General Terms and Conditions – District

Valid as of 1 December 2021

Danske Bank A/S, Suomen sivuliike
Rekisteröity toimipaikka ja osoite Helsinki,
Televisiokatu 1, 00075 DANSKE BANK.
Y-tunnus 1078693-2

Danske Bank A/S, Kööpenhamina
Tanskan kauppa- ja yhtiörekisteri
Rek. nro 61 12 62 28

Danske Bank A/S, Finland filial
Registrerad verksamhetsort och adress Helsingfors,
Televisionsgatan 1, 00075 DANSKE BANK
FO-nummer 1078693-2

Danske Bank A/S, Köpenhamn
Dansk handels- och företagsregister
Reg. nr 61 12 62 28

Danske Bank A/S, Finland Branch
Registered domicile and address: Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Table of contents

Introduction
District is the Bank's Internet-based office-banking system, which allows the Customer and the User of the service access to view account information, make payments and give other orders to the Bank.

The Terms and Conditions for District include a service description.

Part 1 District – general description on the service and the use of District.
Part 2 District – system and security.
Part 3 Contractual entity of District.

Part 1
District –general description

1. Modules and services
In District, the following services can be provided:

- District Basic (comprises different modules and services) or
- District Global (comprises different modules and services)and/or
- Additional modules and services
- Agreement Administrator and/or User Administrator.

The Module Description contains a description of the selected modules and services. An individual module and service cannot be used until Customer has granted one or several Users access to the module or service. For some modules separate agreements must be signed.

2. Transactions
With District, the Customer can perform actions in accordance with this User Rights, such as making

- queries about registered accounts within the Danske Bank Group,
- queries about registered accounts managed via SWIFT message type MT940,
- payment orders between registered accounts within the Danske Bank Group,
- payment orders via SWIFT message type MT101,
- payments to unregistered accounts within the Danske Bank Group or other financial institution, including cheque payments,
- cross-border payments to registered and unregistered accounts within the Danske Bank Group or other financial institution,
- collection, e-Invoice and related documents,
- view and update card- or card agreement administration information.
- Create and change Cash Pool Single Legal Account or Cash Pool Zero Balancing intra group limits and interest rates

In this text, payments, payment order, collections, and queries are jointly referred to as transactions.

3. Registered accounts
In the Access Agreement the Customer determines the accounts it will register in District. These accounts are referred to as registered accounts. This applies to the Customer's own accounts as well as third-party accounts within the Danske Bank Group and other financial institutions. Accounts which are not registered in District are called unregistered accounts.

3.1 Registered accounts within the Danske Bank Group
Accounts within the Danske Bank Group are opened with Danske Bank and affiliates and divisions of Danske Bank under this agreement. If such an account is registered in District it becomes a registered account within the Danske Bank Group.

The following accounts within the Danske Bank Group can be registered in District:

- accounts held by the Customer,
- accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has, issued a third-party mandate to the Customer authorizing to act on behalf of the third party or subsidiary.

Registered accounts within the Danske Bank Group can also be managed via SWIFT message types MT101 or MT940/942, see section 3.2.

3.2 Accounts managed via SWIFT messages
Accounts opened with banks within the Danske Bank Group or other banks which the Customer wishes to use for transactions via SWIFT message types MT101 or MT940/942 can be registered in District via the Access Agreement. The Customer may register both its own accounts and third-party accounts. The Customer or third party must conclude an agreement with the account-holding bank concerning payment orders via message type MT101 or an agreement on Balance Reporting via message type MT940.

Third-party accounts can only be registered if the third party has issued an authorization to the company.

4. Unregistered accounts
Accounts which have not been registered in District are referred to as unregistered accounts. It is only possible to make

payments into these accounts. It is not possible to make enquiries or payment orders from unregistered accounts.

5. Cheques

In countries where one can make payments using a cheque, payments can be made by issuing a cheque drawn on the issuer's own account in Danske Bank Group, or a third party account.

Issued cheques are regarded as banker's cheques, and the amounts are debited to the registered own or third-party account on the date of issue.

The Customer may have the proceeds from uncashed cheques deposited in registered accounts. Before crediting the account with the proceeds, the Bank is allowed to assess the financial status of the Customer.

If the proceeds from uncashed cheques are to be credited to the Customer's or a third-party's account, the Customer or third party must accept to indemnify the Danske Bank If a cheque is subsequently cashed.

If the customer and/or a third party has an agreement concerning payment orders via MT101, cheques can also be drawn on own or third party accounts in other financial institutions than the Danske Bank Group, provided that this option is included in the agreement between the Customer and/or third party and another financial institution than Danske Bank Group.

6. Payment orders

In this text, an order by the Customer or its User for a payment transaction in District, is called a payment order.

The Customer is entitled to use the service in the Bank's website (at address www.danskebank.fi) during the notified service hours.

6.1 Submission of payment requests

When a User submits a payment order on behalf of the Customer and/or a third party, the Bank sends the User an electronic receipt. The moment the Bank has confirmed receipt of the payment order, the risk in relation to its being carried out in accordance with the instructions passes to the Bank.

The User can cancel a payment order one day prior to the due date of the payment.

6.2 Binding orders

Payment orders carried out in accordance with the instructions, are binding on the Customer. Consequently, the Bank cannot reverse payments, trades in foreign exchange or securities or other transactions, including cheque issuance, finalized in accordance with the payment order to the Bank.

6.3 Retention of payment orders

The Bank retains payment orders for at least the time which has been prescribed by law. During this period, the Customer and/or third party whose account is debited may obtain a hardcopy of the order against payment. The fee is that for extraordinary assistance printed in the Bank's List of service charges.

7. Automatic registration for documents from The Archive

The archive is activated in connection with the implementation of District. The documents are file in Archive in District

The Customer receives documents from the Bank to the archive in electronic format with the same legal effect as ordinary documents in paper format.
Third party accounts comprised by the same agreement are treated as own accounts.

