Terms and Conditions
District

25 June 2021

Danske Bank

Contents

Introduction

District is Danske Bank's Internet-based office-banking system, which provides access to account information, payments and other banking transactions requested by the company.

The Terms and Conditions for District include a description of the system.

Part 1 – describes the options available in District and how to use the system.
Part 2 – describes the security requirements for District users.
Part 3 – describes the contractual aspects of connecting to District.

Part 1 – District –general description

1. Modules and services

District comprises separate modules and services.

The Module Description comprises a description of the modules and services available via the company's Access Agreement.

2. Transactions

District allows the company to, for example, make payments and queries on balances and movements in accounts registered in District via the Access Agreement. Payments and queries are jointly referred to as transactions.

3. Registered accounts

Accounts must be registered in District before a company can make transactions via District. Accounts are registered via the Access Agreement.

3.1. Registered accounts within the Danske Bank Group

Accounts opened with Danske Bank and affiliates of the Bank under this agreement are accounts within the Danske Bank Group.

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

- Accounts held by the company and opened in the name of the company
- Accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate to the company authorising the latter to act on behalf of the third party or subsidiary

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

3.2. Registered accounts managed via SWIFT

Accounts opened with banks outside the Danske Bank Group, and accounts within the Group which the company wishes to use for transactions via SWIFT MT101 or MT940, can also be registered in District via the Access Agreement. The company may register both its own accounts and third-party accounts. The company or third party must conclude an agreement with the account-holding bank concerning payment requests via MT101 or an agreement on Balance Reporting via MT940.

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

3.3. Registered accounts in Norwegian Banks

Accounts opened with Norwegian banks outside the Danske Bank Group which the company wishes to use for balance reporting and transactions, must be registered in Danske Bank. The company can register both its own accounts and third-party accounts. The company or third party must conclude an agreement with Danske Bank and the account-holding bank concerning balance reporting or payment requests in District.

Third-party accounts can only be registered if the third party has issude a mandate to the company.

4. Unregistered accounts

If accounts held by the company and/or a third party are not registered in District, it is only possible to make payments into these accounts. It is not possible to inquire about or make payments from unregistered accounts.

5. Cheque payments

The company may make payments by issuing a foreign cheque drawn on a registered account within the Danske Bank Group.

If the company and/or a third party has an agreement concerning payment requests via MT101, cheques can also be drawn on registered accounts outside the Danske Bank Group, provided that this option is included in the agreement between the company and/or third party and the bank outside the Danske Bank Group.

Issued cheques are regarded as banker's cheques, and the amounts are debited from the accounts on the date of issue.

The company may have the proceeds of uncashed cheques deposited in registered accounts.

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

6. Requests

A request by the company or its users for a transaction in District, for example a payment, is called an electronic request.

6.1. Submission of requests

When a user submits an electronic request on behalf of the company and/or a third party, the Bank sends an electronic receipt. The moment we have confirmed receipt of the request, the risk in relation to its being carried out in accordance with the instructions passes to the Bank.

6.2. Binding requests

Requests carried out in accordance with the instructions in the electronic request are binding on the company. Consequently, the Bank cannot reverse payments, trades in foreign exchange or securities or other transactions, including cheque issuance, finalised in accordance with the request.

6.3. Retention of requests

We retain electronic requests for at least ten years. During this period, the company and/or third party whose account is debited may obtain a hardcopy of the request against payment of the fee charged by the Bank for extraordinary assistance.

7. Use of electronic communications - eArchive

The Bank may send all information and messages as electronic documents to eArchive within District.

The company will be notified in Dikstrict every time a new type of document from the Bank becomes available in electronic form in eArchive. The Bank may however decide at any time to send a document by ordinary mail. Where possible, the Bank will give notice of this in District.

Information and messages that the company has received in electronic form will have the same legal effect as if the documents had been sent by ordinary mail.

If the company is a customer of one or more of the Danske Bank Group's other companies, and they send documents to the company electronically, the Group may also send them to District in electronic form.

