Security Policy

Security Information

Please note that some fake or phony websites will try to capture or entice you to reveal your personal information and passwords.
Be alert for such websites and suspicious emails purporting to be from MUFG Bank, Ltd. Singapore Branch.
(hereinafter referred to as 'the Bank').You should report these immediately by contacting the Bank.
Access to cash management application is permitted only for the authorized users.

Remember that the Bank's staff will never ask you for your password and will not make unsolicited requests for customer
information through email or phone unless you initiated the contact. The web page you are now viewing will redirect you to
the login page at http://www.bk.mufg.jp/cms/ only. This page will not take you to any other website.
You should not accept any other links or redirections from other websites or media for the purpose of logging onto the Bank's website.

Adopting the proper safety measures can prevent inherent risks in the internet environment relating to all transactions.
The Bank strives to provide you with a safe and secure environment for online internet transactions.
Safety and security in online internet banking depends on
both the security systems of the Bank and also the precautions taken by you, our valued customer in safeguarding your token,
password and PC. To learn more about safeguards for online internet transactions, please spend some time to read through
the following important information.

Protecting Your Password

- Do select a robust and unique password to make it difficult for anyone to guess;
- Do change your password regularly (minimum 8 characters, maximum 16 characters and alphabetic characters and symbol characters are mandatory to use);
- Avoid using sequential number (eg. 12345678) or the same character more than once (eg. 12245678);
- Do not choose a password that is based on user-id, personal telephone number, birthday or other personal information;
- Do not reveal your password to anyone. Keep it confidential;
- Password should be memorised and not be recorded anywhere;
- Change your password immediately if you suspect any unauthorised access;
- Do not allow anyone to keep, use or tamper with the OTP token;
- Do not reveal the OTP generated by your security token to anyone;
-Do not divulge the serial number of your security token to anyone;
- Do check the authenticity of the Bank's 's website by comparing the URL and the Bank's name in its digital certificate;
or by observing the indicators provided by an extended validation certificate;
- Do check that the Bank's website address changes from 'http://' to 'https://' and a security icon that looks like a lock
or key appears when authentication and encryption is expected.

Quick Tips on Security

1. Never use the same internet banking password for other financial or non-financial web-based services such as for email,
subscription services, online shopping, digital identity and other online;
2. Protect your PC from viruses and malicious programs;
3. Do not store your user password when using internet explorer browsers;
4. Avoid using shared/public PCs for online internet banking;
5. Check your account and transaction history details regularly and report any discrepancy;
6. You are strongly advised to type in the URL manually to access the login page.

How to safeguard your account information

Apart from the security measures put in place by the Bank, you play an equally important role to ensure your online security and account information
is not compromised.

You SHOULD adopt the following recommended security practices while banking online:

1. Install anti-virus, anti-spyware and personal firewall products with security patches or newer version on regular basis;
2. Update operating system, anti-virus and personal firewall products with security patches or newer versions on a regular basis;
3. Remove file and printer sharing feature in computers, especially when PCs are connected to the internet;
4. Protect your critical data by making regular backup of critical data;
5. Consider the use of encryption technology to protect highly sensitive or confidential information;
6. Always log-off your online session;
7. Clear your browser's cache and history after each online session;
8. Do not install software or run programs of unknown origin;
9. Delete junk or chain emails;
10. Do not open email attachments from strangers;
11. Do not disclose personal, financial, or credit card information to little-know or suspect website;
12. Do not use a computer or a device which cannot be trusted;
13. Do not use public or internet café computers to access online services or perform financial transactions.

Contact Us

If you encounter any abnormal behaviour or any suspicious warning message by browser while accessing internet application,
you are advised to inform the Bank about such warning messages that are encountered.

If you have any queries, please call CMS Helpdesk at +65 69185000 (Mon to Fri - 9:00am to 6:00pm) excluding Public Holiday.
The information on the MUFG Bank, Ltd. Singapore Branch. and its global presence in regional markets is available on the following web-site:
http://www.bk.mufg.jp
http://www.bk.mufg.jp/english

Privacy Policy

We are committed to protecting your privacy and to maintain the confidentiality of the information that you give us through this website.

1. We will only collect information from you for the purpose of giving you better customer services and products.
2. We will not make unsolicited requests for customer information through email or the telephone, unless customers initiate contact with us.
3. We will treat any information that we receive from you with care and recognise the need for appropriate action to manage and
protect any information that you disclose to us.
4. This Policy is not intended to, nor does it, create any contractual rights between the customer and us.

Risk and Benefits of Online Internet Banking, Responsibilities, Obligations and Rights

Online internet banking can bring about convenience with faster and easier access to your bank account(s), the inherent risks involved must be addressed and understood by you.
As the internet is an open and publicly accessible platform, web-based systems such as our cash management application.
are inherently subjected to risks such as those related to virus attacks, hacking, unauthorized access and fraudulent transactions.

While the Bank has put in place all the necessary security practices and measures to safeguard against these risks,
the Bank is still unable to fully guarantee the complete security of your transactions against such malicious attacks.
As an user of the online internet banking Services, you play a key role in safeguarding your account information.

Your usage of internet banking is subjected at all times to the Terms and Conditions governing the Electronic
Services (the "Terms and Conditions"). In addition, you are advised to comply with the Bank's recommended security practices to ensure
you do not under any circumstances, compromise your online security.
Under the Terms and Conditions, you will be responsible for all transactions made through the use of your OTP token and password,
regardless of whether such transactions were in fact entered into, or authorized, by you. You should therefore read carefully and
adhere to the recommended security practices described under "How to safeguard your account information".
The Bank is not responsible for any loss or damage in connection with your use of internet banking unless such loss is attributable
to our gross negligence or wilful default.

You should note in particular that the Bank will not be responsible for your losses, which arise as a result of any of the following events:

- Your failure to abide to our Terms and Conditions, and recommended security practices;
- Your failure to promptly report any unauthorized access and/or fraudulent transactions on your account;
- Your failure to report loss or stolen password/ token;
- Negligent handling, disclosure and/or sharing, of password/ token, with third parties;
- Input errors in online banking transactions;
- Unavailability of our internet banking service due to system maintenance/breakdown/non-availability of any network
or any other event beyond our control;

You will have the right to:
- Request the Bank to suspend access to your internet banking immediately should you suspect any unusual activity,
compromise of password and/or unauthorized access;
- Request the Bank to terminate your internet banking access should you wish to discontinue the service;
- Request for a new password if you have forgotten/lost or suspect your password has been exposed;
- Obtain information from the Bank regarding your online transactions;

-

-