7.1 Documents in electronic format

The Customer will receive all documents from the Bank in electronic format to the District Archive. In special cases Danske Bank may send such documents in hardcopy by ordinary mail.

Such documents are documents in electronic format sent to the Customer by the Bank, for ex. Balance statements and different kinds of service agreements.

If the company is a customer of one or more of the Danske Bank Group's other subsidiaries and branches, and they send documents to the company electronically, the company will also receive such documents in District Archive

The Bank will send the Customer information via District of new electronic documents.

7.2 Who has access to the documents

A User may be authorized to view the documents in the Archive in District. The User Rights granted to a User will define the type of documents he or she has access to view. A User is always allowed to view his or her own User Right Agreement.

7.3 Filing in the archive

The Bank files the electronic documents in the Archive for the current year plus the following five years, as a minimum. The filed documents will be deleted when the Customer deregisters an account from District, cancels the use of District, or if

the customer relation-ship with the Bank terminates. It is recommendable that the Customer prints the documents on paper or in some other lasting manner prior to deleting the documents.

If the Customer must keep the documents for a longer period than is possible in District, it should save the documents in its own systems.

7.4 Deregistering the Archive
If the Customer does not wish to receive documents to the Archive, it shall notify the Bank when concluding the Agreement. The Bank will send the Customer the documents in paper format against a separate service fee.

7.5 Termination
Filed documents will be deleted when the Customer deregisters an account. The Customer will terminate the use of District, or the customer relationship with the Bank terminates. See section 7.3.

8. User Authorizations for District
All Users using District on behalf of the Customer or a third party must have a valid User Right issued by the Customer. This User Right is created by using the User Authorization in District.

If a third party, a company or other legal entity, has signed a Third party authorization, it can delegate this authorization to a designated and authorized User of District. This shall be done by using the User Authorization in District.

When the Customer creates a User Authorization for District, the Customer shall have the consent of the User to pass on the personal data and CRP to the Bank.

For the withdrawal of cash in a branch of the Bank, or for making payment orders Customer shall authorize the User to represent the Customer by using a separate Authorization on Use of Account drawn up for this purpose.

8.1.1 Digital channel access
Users can access District via various browsers and Business Apps. You can deny a user access to District via Business Apps. Regardless of the choice of channel, users have only the rights set out in the User Authorization for District.

8.1.2 Types of payment orders
The Customer must state which types of payment orders a single User is to have access to:

- payment orders created on registered accounts in the same country within Danske Bank Group, and which are registered in the Access Agreement;
- payment orders via SWIFT message type MT101,
- payment orders, including cheque payments, created on unregistered accounts within Danske Bank Group or other financial institutions, and which are registered in the Access Agreement;
- crossborder payments to registered or unregistered accounts in Danske Bank Group or accounts in other financial institutions
- euro payments into accounts in SEPA countries not registered on District within or outside the Danske Bank Group - including payment of drafts.

Acceptance of the received e-Invoice is a payment order.

Furthermore, the Customer must state the scale of the User Rights, or the authorization of the User to

- create and approve payments
- or only to create the selected payments.

If the User is empowered to both create and ap-prove payments, the relevant authorization within each transaction type must also be stated. The fol-lowing authorizations are available:

- separate authorization,
- two persons jointly (A authorization).

The various levels of user authorization are described in section 10.

The selected authorization is used for each payment types. If the Customer has selected a more restrictive authorization at account level, this authorization will apply for payments to unregistered accounts and cross-border payments. If the User has been granted no authorization at account level, this is also regarded as a restricted user authorization.

8.2 Access to use accounts
The Customer must define on which accounts each individual User may make inquiries and/or payments, including approving any Finnish e-Invoices. If the Customer empowers a User to make payments from a certain account, the User is granted access to the trans-action types he or she the Customer has empowered him or her to have access to.

The User's authorization must be stated for each ac-count that the User is granted access to. The following authorizations are available at account level:

- use of account, separate authorization ,
- two persons jointly (A authorization),
- two persons jointly (B authorization),
- two persons jointly (C authorization).

The various levels of User authorizations can be read in section 10.

An authorization granted at account level is valid in all District agreements under which the account is registered.

8.3 Confidential payments
The Customer can authorize some of designated his Users to make confidential payments. Confidential payments include payments such as wages and salaries, which may be viewed, created or approved only by designated and authorized Users.

A User is empowered to make confidential payments only within the transaction types to which they have been granted access to in section 8.5.

In addition, Users may inquire about confidential payments within the limits they have been granted query access.

8.4 Administrator privileges
A Customer who has access to use the Administrator module gives the Users the right to manage the Agreement as follows:

- Agreement Administrator, principal user,
- User Administrator,
- viewing Agreement information,
- ordering and blocking passwords,
- viewing and updating cardinformation,
- viewing and updating cardadministration,
- viewing and updatting cardagreement administration

Users will be granted rights to manage the Agreement and User Rights as follows:

- separate authorization,
- two persons jointly (A authorization),
- to create.

The various authorization levels granted by the Bank are described in section 10.

8.4.1 Agreement Administrator
The Principal User who has been granted rights to manage the Agreement can, in the name of the Customer:

- add or change Agreement Administrator user rights to others or own User Rights,
- delete Agreement Administrator rights,
- create, change or delete User Rights - see section 8.2.1,
- create or delete rights to view agreement information – see section 8.2.2,
- create, change or delete user or account limitations for payments,
- Viewing and updating cardinformation,
- Viewing and updating cardadministration.

Agreement Administrator can give these user rights to oneself or other users.