7.1. Who has access to the documents

The rights and authorisations to accounts, depots, products and services granted to the individual user determine which documents the user can view in District. Users with query access to the account(s) have access to the documents in eArchive linked to the specific account(s).

7.2. Archiving

The Bank will retain the electronic documents in eArchive for the current year plus five years as a minimum. The company should be aware, however, that the documents will be deleted if the company deregisters an account, changes customer number or cancels District. In such cases we recommend that the company save the documents itself.

If the company needs to keep the documents for a longer period than the Bank allows via District, it should save the documents for its own files.

7.3. Deregistering eArchive

If the company does not wish to receive documents in eArchive, it must notify the Bank of this. Subject to agreement, the Bank may forward documents by ordinary mail, against payment of a fee.

7.4. Termination

If the company's District agreement is cancelled, its registration number changes or accounts are removed from its District agreement, it will no longer be able to receive or retrieve electronic documents from eArchive either. See section 7.2 Archiving, etc.

8. User Authorisations for Districte

All users performing transactions in Districtmust be duly authorised to do so by the company. This authorisation is created via the Bank's User Authorisation District.

If a third party has signed a mandate to the company, the company may delegate this mandate to a user. This is done via the User Authorisation in District.

When creating a User Authorisation for District, the company must obtain the user's consent before passing on his or her national identity number to the Bank.

If a user needs to have cash access, e.g. to carry out transactions via the cashier's

desk, the company must sign the Mandate – Corporate customers form.

8.1. Digital channel access

Users can access District via various browsers and Business Apps. The company may deny a user access to District via Business Apps. Regardless of the choice of channel, each user has only the rights set out in the User Authorisation for District.

8.2. Administrator privileges

Companies with access to the Administrator module must consider whether users are to be granted administrator privileges. The following administrator privileges may be granted:

- Agreement Administrator
- User Administrator
- Agreement Information
- PIN and blocking
- Payment Limit – Account

For users granted Agreement and/or User Administrator privileges, the company must decide what level of authorisation the user is to have. The following may be granted:

- Create/set-up
- Separate authorisation
- Two persons jointly (A authorisation).

For a description of our authorisation types, see section 10.

8.3. Agreement Administrator

A user who is granted Agreement Administrator privileges will be able to

- create, modify and delete Agreement Administrator privileges
- create, modify and delete User Administrator privileges – see section 8.3
- create and delete Agreement Information privileges – see section 8.4
- create and delete user privileges in relation to PINs and blocking – see section 8.5
- Create, edit and delete Payment Limit – Account privileges – see section 8.6.

Agreement Administrators may grant these privileges to themselves and others.

When a user with Agreement Administrator privileges creates or modifies a user with Agreement Administrator privileges, a User Authorisation with a signature field is generated in District. The User Authorisation is accessible in eArchive to users with Agreement Information privileges. The User Authorisation must be signed by the company and sent to the Bank. In other cases, the user accepts and signs using his or her digital signature.

Users with Agreement Administrator privileges also have User Administrator privileges.

8.4. User Administrator

A user who is granted User Administrator privileges will be able to

- create and modify users, including giving users access to modules, products and services, accounts, authorisations and transaction types
- create and delete users' access to ordering basic products – see section 9.1
- create and modify user master data

- delete all user details, including master data.

User Administrators may grant these privileges to themselves and others.

8.5. Agreement Information

Users with Agreement Information privileges can access the users on the agreement and view their individual privileges (including master data, modules, administrator privileges, access to accounts and payment access).
Users also have access to selected documents shown in District.

8.6. Log-on and Blocking

A user whom you grant Log-on and Blocking privileges is authorised to perform the following on behalf of your company:

- order temporary PINs for users
- order eSafeID device and complete activation of a new eSafesID
- block and unblock users

8.7. Payment Limit - Account

A user whom you grant Payment Limit – Account privileges is authorised 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 authorisations should be granted to the user:

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

Our account authorisation types are described in section 10.

