

Confirmation of Application for Corporate Electronic Banking Service(Customer Copy)

Corporate Banking (Corporate Smartphone Banking) CMS^{iNet} Tele-Banking

Online Printing Section (Please compare the following with what you describe)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

■ Thank you for enrolling in Hana Bank's Corporate Electronic Banking service. The Bank will do its utmost to provide you secure and convenient electronic banking services.

Guide to [Corporate Electronic Banking service]

- ① Access Hana Bank's website <https://biz.kebhana.com>
- ② Click on the Digital Certificate Center at the top and proceed with 'Prior consent to online issuance of digital certificate' and 'Issue/Re-issue digital certificate'
※ If you hold a digital certificate issued by another financial institution, use the column marked 'Registration of Other Bank/Other Institution's Digital Certificate'
- ③ Proceed to Log-in page and log in with digital certificate or ID & Password after completing the '(New) Password Registration' process.
- ④ If you wish to use Multi-Approval Lines, log in as Master User and set up authority for each user and approval operations
※ For support, contact 1588-1111, 1599-1111 speed dial 0>5

Guide to [Hana 1Q bank CMS^{iNet}]

- ① Access Hana Bank's website <http://inet.kebhana.com> and click on log-in
- ② Register Administrator's PW and log in with ID/PW
- ③ For transfer, issue a digital certificate in Digital Certification Center after log-in
※ For support, contact 1588-3555(extension 3)

Guide to [Corporate Smartphone Banking]

- ① Search Hana Bank in app store, and download and install '1Q bank Corporate' or '1Q bank CMSiNet' onto your smartphone
- ② For transfer, use "Import Digital Certificate" or "Issue(Re-issue) Digital Certificate" in Digital Certification Center
- ③ Log in with digital certificate or ID/PW to use the service

■ Hana Bank provides a variety of corporate e-banking services to deliver effective asset management services. If you have any questions, please contact a nearby branch.



■ Important information about electronic banking services:

1. Do not use a password that can be easily guessed by another person.
2. Use a different password for electronic financial transactions than your account password.
3. Change password on a regular basis. If you suspect that your password has been compromised, promptly notify the Bank and change the password.
4. Do not save a digital certificate on a hard drive.
5. Do not write or record any information required for electronic financial transactions in your notebook, wallet, etc.
6. Do not ask another person to conduct electronic financial transactions on your behalf or provide them with security-related information.
7. Use the Bank's service of immediately informing the customer of any use of electronic financial transactions.
8. Refrain from using a public or shared computer. If such use is unavoidable, delete all information after using such a computer.
9. Set appropriate daily/one-time transfer limits for electronic banking transactions.
10. Install vaccine programs in computer used for electronic financial transactions to prevent hacking and other security accidents.

■ Key Points of 'General Terms & Conditions for Corporate Electronic Banking Service'

Article 8 (User verification)

- ① In the case of services the User may use without concluding an agreement for electronic financial transactions in accordance with Paragraph 1 of Article 4 of the General Terms & Conditions, if account number and account password are correct, User may be recognized as the principal.
- ② In the event the User enters such items as requested by the Bank for each service type as described below and the information entered by the User is identical to what is registered with the Bank, the Bank may regard the User as the principal and provide service. However, when deemed necessary for security, the Bank may request additional items to verify identity.
 1. Corporate mobile banking:
User ID, user password, pass-code generated by OTP (one-time pass-code generator), digital certificate, account number, account, password, business (resident) registration number, PIN number(6 digits), Pattern authentication, 'Mobile integrated authentication(Hana One Sign)'
* However, in case of PIN number(6 digits), pattern authentication and ' mobile integrated authentication(Hana One Sign)', it is limited to cases where the registered mobile device and mobile device used match and input item matches the item stored in the mobile device.
 2. Corporate Internet Banking :
User ID, user password, pass-code generated by OTP (one-time pass-code generator), digital certificate, account number, account password, business (resident) registration number

Article 12 (Standards for handling transaction instruction)

In addition to the General Terms & Conditions, the Bank shall handle transaction instructions as described below.