Requests for Agreement Administrator privileges must always be signed by persons legally authorized to sign for the company. When a user with Agreement Administrator privileges has requested the creation or modification of a User Authorization with Agreement Administrator privileges, a User Authorization District with a signature field is generated in District. The User Authorization is accessible to users with Agreement Information privileges. The User Authorization must be signed as above and sent to the Bank.

In other cases, the user accepts and signs using his or her digital signature.

8.4.2 User Administrator
A user who is granted User Administrator privileges is authorized to perform the following on behalf of the company:

- create and change users, including giving users access to the required modules, accounts, authorizations and transactions types,
- create and delete users access to ordering basic products - see action 8.2.3
- create and change user master data,
- delete all user details, including master data.

User Administrators can grant these privileges to themselves and others.

8.4.3 Agreement Data
A User who has access to Agreement Data can view or retrieve user data, User Rights (data on users, modules, management rights, rights to use the account, and rights to make payments) of the Agreement. The User has access to the user interface and the selected documents through District.

8.4.4 Payment Limit - Account
A user whom you grant Payment Limit – Account privi-leges is authorized to perform the following on behalf of your company:

- Create, edit and delete payment limits on the accounts which the user can at any time dispose of under the agreement.

For users granted Payment Limit – Account privileges, you must state which of the following authorizations should be granted to the user:

- Separate authorization
- Two persons jointly (A authorization)
- Two persons jointly (B authorization)
- Two persons jointly (C authorization).

Our account authorization types are described in section 10.

8.4.5 Ordering of Basic Products
With District Administration, you have access to Ordering of Basic Products, enabling you to make agreements about basic products in District. If you grant a user the Ordering of Basic Products privilege, you authorize the user to make binding agreements – on be-half of the company - about the basic products available from time to time in District.

8.5 Message system
All users can send messages electronically to Danske Bank through a secure communication line. Users can view only messages that they themselves send and receive in District. The message system cannot be used for transmitting orders to Danske Bank.

8.6 Changing District User Rights
If the Customer wishes to extend or limit a User's access to District, a new User Authorization for District must be signed, replacing the previous one.

If the change relates to the User's User Rights at account level, the Customer and/or third party must sign an account mandate in addition to the User Authorization.
If the customer issues an Account Authorization to access other services than Business Line, the Customer should note that this may affect the authorizations given earlier by the Customer to the User.

If the changes are made via District Administration by the Agreement and/or User Administrator of the agreement, the changes are approved by using digital signature. If the change also comprises Agreement Administrator privileges, User Authorization, must be signed in compliance with your company's signing regulations.

8.7 Revoking District User Rights
User Rights for District remain in force until revoked by the Customer in writing. User Rights may also be revoked by telephone, but this must always be followed up by written confirmation. The User's access to act on behalf on the Customer via District is blocked after the telephone call.
When the Bank has received notice of revocation, it sends written confirmation that the Users right to use bank identifiers has been deleted from the Customer's District.

If the validity of a District Access Agreement terminates, all User Rights granted under the agreement are also terminated.

If the Customer and/or a third party has granted the User Rights other than User Rights to District – e.g. for cash withdrawals at a specified branch of the Bank – such authorizations must be revoked separately.

9. Other User Rights in District
9.1 Third-party authorizations granted to The Customer
A third party may authorize the Customer in writing to make payments from his account. With this User Right the third party authorizes the Customer to register its accounts under the Customer's District agreement and to delegate these User Rights to one or more Users of the Customer. The Customer delegates the powers via the District User Right Agreement.

If the Customer is to make payments from a third party's accounts are held in another financial institution than Danske Bank Group, an agreement must be sent to the Bank stating that the Customer may send payment orders to the third party´s bank(s) via Danske Bank Group.

The Bank registers the third-party accounts in District via the Customer's Access Agreement.

9.2 Authorization to use District Markets Online
If a User is to have access to information, be able to view trade positions and buy and sell foreign exchange (spot and forward), as well as Finnish and foreign shares and securities, the User must be granted access to one or more Markets Online modules. Access to buy and sell foreign exchange (spot and forward) and to buy and sell shares and securities also requires that the Customer has authorized the User to use Markets Online. These authorizations empower the User to perform transactions which are binding to the Customer and on behalf of the Customer via Markets Online.

All transactions relating to purchase and sale of foreign exchange (spot and forward) are subject to the provisions of the framework agreement on netting and final settlement of trades concluded between the Customer and the Bank.

The User Right must state the accounts and custody accounts that the User is authorized to receive information about or trade in.

9.3 Trade Finance Authorization in District
If a User is to be able to issue letters of credit, collect debt and/or issue guarantees, the Customer must sign an agreement to this effect, a Trade Finance Module Agreement.

In this connection, the Customer must state whether the User is to have access to:

- letters of credit (exports and/or imports),
- debt collectin (exporta and/or imports),
- guarantees.

Furthermore, the Customer must state whether the User is to be authorized to:

- make inquiries,
- create and approve orders and amendments separately (Separate authorization),
- create and approve orders and amendments two persons jointly (A authorization).

The User shall have access to the Trade Finance module.

9.4 Collection Service SEPA Direct Debit Authorization in District
If a user is to be able to create SEPA Direct Debit collections, the company must register the user for the Collection Service – SEPA Direct Debit module. In this connection, the company must state whether the user is to have access to

- collections,
- reimbursements,
- revocations.

Furthermore, the company must state whether the user is to have access to

- creating and inquiring on all transactions, including transactions which cannot be created by the user.

9.5 Collection Service Finnish e-Invoice Authorization in District
The Customer must agree on the functions of the Col-lection Service with the Bank and name the users who will be granted access rights to the Collection Service.

Assignment of the module to a user gives the user access to all functions under this module, including creating and/or changing accounts connection to Collection Service.

10.Authorization levels
The Bank operates with the following authorization levels:

- separate authorization,
- two persons jointly (A authorization),
- two persons jointly (B authorization),
- two persons jointly (C authorization).