8.8. Access to accounts

For each user, the company must state which accounts the user may inquire about and/or make payments from. If the company authorises a user to make payments from an account, the user is granted access to the transaction types determined by the company.

For each account that the user is granted access to, the user's authorisation must be stated. The following authorisations are available at account level:

- Separate authorisation
- Two persons jointly (A authorisation)
- Two persons jointly (B authorisation)
- Two persons jointly (C authorisation)

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

Note that the authorisation granted at account level is reflected in all District agreements under which the account is registered.

8.9. Transaction types

For each user, the company must state which transaction types the user is to have access to:

Payments between registered accounts in the same country within the Danske Bank Group
Payment requests via SWIFT MT101
Payments to unregistered accounts within or outside the Danske Bank Group, including cheque payments

Cross-border payments accounts within or outside the Danske Bank Group Furthermore, the company must state whether the user is to be authorised to create and approve, or only to create, the payments selected. If the user is authorised to both create and approve payments, the relevant authorisations for each transaction type must also be stated. The following authorisations are available at transaction level:

- Create/set-up
- Separate authorisation
- Two persons jointly (A authorisation)

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

In general, the selected authorisation is used for all payments within each payment type. If the company has selected a more restrictive authorisation at account level, this authorisation will apply for payments to unregistered accounts and cross-border payments. Note that if the user has not been granted any authorisation at account level, this is also regarded as a restriction.

8.10. Confidential payments

The company must state whether the user is authorised to make confidential payments. Confidential payments include payments such as wages and salaries, which may only be viewed, created or approved by users with these privileges.

Users are authorised to make confidential payments within the transaction types to which they have been granted access.

Note that no distinction is made between confidential and non-confidential payments in connection with account queries.

8.11. Changing District User Authorisations

If the company wishes to extend or limit a user's access to District, a new User Authorisation for District must be issued, replacing the previous one.

- If the change relates to the user's authorisations at account level, the company and/or third party must also sign an account mandate.

Note that a user's authorisation in District may be affected if the company issues a Mandate – Corporate customers.

8.12. Revoking District User Authorisations

User Authorisations for Dikstrict remain in force until revoked by the company in writing. Authorisations may also be revoked by telephone, but this must always be followed up by immediate written confirmation. The user's access to act on behalf on the company via District is blocked after the telephone call.

When the Bank has received notice of revocation, we will send written confirmation that the user number and key have been deleted in its systems.

If the company terminates the entire District Access Agreement, the Bank construes this as revocation of all User Authorisations granted under the agreement.

If the company and/or a third party has granted the user an account mandate, this mandate must be revoked separately. It is not sufficient for the company merely to revoke the District user authorisation.

9. Other mandates in District

9.1. 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 authorise the user to make binding agreements - on behalf of the company - about the products available from time to time in Ordering of Basic Products in District.

9.2. Third-party mandates granted to the company

If the company wishes to make transactions on third-party accounts with the Danske Bank Group, the third party must sign the Bank's third-party mandate form.

If account queries are to be possible on third-party accounts outside the Danske Bank Group, an agreement stating that the Danske Bank Group may receive data about the third party's external account(s) must be submitted to the Bank.

If the company is to make payments from the third party's accounts outside the Danske Bank Group, an agreement stating that the company may send payment instructions to the third party's bank(s) via the Danske Bank Group must be submitted to the Bank.

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

9.3. Third parties right to order product and services

Third party who has, with consent from the Company, entered into the District Agreement as third party, has the right to enter into an agreement with an external third party (e.g. Servicebureau) with use of the District agreement.

9.4. Authorisation to buy/sell foreign exchange and securities

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 to buy and sell Norwegian and foreign shares, bonds and investment certificates, the user must have access to one or more Markets Online modules. Access to buy and sell foreign exchange spot and forward and to buy and sell shares, bonds and investment certificates also requires that the company grants the user Currency trading and/or Securities trading authorisations. These authorisation only authorise the user to perform transactions on behalf of the company 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 company and the Bank.