1. Despite the General Terms & Conditions and the agreement for relevant deposit product, withdrawal from a withdrawal account may be handled without payment order or check, and withdrawal amount shall be limited to deposit balance (including credit limit) in cash at the time of transfer.
2. When using approval service, if approval password or one-time pass-code (OTP) and digital certificate included in final approver or executor's transaction instructions are identical to those registered with the Bank, transaction instruction shall be deemed to have been given.
3. User shall frequently make a balance inquiry and update bankbook to check whether there are any problems with transactions.

Article 20 (Management of password, one-time password (OTP) and Mobile integrated authentication(Hana One Sign))

- ① The User may register password through electronic device, and shall ensure the registered password, along with security device given at the time of applying for the service, will not be leaked or disclosed to any one including bank staff.
- ② It shall be impossible to inquire or confirm user password. If password is forgotten, it shall initialize password through electronic device or at Bank branch.
- ③ If security device is lost or if it is deemed that security device information is leaked to other person, the User shall immediately submit written or electronic report to the Bank, and reissue security device in order to continue to use the relevant service.
- ④ When the User saves biometric information in a mobile device designated by him/her for 'Mobile integrated authentication(Hana One Sign)', must use his/her own biometric information, not someone else's, and must prevent the leakage of integrated authentication

information including biometric information. In case the User assumes the integrated authentication information has been leaked to others, immediately cancel the mobile integrated authentication registration through corporate mobile banking

Article 21 (Service restrictions)

In case falling under any of the following, the Bank may restrict the transaction and the relevant reason will be notified through the relevant electronic device

1. In the case falling under Paragraph 1 and Paragraph 2 of Article 14(restrictions on transaction) of the 'General Terms & Conditions'
2. In the case of entering wrong User password for identity verification 5 straight times regardless of date, wrong withdrawal account password 3 straight times regardless of date, wrong OTP-generating password 10 straight times in total for all financial institutions regardless of date , or 'Mobile integrated authentication(Hana One Sign)' does not match 5 straight times regardless of date.

■ Key Points of 'Terms & Conditions for Hana 1Q bank CMSiNet'

Article 6 (Suspension of service)

The Bank may suspend its service in cases falling under any of the following subparagraphs.

1. Circumstances which are unavoidable such as system error, system maintenance, etc.
2. Telecommunication operator defined in the Telecommunications Business Act suspends service
3. Any justifiable reason that the Bank cannot provide service

Article 9 (Confirmation of transaction details)

The Customer agrees to make inquiries of transactions occurring in relation to the Customer's usage of the service provided by the Bank, and the Bank shall not separately prepare or issue a bank statement.

Article 10 (Service program and data management)

- ① The Customer shall not lend, entrust, or assign any program provided by the Bank to any third party
- ② Bank may change or revise a program if deemed necessary to improve the service, etc.
- ③ The Customer shall manage and maintain a program provided by the Bank by fulfilling the duty of care as a manager.
- ④ The Customer shall register authentication information necessary for service, such as financial information, ID, and digital certificate, in the User's computer, etc., and manage it responsibly. The Customer shall also undertake security measures to prevent the leakage of information.

Article 11 (Indemnification)

- ① the Bank shall not be held liable for all or any part of the damages suffered by the User in any of the following cases:
 1. In case that the User violates or fails to observe this Agreement;
 2. In case that the User fails to manage his/her Means of Access safely to prevent any abuse, counterfeit or fraud related to electronic banking. Provided, if there is no significant fault or intention of the User, the Bank shall be held liable;
 3. In case that the User made mistake or error in the process of the application;
 4. In case that the transactions cannot be executed due to service disruption, suspension, or change of other financial institutions;
 5. In case that the transactions cannot be executed based on the service program due to the User's internal system;
 6. In case that accident occurs due to the User's failure to keep the security information safe in the User's PC or internal system leading to information leakage or incident.

※ The complete contents of the Terms & Conditions for Electronic Banking Service, Terms & Conditions for Corporate Electronic Banking Service, Terms & Conditions for Hana 1Q bank CMS^{iNet} Service, etc. can be viewed on Hana Bank's website.

Nationwide Customer Service Number | 1599-1111; 1588-1111 Calling from overseas | 82-42-520-2500