These authorizations allow the Customer to specify which Users may, separately or jointly, approve a payment or an order. The authorizations are described below.

10.1 Separate authorization
When requests or payments are created or changed by a User with this authorization, they are automatically deemed to have been approved by the User. Users with this authorization can also approve inquiries or payments entered by Users with all other authorization types.

10.2 Two persons jointly (A authorization)
When inquiries or payments are created by a User with an A authorization, they are automatically approved by this User (1st approval). Further approval (2nd approval) is required by a User with a separate, A, B or C authorization. Users with An authorizations rank equally, and the order of approval is therefore of no consequence.

10.3 Two persons jointly (B authorization)
When inquiries or payments are created by a User with a B authorization, they are automatically approved by this User (1st approval). Further approval (2nd approval) is required by a User with a separate, A or C authorization. Two users with B authorization cannot jointly approve a payment.

10.4 Two persons jointly (C authorization)
When inquiries or payments are created by a User with a C authorization, they are automatically approved by this User (1st approval). Further approval (2nd approval) is required by a user with a separate, A or B authorization. Two users with C authorizations cannot jointly approve a payment.

10.5 Cancellation of authorizations
An authorization is valid until it is cancelled by the Company, in writing.

10.6 Create authorization
When inquiries, authorization or payments are created by a User with to create authorizations, these must be verified by

either a user with a separate authority or two users with the 'two persons jointly' authority.

11. Customer support

11.1 General

The Bank provides the Customer service and relevant Customer support including among other the following:

- Management of User Rights,
- Telephone support , also including freezing of District Agreements,
- Instructions on www-pages and in District service.

Management of User Rights includes e.g. establishment of an Access Agreement and a User Right Agreement, for the Customer and its Users to amend various support and service features, delete and block users, and to transmit Bank identifiers.

Telephone support may include training, User instructions, troubleshooting assistance and guidance in relation to modification, as well as freezing District Agreements. Telephone support is provided in connection with installation, training and troubleshooting, etc. of District.

Internet-based support may include training, trouble-shooting assistance and guidance in relation to modification.

Customer support is provided in cooperation with the Customer's authorized IT department and at the risk of the Customer.

Part 2
District security system

12. Technical elements

12.1 Transmission and access

In order to use District, you must establish a data communication link with Danske Bank. You must bear all related expenses and purchase, install, set up and maintain the IT equipment required. The minimum technical requirements for the use of District are available on Danske Bank's website. You must also arrange for any adaptations to your IT equipment that may be required to use the connection as well as to ensure the continuity of operations.

You may not use special software, such as 'overlay services' or similar types of software, when you use District. Users must operate the system directly via the user interface and the software provided by Danske Bank.

12.2 Distribution, control and storage of software

Danske Bank distributes the programs you need to run District, which may, for example, be relevant in connection with file exchanging. The programs can be downloaded from the internet.

When you download programs from the internet, you or a user must check that the program delivery is digitally signed by Danske Bank.

If the programs are not digitally signed by Danske Bank, it may be because they have been changed or do not come from Danske Bank. The signature can subsequently be verified by checking the 'properties' for the downloaded program file(s). If you discover that the digital signature is not Danske Bank's, you may not install the downloaded program.

Danske Bank may at any time and without notice modify its own equipment, basic software and related procedures in order to be able to optimise its operations and service levels. Danske Bank must notify you of any modifications requiring adaptation of your systems in order to use Danske Bank's services at least one month in advance. Such notice must be given in writing via District or another channel.

12.3 Data security

BankID, eSafeID, e-Safekey, OpenPGP and EDISec are the general security systems used in District.

eSafekey, OpenPGP and EDISec are Danske Bank's security systems for customers who want to exchange information digitally with Danske Bank directly through their own business systems. eSafekey, OpenPGP and EDISec are based on a password and use permanent code files that are stored in the business's IT environment.

Use of the above security systems ensures that data can be encrypted before transmission to Danske Bank and that data is not altered during transmission.

The identity of the sender is also always verified, and all financially binding transactions are signed digitally.

12.3.1 eSafeID and Danske ID

eSafeID is Danske Bank's web-based security system for logging on to District. eSafeID is a two-factor authentication solution, based on something you know and something you have: a personal password and an eSafeID device that generates security codes, which can be used only once. These two factors are used to authenticate the person, after which sessions and customer-specific codes are generated and saved

temporarily in the browser session while the user remains logged on to District.

When a user is created in District using the eSafeID security system, the user receives a personal user ID, a temporary password and an eSafeID device. The user must activate the eSafeID device and create a personal password before the eSafeID security system can be used to access District.

Activation of the eSafeID device requires two-factor identification, of which the password/temporary password constitutes the first factor. If the user registered a mobile phone number when the user was created in District, an activation code can be sent as a text message and will constitute the second factor. If the user registered using his or her civil registration (CPR) number, activation is supported by the Finnish Trust network. Alternatively, the agreement administrator may complete the activation of a user who does not have the above options.

Users who have already been created and who receive a new eSafeID device must activate it before it can be used. The activation procedure is the same as that described above.

As an alternative to an eSafeID device, you can use a mobile authentication application provided by Danske Bank. This app is called Danske ID.

12.3.2 eSafekey
eSafekey is the security system in Danske Bank's Business API solution. When a user is to be created in District using the eSafekey security system, the user receives a personal user ID and a temporary password. The temporary password is used for first-time identification when the user is registered in the system.

12.3.3 EDIsec
EDIsec is a security solution used to protect data during direct data transmission between a customer and Danske Bank via a communication channel established between the customer and Danske Bank.

When a user is to be created using the EDIsec security system, Danske Bank allocates a personal user ID to the user, but not a temporary password. The validity of the customer's public EDIsec code is confirmed by the fingerprint that the customer must make of the code and that is exchanged with Danske Bank in accordance with the guidelines described in the EDIsec implementation guide.