The User Authorisation District must state the accounts and custody accounts that the user is authorised to inquire about or trade in.

9.5. Trade Finance Authorisation in District

If a user is to be able to issue letters of credit, collect debt and/or issue guarantees, the company must register the user for the Trade Finance module and sign the Connection to/Modification of the Trade Finance Module in District agreement. In this connection, the company must state whether the user is to have access to letters of credit (exports and/or imports) debt collection (exports and/or imports) guarantees.
Furthermore, the company must state whether the user is to have access to

- create and inquire
- create and approve – two persons jointly (A authorisation)
- create and approve – separately (Separate authorisation)

9.6. Collection Service SEPA Direct Debit authorisation in District

To be able to create SEPA Direct Debit collections, the user must be registered for the Collection Service - SEPA Direct Debit module. This will give the user access to

- collections
- reimbursements
- revocations

in euro accounts attached to District.

10. Authorisation types

10.1. Authorisation types

The Bank operates with the following authorisation types:

Separate authorisation

- Two persons jointly (A authorisation)
- Two persons jointly (B authorisation)
- Two persons jointly (C authorisation)

These authorisations allow the company to specify which users may, separately or jointly, approve a payment or request. The authorisations are described in the following.

10.2. Separate authorisation

When requests or payments are created or changed by a user with this authorisation, they are automatically deemed to have been approved by the user. Users with this authorisation can also approve requests or payments entered by users with all other authorisation types.

10.3. Two persons jointly (A authorisation)

When requests or payments are created by a user with an A authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A, B or C authorisation is required.
Users with A authorisations rank equally, and the order of approval is therefore of no consequence.

10.4. Two persons jointly (B authorisation)

When requests or payments are created by a user with a B authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A or C authorisation is required. Two users with B authorisations cannot jointly approve a payment.

10.5. Two persons jointly (C authorisation)

When requests or payments are created by a user with a C authorisation, they are

automatically approved by this user (1st approval).
Further approval (2nd approval) by a user with Separate, A or B authorisation is required. Two users with C authorisations cannot jointly approve a payment.

11. Customer support

The Bank provides support and service to the company. Support and service includes

- user administration
- on-site support
- telephone support
- Internet-based support functions

User administration often includes establishment of Access Agreements and authorisations, adjustment of the company's and its users' access to the various support and service features, deletion and blocking of users, ordering of temporary PINs and registration of modifications to authorisations, etc.

On-site support may include installation of and training in District, as well as related troubleshooting. Troubleshooting may result in adaptation and/or modification of the computer set-up and the company's IT systems, including modification of registration databases, installation of routers, firewalls and proxy servers, internal security systems and other software and hardware modifications. Installation and troubleshooting take place in cooperation with the company's IT department and at the risk of the company.

Telephone support may include training, user instruction, troubleshooting assistance and guidance in relation to modification. Telephone support in connection with installation, set-up, training and troubleshooting, etc. of District is provided in cooperation with the company's IT department and at the risk of the company.

Internet-based support may include training, user instruction, troubleshooting assistance and guidance in relation to modifications. Internet-based support is provided in cooperation with the company's IT department and at the risk of the company.

Part 2 – District – security system

12. Technical issues

12.1. Transmission and access

In order to use District, the company must establish a data communication link with the Bank. The company must establish and bear the costs related to the link and must purchase, install, set up and maintain the required IT equipment.

Likewise, the company must ensure the necessary adaptations to its IT equipment – in order to use the link and ensure 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

The Bank distributes the programs required to install District. The company must download the programs from the Internet.

When programs are downloaded from the Internet, the company or a user must check that the program delivery has been electronically (digitally) signed by the Bank.

If the programs have not been electronically signed by the Bank, the reason may be that they have been tampered with or do not come from the Bank. The signature can subsequently be verified by checking the properties of the downloaded program file(s). If the electronic signature is not from the Bank, the downloaded program may not be installed.

