any reason at the request of someone by telephone or by other means. Officially register J TRUST NET INDIVIDUAL & J TRUST MOBILE only through the Branch Office or J TRUST NET Individual Portal.
5. If there is a notification from J Trust Bank regarding an activity on a temporary account you have never done that, immediately follow up by visiting the nearest J Trust Bank Branch Office or contact the call center.
6. Confirm to the J Trust Bank to J Trust Call Center “ASK J 24 hours” in 1500615 if there is a suspicious request.
7. Stop transaction activities if you feel that there is something unusual / unusual on a computer / laptop or smartphone / tablet or web page / application that is being accessed.