12.3.4 OpenPGP
OpenPGP is a security solution used to protect data during direct data transmission between a customer and Danske Bank via a communication channel established between the customer and Danske Bank.

When a user is to be created using the OpenPGP security system, Danske Bank allocates a personal user ID and a temporary password to the user. The customer must generate the customer's own OpenPGP codes and send them to Danske Bank together with the temporary password in accordance with the instructions described in the OpenPGP Security Implementation Guide from Danske Bank.

If a certificate has been issued by a third party's issuer, Danske Bank regards the user as the certificate owner and thus as responsible for the validity of the certificate and updating thereof. Danske Bank uses only the public cryptographic code contained in the certificate.

The customer is responsible for acquiring and using suitable OpenPGP software (own or third-party software) that can handle OpenPGP security. This means that the software must be able, for example, to handle OpenPGP codes and file signing/encryption.

12.3.5 EDIsec codes and OpenPGP codes
For EDIsec and OpenPGP, a customer is responsible for using valid codes and securing data communication with Danske Bank. The following applies specifically:

- Danske Bank must have valid versions of the customer's codes. When the customer's personal codes are about to expire, the customer must ensure that the customer's public codes are exchanged with Danske Bank.
- The customer must use valid versions of Danske Bank's codes to secure the data communication with Danske Bank. When Danske Bank's public codes are about to expire, the customer must ensure that the customer's system is updated with a new version of Danske Bank's codes, which Danske Bank will make available.
- If the customer's codes are compromised, the customer must contact Danske Bank to have the codes blocked.

When Danske Bank receives a customer's public EDIsec code or public OpenPGP certificate, they will be stored in Danske Bank's IT infrastructure and will not be exchanged with parties outside Danske Bank.

Danske Bank is responsible for ensuring at any given time that valid versions of Danske Bank's public EDIsec code and public OpenPGP certificate are available to the customer.

13. Acquiring a user ID, temporary password and eSafeID device

When a user is created in District using the eSafeID security system, the user receives a personal user ID, a temporary password and an eSafeID device. Together with the eSafeID device, the temporary password is used for first-time identification when the user is registered in the system.

When a user is created using the EDIsec or OpenPGP security system, the user receives a user ID from Danske Bank. In OpenPGP, the user also gets a temporary password, which is used for first-time identification of the user.

The temporary password is machine-created and printed without anybody seeing it. If the letter containing the temporary password and/or the letter containing the eSafeID device has been tampered with or is not intact, the user must contact Danske Bank to order a new eSafeID device or a new temporary password. For security reasons, the letters containing the eSafeID device and the temporary password are sent at different times.

If the user has not received the letter containing the temporary password within seven business days of ordering, the user must, for security reasons, contact Danske Bank to cancel it and order a new one.

If the user has registered a mobile phone number in District, the user has the option of receiving the temporary password via text message. If the user does not receive a text message containing the temporary password within 15 minutes of ordering it, the user must, for security reasons, contact Danske Bank to cancel it and order a new one. When registering in the security system, the user must select a personal password and delete the temporary password. Danske Bank is not liable for any errors or losses resulting from the user or administrator not being able to update the user's mobile phone details in District.

During registration, the user creates his or her own password. The password must be changed regularly, and it is your responsibility to ensure that this happens. The user must then destroy the temporary password.

13.1 Storing user IDs, temporary passwords and eSafeID devices

You must implement effective security procedures to prevent unauthorised use of District, including unauthorised access to user code files and eSafeID devices.

The following rules apply to the use of eSafeID, e-Safekey, OpenPGP and EDISec:

- Only the user may use the user ID, password and eSafeID device.
- The password, eSafeID device and codes are strictly personal and may not be disclosed to third parties.
- The password and codes may be used only for communication with Danske Bank (except for OpenPGP, which you may use in other contexts)
- You may not write down the password and store it with the eSafeID device.
- Danske Bank recommends that you store secret codes in crypto hardware to the extent possible.

Further information about security recommendations is available under the Security menu in District, on the websites of Danske Bank and in other guidelines.

13.2 Deregistering or blocking the business´s or a user´s access to District

You must notify Danske Bank if you want it to remove the business's or a user's access to District. You must contact Danske Bank immediately to block user access if

- unauthorised use of a user's personal password, your business's or a user's code file or an eSafeID device is suspected
- third parties have gained access to a personal password or code file or an eSafeID device

Blocking can be requested or cancelled via District, telephone or one of Danske Bank's branches. If the request is made by telephone, the message must subsequently be confirmed in writing. However, the user will be blocked in the interim period.

You are responsible for all transactions executed by a user until Danske Bank has been requested to delete or block the user. You are also responsible for all future transactions previously ordered by a deleted/blocked user until Danske Bank has been notified that the transactions must be deleted and confirms that this is possible.

A user with administration rights may also delete and block a user's access to District, see sections 8.4.2 and 8.4.4.

13.3 Danske Bank´s right to block the business´s or a user´s access to District

Danske Bank reserves the right to block your business's or a user's access to District if we detect an attempt at unauthorised use. Danske Bank also reserves the right to

block your business's access to District if your business's equipment, software or interfaces damage, interfere with or in any other way cause inconvenience to Danske Bank or its IT infrastructure. If access is blocked, you will be notified of this as soon as possible.

14.Encryption bans
National legislation in the country in which District is being used may contain a general ban or restrictions on encryption. It is therefore important to be aware of a given country's legislation.

Part 3
Contractual entity of District

15. District – Corporate financial portal
District is intended for and is to be used for companies and corporations only. The information made available to the Customer, including price information, is solely for its own use. The Customer may not pass on the information to others, except by written permission from the Bank.