The Bank may at any time and without notice modify its own equipment, basic software and related procedures in order to optimise operations and service levels. We will provide notification of any modifications requiring adaptation of the company's equipment in order to retain the link and access by giving one month's written notice via District or otherwise.

12.3. **Data security**

BankID, eSafeID, e-Safekey, EDISec, and OpenPGP Security are the general security systems used in District.
BankID and e-safeID are security solutions for webbased log on and signing in District.

e-Safekey, EDISec, and OpenPGP Security are Danske Bank supported security systems for the customers who want to exchange information with Danske Bank electronically directly through their own business systems.

e-Safekey, EDISec, and OpenPGP Security use permanent digital signing and encryption keys stored in the company's IT environment.

Using these security systems ensures that data is encrypted and/or electronically signed before being transmitted to and from Danske Bank and is not tampered with during transmission. In addition, the authenticity of the sender's digital signature is always checked, and all financially binding transactions are provided with a digital signature.

12.4. **eSafeID security system**

eSafeID is Danske Bank's web-based security system to log on to District. The eSafeID is a two-factor authentication system, which means that it is based on something you know (your personal password) and something you have (your eSafeID device that generates security codes).

When a user is to be created in District with the eSafeID security system, Danske Bank gives the user an individual 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. The user can also activate the eSafeID device by using BankID. Alternatively, the agreement administrator

may complete the activation of a user without 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.

12.5. BankID

Precondition to use BankID is that the BankID user has a norwegian social security number (11 digits) or a d-number, and have a BankID issued from a Norwegian bank. BankID can be used to log on and sign wihtout use of other security solution.
BankID is a standard security solution for users with a norwegian social secutity number.
For BankID is the following logon and signing options available for District;

- BankID

Using BankID for log on to District give users with access to sevral District agreements, the option to select agreement and switch between agreements without making a new log on.

12.6. eSafekey

e-Safekey is the security system in Danske Bank's Business API solution.
When a user is to be created in District with the e-Safekey security system, Danske Bank gives the user an individual user ID and a temporary password. The temporary password is used for first-time identification when the user is registered in the security system.

12.7. EDISec

EDIsec is a security solution used to protect data in direct data transmission between the customer and Danske Bank via a communication channel established between the customer and Danske Bank. When a user is to be created for data communication with the EDISec security system, Danske Bank gives the user an individual user ID but no temporary password. Validity of the customer public key is ensured by generating a fingerprint of the key and exchange it with Danske Bank according to the EDISec implementation guide.

12.8. OpenPGP Security

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

When a user is to be created for data communication with the OpenPGP Security system, Danske Bank gives the user an individual user ID and a temporary password. Initially, an OpenPGP Security certificate is generated containing the security keys. The certificate is sent to Danske Bank together with the temporary password according to the OpenPGP Security implementation guide.

If an OpenPGP Security public certificate is issued by a third party issuer on behalf of a customer, Danske Bank will hold the customer as owner of the key and thus responsible for the validity and maintenance of the certificate.

It is the responsibility of the customer to acquire and maintain its own or third party OpenPGP Security software to handle the OpenPGP Security concept. Among other things the system must be able to handle certificates and have encryption and signing features.

12.9. EDISec keys and OpenPGP certificates

For EDISec and OpenPGP Security, it is the responsibility of the customer to ensure usage of valid keys at any time for securing Data communication. To be more specific, the customer must make sure that:

- Danske Bank has got a valid set of the customer's public keys. When the customers public keys are about to expire then the customer must update the bank with new public keys (provided by the customer).

- The customer is using a valid set of Danske Bank's public keys for securing the data communications. When Danske Bank's public keys are about to expire the customer must ensure that the customer's system is updated with a new version of Danske Bank's keys , which Danske Bank will make available

- If customer keys are compromised or damaged, then they should be revoked by contacting the bank.