16. Changes to service and support
The Bank is allowed to change the Terms of Agreement and its District service.

The Bank shall notify the Customer in writing or electronically of any changes to the Agreement or its District service which considerably increase the liabilities of the Customer or considerably decrease the Customer's rights, and which are not prescribed by law, a decree by authorities or changes to the Banks' payment transmission system. The change will be in force as from the date notified by the Bank, however, no earlier than one (1) month from the date the notice of information was sent to the Customer. The Bank is entitled to notify of the change also by publishing it on the Bank's Internet pages at the address www.danskebank.fi. In these cases the said date starts from the time of publication of the change.

If the changes do not considerably increases the liabilities of the Customer or decrease the Customer's rights, or if the change is prescribed by law, a decree by authorities or changes to the Banks' payment transmission system, the Bank is entitled to notify of the change by publishing it in the branches of the Bank or on the Bank's Internet pages at the address www.danskebank.fi. The change will become valid on the date notified by the Bank.

The Agreement will stay valid as changed as from the date notified by the Bank unless the Customer terminates the Agreement before the change becomes valid.

17. Intellectual property rights
The owner right, copyright, brand and any other intellectual property right to the District service material are held by the Bank, unless notified otherwise. Quoting, copying, saving, changing, amending, transferring, and otherwise utilizing the material or even part of it without the Bank's prior written consent is strictly forbidden.

18. Responsibilities and liabilities in respect of use of the service
18.1 The Customer´s responsibilities
The Customer uses District at its own responsibility and risk and is responsible for the use of it of its authorized Users.

The Customer bears the risk in relation to sending information to the Bank and in relation to any transmission being destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during intermediate handling or processing of data content. The Customer also bears the risk in relation to information becoming accessible to third parties as a result of errors or unauthorized intrusion on the data transmission line.

The Bank is not liable for any consequences of omitting to fulfill the above responsibilities of the Customer.

It is the responsibility of the Customer to

- get the consent by the User before submitting his personal ID and other personal data to the Bank and to adhere to the valid jurisdiction in Finland relating to the protection of personal data,
- check that the User Rights created in the service always adhere to the authorizations given to the User by the Customer or third party,
- ensure that the contents of User Rights comply with the information which the Customer has notified the Bank.

Furthermore, it is the responsibility of the Customer to ensure that the Users are aware of the Terms and Conditions in the Agreement on District, and that all Users observe them, including that they comply with the on-screen Help function.

A Customer is responsible for

- all orders and other measures made using the Customer's own or its Users' Bank identifiers. No economic limit is placed on the Customer's responsibility for the use of Bank identifiers.
- ensuring that the Users keep their Bank identifiers in a safe place and in a way which disallows them to be known to third parties
- errors or misuse of any user of the District service.

The customer cannot make any claims on the Bank in respect of errors and omissions resulting from neglect to carry out actions which are the responsibility of the Customer, including non-observance of safety and control procedures. No economic limit is placed on the Customer's responsibility for the use of Bank identifiers.

Complaints about District service shall be submitted to the Bank immediately, no later than one (1) month after the Customer or the User has noticed or should have noticed the reason for the complaint.

18.2 The Bank´s responsibilities
The Bank will be liable for direct damages if, through errors or neglect, it is late in performing its obligations under this Agreement or performs its obligations in-adequately.

18.2.1 Indirect damage
The Bank is under no circumstances liable for indirect damages such as loss of income or revenue, interest rate loss, non-receipt of revenue, decrease or inter-mission of business activities, agreement between the Customer and a User or a third party, or for non-adherence to same, or for any other claims on the Customer by a third party.

18.2.2 Force majeure
The Bank is not responsible for any damage resulting from unusual or unforeseeable reason beyond the Bank's control and which the consequences of which it could not have avoided by careful action. Such reasons may be:

- decree by law or authority,
- war, threat of war, rebellion or riot,
- disturbance inn mailing services, automatic data processing, data transmission, other electronic communication or availability of electricity beyond the Bank's control,
- industrial action like strike, lockout, boycott or blockade, even if only part of the Bank's staff is involved in it or the staff of a subcontractor to the Bank, irrespective of whether the Bank is a part of it or not, or
- any other comparable reason acting excessively hampering the activities of the Bank.

The Bank is liable to inform the Customer of Force Majeure as soon as it is reasonably possible. Force Majeure entitles the Bank to discontinue its activities until further notice.

19. Other terms and conditions
19.1 Structure of the District Agreement
These Terms and Conditions are part of the complete District Agreement comprising also the following documents:

- District - Access Agreement,
- District – User Authorization,
- District – Instructions,
- District - Module Description,
- District – Service prices and cut off times,
- Terms and conditions for Electronic Communication,
- General terms and conditions for Corporate cards.

In addition, terms and conditions valid at any time shall be applied on the service. Such terms and conditions can be read in agreements applying to individual modules and service agreements. If there is contradiction between the different language version of these terms and conditions, the terms and conditions of the version in the Finnish language will apply in the first place.

The above terms and conditions of District will apply when the Customer and the Bank agree on District service or other electronic banking services. To those parts that the above terms and conditions contain no instructions in respect of electronic services, Bank's Terms and Conditions for Material Transmission Service and Terms and Conditions for Electronic Communication valid at any time will apply. By signing the Dis-trict Access Agreement the Customer confirms hav-ing read, understood and approved the above mentioned terms and conditions of Agreement as binding unto itself and as part of the agreed service.

The General Terms and Conditions for District service, Terms and Conditions for Material Transmission Service and the Bank's Terms and Conditions for Electron-ic Communication are accessible to the Customer at the address www.danskebank.fi/corporateterms
Furthermore, the Customer approves that the Bank may change its General Terms and Conditions of Agreement within the time frame of notice stated in these Terms and Conditions.