When Danske Bank receives the customer's public EDISec key or public OpenPGP Security certificates the keys/certificates will be stored in Danske Bank's systems in a secure way and will not be shared with anyone outside Danske Bank.

It is the responsibility of Danske Bank to make sure that a valid set of the bank's public EDISec key or OpenPGP Security certificates are always available to the customer.

13. Access

13.1. Acquiring a user ID and a temporary PIN and eSafeID device

When a user is to be created in District with the eSafeID security system, Danske Bank gives the user an individual 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 security 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 system-generated and printed electronically without anybody seeing the combination. If the letter containing the temporary password and/or the letter containing the eSafeID device has been opened or is not intact, the user must contact Danske Bank to order a new temporary password and/or a new eSafeID device. For security reasons, the letters containing the temporary password and the eSafeID device are not sent at the same time.

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

If the user has registered his or her mobile phone number in District, the user will have the option to receive the temporary password in a text message.
If the user does not receive the text message with 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.

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

Danske Bank is not liable for any errors or losses caused by a failure of the user or administrator to update the user's mobile phone details in District.

13.2. Storing the user ID, personal password and eSafeID device

The customer 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, EDISec and OpenPGP Security:

- Only the user may use the user ID, personal password and eSafeID device
- The password, eSafeID device and security codes are strictly personal and must not be shared with any third parties
- The password and security codes may be used only when communicating with Danske Bank
- The user may not write down the password and store it with the eSafeID device.
- Danske Bank recommends that the customer 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.

13.3. Deregistration or blocking the business's or a user's access to District

The customer must notify Danske Bank if it want to remove the business's or a user's access to District. The customer or user must immediately contact Danske Bank 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
- For BankID as a security solution the userID need to be blocked as the user can log in and sign without a having an additional separate security solution issued from Danske Bank.

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.

The customer 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 8.3 and 8.4

13.4. 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. Ban on encryption

Local, national legislation in the country where District is used may include a general ban or limitations on encryption. Therefore, it is important to be familiar with national legislation.

Part 3 – Contractual aspects

15. For business purposes only

District is to be used for business purposes only. The information made available to the company, including price information, is solely for its own use. The company may not pass on the information to others, except by written permission from the Bank.

16. Changing District

District gives access to products and services offered by the Bank at any time. The Bank may at any time extend or reduce the scope of District. The bank may extend the scope of District without notice. When the bank adds new services to District this will not require new signatures from the company, provided that the new services are advantageous to you and do not imply any material cost increase. If the bank reduces the scope and/or content we may only do so with 30 days' prior notice.

The Bank shall provide written information of any changes via Business Online or otherwise The company shall be considered to have accepted the changes if the company does not give the Bank written notice to the contrary and terminates the District agreement before the date of implementation of the change.

17. Changes to service and support

The Bank may change the scope and content of its service and support at any time by giving one month's written notice via District or otherwise. The price list shows the prices charged for the various services and support functions.

18. Responsibilities and liability

18.1. The company's responsibilities

The company uses District at its own responsibility and risk.

The risk borne by the company includes, but is not limited to, the risk in relation to

- sending information to the Bank, as well as the risk that a transmission is destroyed, lost, damaged, delayed or affected by transmission errors or

omissions, e.g. during intermediate handling or processing of data content
- information becoming accessible to third parties as a result of errors or unauthorised intrusion on the data transmission line
- misuse of District

The company cannot hold the Bank liable for any consequences thereof.

It is the responsibility of the company to
- check that the content of User Authorisations always matches the authorisations given to the user by the company and any third party
- ensure that the content of the User Authorisation is in accordance with the company's wishes

Furthermore, it is the responsibility of the company to ensure that users are aware of the Terms and Conditions for District, and that all users observe them, including that they comply with the on-screen Help.

The company is responsible for
- all operations and transactions made using the company's own key or that of a registered user
- ensuring that users keep their passwords secure so that no third party becomes aware of them
- ensuring data security in connection with storage of user keys in the company's IT environment to prevent unauthorised access to the keys
- any incorrect use or misuse of District by registered users

The company cannot make any claims on the Bank in respect of errors and omissions resulting from the company's circumstances, including non-observance of safety and control procedures.

18.2. The Bank's responsibilities

The Bank will be liable for damages if, through errors or neglect, it is late in performing its obligations under the Agreement or performs its obligations inadequately.

However, the Bank is not liable for errors and omissions resulting from
- errors and omissions in third-party software which is part of the District security system
- a user's disclosure of the temporary PIN and/or the password
- modifications to the security system (not performed by the Bank)
- the security system's integration with other systems or software not supplied by the Bank

In areas that are subject to stricter liability, the Bank will not be liable for losses resulting from
- IT system failure/downtime or corruption of data in these systems as a result of the events listed below, irrespective of whether the Bank operates the systems itself or has outsourced operations
- telecommunication or power failures at the Bank, statutory intervention or administrative acts, natural disasters, wars, rebellions, civil unrest, acts of sabotage, terrorism or vandalism (including computer viruses and hacking)
- strikes, lockouts, boycotts or blockades, irrespective of whether the conflict is targeted at or initiated by the Bank or its organisation and irrespective of the cause of the conflict. This also applies if

the conflict affects only parts of the Bank
- any other circumstances beyond the Bank's control

The Bank's exemption from liability does not apply if

- the Bank should have predicted the circumstances resulting in the loss at the time when the agreement was concluded, or should have prevented or overcome the cause of the loss
- legislation under any circumstances renders the Bank liable for the cause of the loss

In accordance with general liability provisions in force the Bank is liable for direct losses attributable to errors made by the Bank. Apart from that, its liability is limited to remedying the deficiencies. No further claims can be made against the Bank, including for indirect or consequential damage.

19. Other terms and conditions

19.1. Structure of the District Agreement

A District Agreement is comprised by:

- Access Agreement District
- User Authorisation(s) District
- Module Description District
- Terms and Conditions District
- General Terms for deposits and payment orders – corporate customers
- Prices for District
- The "Getting Started" user guide on the District website and on-screen Help

as well as other sets of rules applying at any time, as stated in the individual Module Agreements.

By signing the Access Agreement for District the Company also acknowledges having read and accepted the above set of rules, which forms part of the Agreement. The Terms and Conditions for District and other terms and conditions in force at any time are accessible at www.danskebank.no/betingelser.

19.2. Prices

The Bank may at any time change its prices by giving written notice via District or otherwise. We will debit various fees and charges from the account(s) specified as fee account(s).

19.3. Other amendments to District agreements

The Bank may unilaterally amend the District agreement to the detriment of the company one month after the Bank has sent notice of the amendment to the Customer.

The Bank notifies the Company about the amendment in writing through District or otherwise.

The Company shall be considered to have accepted the amendment if the company does not give the bank written notice to the contrary and terminates the District agreement before the date of implementation of the amendment.

19.4. Assignment, transfer and third parties

This Agreement has been concluded by the Bank on behalf of the Danske Bank Group. This means that any member of the Danske Bank Group is entitled to fulfil and enforce this Agreement. It also means that the Bank may transfer its rights and

obligations to another member of the Danske Bank Group at any time.

The Bank is entitled to transfer the performance under this Agreement to subcontractors. Such transfer shall not affect the responsibilities of the Bank under the Agreement.

20. Termination and breach

The company may terminate the Access Agreement without notice – provided that it does so in writing. Requests and agreements made before the time of termination will be carried out. Paid subscription fees will not be refunded. The Bank may terminate the Access Agreement in writing by giving one month's notice.
The Bank may, however, terminate the Agreement without notice if the company is in breach of the Agreement, including the Terms and Conditions for District. The company is in breach if it, for example, omits to pay as agreed in the Access Agreement, suspends its payments, 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.