19.2 Service charges and fees
The Customer is liable to pay the Bank the service charges and fees notified in the List of service charges or agreed separately. The Bank is entitled to debit the service charges from the Customer's account.

The Bank may change its List of service charges. The Bank publishes the change of service charges or fees in its List of service charges. The change will become valid on the day notified by the Bank, however, no earlier than one (1) month after the publication of the change. If the change is based on a change in the decrees by law or authorities, the change shall become valid on the date notified by the Bank. The List of service charges is available in the branches of the Bank.

19.3 Transfer of the Agreement
The parties are not entitled to transfer any parts of the Agreement to a third party without the written consent of the other party. However, the Bank has the right to transfer the Agreement to a party in the same group as itself without prior notice to the Customer to this effect.

The rights and obligations based on this Agreement are valid to the recipient of the business activities if the Bank merges or splits or concedes its business wholly or in part.

19.4 Act on Payment Service and Advance information
If conflicts arise between the decrees in paragraph 7 of the Act on Payment Services (290/1.5. 2010) which are compulsory only to those in capacity of consumer, and these Terms and conditions, the Terms and conditions of this Agreement shall apply. The Bank digresses from the act on Payment Service to the effect it is possible based on the decree, unless other-wise agreed in this Agreement.
The Customer confirms having received sufficient advance information regarding the Agreement by signing this Agreement and by receiving its own copy of the Agreement, of these Terms and Conditions, and of other Terms and Conditions mentioned in these Terms and Conditions.

The above also applies if the company sends a collection request through District, and the request turns out to be unauthorized and the debtor subsequently seeks restitution.

19.5 Information about data protection
When dealing with the Bank in the capacity of being an individual, e.g. employee, director, beneficial owner and other individual associated to the Customer, the Bank registers and uses the personal data of the individuals to offer the Customer the best advice and solutions, and to comply with the legal requirements that apply to the Bank as a financial institution. More information about what such personal data the Bank registers, how the Bank uses it and the Customer's rights is written in the Bank's privacy notice www.danskebank.fi/tietosuoja, which can also be provided in hard-copy for the Customer. The notice also provides contact information if any questions arise.

When the Customer, or anyone on behalf of the Customer, provides the Bank with personal data, the Customer warrants that the Customer is entitled to dis-close such personal data. The Customer also ensures that the person has been informed where to find the Bank's privacy notice.

20. Termination of the Agreement and restricting service use

20.1 Termination
The Customer may terminate the District Access Agreement without notice by notifying the Bank hereof in writing. Fees, expenses and service charges debited in advance shall not be reimbursed although they when the service or Agreement is terminated apply to the time after the time of termination.

The Bank may terminate the Agreement with one (1) month's written notice either in District service, by mail or in a branch office.

Service requests and orders made during the validity of this Agreement will be carried out by the Bank. The Customer is responsible for all obligations and responsibilities with regard to service requests made under this Agreement and in the name of the customer during the time of termination. The Customer's or User's right to use District will cease when the time of termination has elapsed.

20.2 The Bank´s right to terminate the Agreement
The Bank is entitled to terminate this Agreement with immediate effect if the use of District or its module has been discontinued or prevented due to misuse or essential breach of the Agreement by the Customer or a User.

Termination shall be notified in District or by mail. The Agreement will cease when a notification of termination has been sent.

20.3 Restriction of service use
The Bank has the right to discontinue or block the use of the service, its part or module when

- it is necessary due to maintenance or repair;
- the devices, software, systems of communication connections used by the Customer cause damage or disruption or otherwise endanger the security or operating condition of the Bank's services;
- it is necessary to protect the Customer from an information security threat, another security-related threat or unauthorized use;
- the Customer or User are guilty of misuse, breach of the Agreement or an essential breach of the Agreement; an essential breach of the Agreement is a situation in which the Customer omits to pay service charges as agreed in the Access Agreement, is subject to bankruptcy proceedings or other insolvent administration of its estate, negotiates for a composition or is subject to an execution or attachment order;

- the Bank holds that it has another justified reason for it. The justified reason may be, for example, that the Customer or User is the target of international or other sanctions that the Bank must be complied with according to law, official regulations or agreements.

If the service, its part or module is used as a means of payment in accordance with the Finnish Payment Services Act (290/2010), the Bank is entitled to prevent its use as described in Section 57 of the Payment Services Act.
The Bank will notify the Customer of a restriction referred to in this section of the Agreement in advance in writing or by using an electronic messaging system or, if necessary, to prevent or limit damage, immediately after the restriction has been imposed. The Bank will not, however, provide notification of the matter if the notification would endanger the reliability of security of the services offered by the Bank, or if such notifications are forbidden by law.

21. Governing law
This Agreement is governed by Finnish law and the le-gal venue is Finland irrespective of in which country District is used. If any disputes arising from this agreement cannot be settled through negotiation, such disputes shall be settled in the District Court of Helsinki, in Finnish.

If the Customer is registered as a User of a module that is solely intended to be used abroad, the Customer accepts – to the same extent as the Bank – which it is subject to the Acts and usage applying in the country where the Customer operates as well as any particular terms and conditions relating to the specific country and the use of the module in that country.

22. Definitions and glossary
Authorization: Authorization by the customer to a physical person or a registered authority to represent itself in a legally binding way in District. The authorization can be e.g. access authorization to District, the bank's general authorization form or any other authorization form by the bank for District.

Authorization holder: One or several registered (legal entity or natural) person who have been granted authorization are registered in District.

Bank: Danske Bank A/S, Finland Branch, company registration No. 1078693-2.
Postal address: Televisiokatu 1, PL 1561, 00075 DANSKE BANK. Tel +358 (0) 10 515 15. Web page www.danskebank.fi. BIC code (SWIFT address) DABAFIHH. The bank is the Finland branch of Danske Bank A/S which is registered in Denmark, and thus part of Danske Bank Group. Business ID code number of Danske Bank A/S is 61126228.

Banking credentials: Credentials consist of a user ID, passwords and security devices as defined in the Bank's currently valid terms and conditions of online banking.

Banking days: Saturdays, Sundays, public holidays in Finland, 1 May, Midsummer Eve, 6 and 24 December and days not otherwise considered as banking days are not banking days in Finland.

Basic products are simple products, available from time to time in Business Online.

District: is the collective term for Danske Bank's Internet-based payment and information systems for companies. It covers both the District webbased interface where customers can create payments, administrate users, see account information etc. – as well as the system enabling customers to exchange information (files) with Danske Bank via a data communication channel secured by either EDIsec or OpenPGP Security.

Certificate: An electronically exchangeable document used for holding at least one security key and associated identification and verification information.
Confidential payments: Confidential payments are payments (e.g. wages and salaries) that may only be viewed or processed by users with special privileges. Payments classified as confidential can only be processed by users with these privileges.

Cross-border payment: A payment is classified as a cross-border payment if it is paid between Finland and an ETA country in another currency than that of an ETA country, or in any currency between Finland and a non-ETA country. This applies to payments between registered accounts as well as to payments to unregistered accounts.

Customer: A legal company or other corporate customer having a District Access Agreement based customer relationship with the Bank in respect of a product or a service. The customer may also be a physical person if he is performing business activities and uses the service offered by the Bank in his business activities.

Danske Bank Group: Danske Bank A/S, its subsidiaries and branches in Finland and other countries.

Data transmission: Transfer of data between customer and bank. For example, a data transmission may contain payment instructions by the customer to the bank.

Digital signature is an electronic signature appended to binding transactions, e.g. payments, and used when linking to Danske Bank.

eSafeID device is personal. The devices come in various formats. A common feature is that they show a security code to be used when logging on to District with the eSafeID security system.

eSafeID is a web-based security system to log on to District. eSafeID is a two-factor authentication system consisting of something the user knows (the personal password) and something the user has (the eSafeID device that generates security codes).

EDISec is a security system used for integrated solutions when connecting to Danske Bank's systems via data communication channels.

Encryption keys are used for the e-Safekey, EDISec, and OpenPGP Security systems. Each user generates an encryption key that comprises a pair of keys: a private key to create digital signatures and a public key to confirm the digital signature and encrypt data from Danske Bank to the customer. Each user has a secret encryption key in order to create unique, personal digital signatures. Access to use the encryption key is protected by the user's personal password. The encryption key is stored in the company's IT environment.

e-Safekey is a security system used for integrated solutions to connect to District.

International sanctions: Sanction, economic sanction, ban on export or import, embargo or other restrictive measure imposed, administered, approved or implemented by the Finnish Government, the United Nations, the European Union, The United States of America or the United Kingdom or their competent authorities or bodies.

Module agreement: An agreement containing provisions about the individual module and the services contained in it, as well as rights, obligations and liabilities connected to it, e.g. Trade Finance.

Module description: Bulleted short description of the functionality of the individual modules.

OpenPGP Security is a security system used for integrated solutions to connect to Danske Bank's systems via data communication channels.
Password is a code to protect a user's private key that is used to create digital (electronic) signatures.

Payments between registered accounts: Payments between registered accounts within the Danske Bank Group, which are registered in the same country.

Party: In this agreement, the customer, the bank or the user separately or together.

Role ID: A six-charcter aplhanumeric ID assigned to the individual District user. The Role ID is stated in the User Authorization.

Security code is used together with the user ID and the personal password for logging on to District with the eSafeID security system.

Security registration is the registration process that a user must go through before using District for the first time.

Security device: A personal device, tool or application that the Bank gives to the Customer or the User for an identification purpose.

Support Direct is a function at Danske Bank offering technical support or support for District users by tele-phone.

Temporary password is generated by Danske Bank that sends it to the company's user(s). The password consists of four or eight characters and is used by the company's user(s) for registering in District.

Transactions are payments, collections, other operations and queries in District.

User: A user is a person who has been authorized by the customer to act on its behalf via District. Any actions by the user are binding for the customer. If your company's and Danske Bank's IT systems are directly integrated, a user may also be a computer or system located within your company.

User Authorization: The customer's authorization of a user, specifying the services, accounts, authorizations and duties to which the individual user has right and access.

23. Customer service and regulating authorities

In matters regarding District, the Bank should always be contacted primarily by sending the Bank a request for contact via District, using a form on the Bank's web page or by phoning the telephone service for corporate customers, tel. +358 (0) 100 2580 (lnc/mnc).

The Customer may also contact the following regulating authorities:
The Bank's operations are supervised by the Finanstilsynet, Århusgade 110, DK-2100 Copenhagen Ø, Den-mark, telephone +45 33 55 82 82, www.finanstilsynet.dk.

Within the scope of the authority, the operations of the Bank are also supervised by the Financial Supervisory Authority, Snellmaninkatu 6, P.O. Box 103,
FI-00101 Helsinki, Finland.

The Bank's activities are supervised in the case of consumer issues, also by the Consumer Ombudsman (www.kkv.fi), Finnish Competition and Consumer Authority, P.O. Box 5, FI-00531 Helsinki Finland,
telephone +358 (0)29 505 3000 (switchboard).

LETTER OF CONSENT

I hereby consent to

Name of company (hereinafter called the Customer)

Business ID

Address

Passing on my name and identity number to Danske Bank. The information is passed on so that I can be cre-ated as a User under the Customer's District agreement. The Bank has the right to register the User Right issued by the Customer under my identity number.

The information may be used within the Bank and Danske Bank Group for administration transactions agreed between the Customer and the undersigned in connection with my creation as a User under the Customer's District service agreement.

Date

Full name

Signature

Identity number

_____