21. Choice of law and legal venue

Disputes or claims and all other issues between the customer and the bank that have arisen in connection with or are linked to these business terms are to be resolved pursuant to Norwegian law, with Trondheim District Court as the legal venue.

If the company is registered for a module that is solely intended to be used abroad, the company accepts – to the same extent as the Bank – that it is subject to the legal rules and usage applying in the country where the company operates.

22. Definitions and glossary

- **Access Agreement**: Agreement between the company and the Bank concerning the use of District.
- **Authorisation/mandate:** Either User Authorisation for District, Mandate – Corporate customers, District account mandate or one of the Bank's other mandate forms for District.
- **Authorisation/mandate holder**: One or more registered mandates or authorisations and/or physical persons who have been granted authorisations/mandates.
- **Banking days**: Saturdays, Sundays, public holidays, Constitution Day and 24 December are not banking days in Norway.
- **Basic Products:** are simple products, available in District at any given time and are subject to change.
- **Business Online** is the former designation for Danske Bank's internet-based payment- and information systems for businesses. A reference to Business Online is therefore a reference to District.
- **District**: an Internet-based payment and information system.
- **Confidential payments**: Confidential payments are payments (such as wages and salaries) that may only be seen 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 a cross-border payment if it crosses a national border – even if it involves only

one transaction currency, e.g. the euro. This applies to payments between registered accounts as well as payments to unregistered accounts. In the countries where the Danske Bank Group is represented, payments between accounts in the same country are not cross-border payments.

- **Customer support**: Function at the Bank offering technical support or support for District users by telephone.
- **Data delivery**: Transfer of data between customer and bank. For example, a data delivery may contain payment instructions.
- **Digital signature**: An electronic signature appended to binding transactions, e.g. payments, and used when linking to the 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 via data communication channels.
- **Encryption keys** are used for the e-Safekey and EDISec 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.
- **Instruction:** Electronic, written or oral request to the Bank to carry out changes, transactions, etc.
- **Keys**: Each user generates two keys (a set of keys) – a private key used to generate digital signatures and a public key used to verify the digital signature. Each user has his or her own private key in order to create unique, personal digital signatures. Access to use the keys is protected by the user's password. The keys are stored in a key file or key database on the company's IT system.
- **Master data**: First name, middle name (if any), surname, user name, customer number, national identity number and related company's address.
- **Module agreement**: An agreement containing provisions about the individual module, e.g. Trade Finance or Collection Service.
- **Module description**: Bulleted description of the functionality of the individual modules registered under the agreement.
- **On-site support**: Training, technical assistance or other assistance provided by the Bank at the company's premises.
- **OpenPGP Security**: A security system used for integrated solutions to connect to Danske Bank's systems via data communication channels.
- **Password**: A code to protect a user's private key that is used to create digital

(electronic) signatures. The password is at least 4 characters and must contain at least one number.

- **Payments** between registered accounts: Payments between registered accounts in the same country within the Danske Bank Group
- **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**: The registration process that a user must go through before using District for the first time.
- **Temporary PIN**: A code issued and sent by the Bank to the company's user(s). The code consists of four or eight characters and is used by the company's user(s) to register in the District security system.
- **Transactions**: Payments, payment requests and queries in District.
- **User**: A user is a person (for example an employee) who has been authorised by the company to act on its behalf via District. If the company's and the Bank's IT systems are directly integrated, a user may also be a computer or system located within the company.
- **User Authorisation**: The company's authorisation of a user, specifying the services, accounts, authorisations and privileges to which the individual user has access.
- **User ID**: A six-character number assigned to the individual District user. The ID might contain both numbers (digits) and upper letters. The User ID is stated in the User Authorisation.

Danske Bank
Enterprise No. NO 977 074 010 MVA

Danske Bank A/S
Erhvervs- og Selskabsstyrelsen CVR-nr. 61 12 62 28

Holmens Kanal 2-12
DK-1092 København K - Danmark