September 2014

Special Terms and Conditions for Business eBanking

(Please note that these Special Terms and Conditions apply in addition to the General Terms and Conditions for Business. In the event of a conflict between these Special Terms and Conditions and the General Terms and Conditions for Business, the General Terms and Conditions for Business shall prevail.)

Introduction
Business eBanking is Danske Bank's Internet-banking system, which provides access to account information, payments and other banking transactions requested by our business customers such as you.

These Terms and Conditions for Business eBanking include a description of how Business eBanking operates.
Part 1: describes the options available in Business eBanking and how to use the system.
Part 2: describes the security requirements for Business eBanking users.
Part 3: sets out some contractual aspects for connecting to Business eBanking

Part 1-Business eBanking - general description

1. Modules and services
Business eBanking comprises separate modules and services. The Module Descriptions comprise a description of the modules and services available via your Access Agreement.

Please note that not all Business eBanking Services are available through our Business Mobile Banking App. You accept that by using a Mobile Device to access Business eBanking you will only have access to a reduced range of services, full details of which can be viewed on our website.

It is important that You and each User only download the Business Mobile Banking App in accordance with the Terms and Conditions agreed with Apple (for the App store) and Google (for Google Play).

2. Transactions
Business eBanking allows you to, for example, make payments and queries on balances and movements in accounts registered in Business eBanking via the Access Agreement. Payments and queries are jointly referred to as "**transactions**". Use of your Digital Signature shall be your authorisation of and consent to payments through the Business eBanking service. It also allows you to collect payments as an originator e.g. under the SEPA Direct Debit Scheme. Where this applies you will have entered a separate agreement with the Bank.

3. Registered accounts

3.1 Accounts must be registered in Business eBanking before you can make transactions via Business eBanking. Accounts are registered via the Access Agreement.

3.2 The following accounts can be registered in Business eBanking: (a) Accounts held by you and opened in your name with the Bank and affiliates and divisions of the Danske Bank Group, (b) Accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate to you authorising you to act on behalf of the third party or subsidiary.

3.3 Registered Accounts within the Danske Bank Group can also be managed via SWIFT MT101 or MT940; see Clause 3.4 for further details.

3.4 Accounts opened with banks outside the Danske Bank Group, and accounts within the Danske Bank Group which you wish to use for transactions via SWIFT MT101 or MT940, can also be registered in Business eBanking via the Access Agreement. You may register both your own accounts and third-party accounts. You or the third party must conclude an agreement with the account-holding bank concerning payment requests via MT101 or an agreement on balance reporting via MT940.

4. Unregistered accounts
If accounts held by you and/or a third party are not registered in Business eBanking, it is only possible to make payments into those accounts. It is not possible to inquire about or make payments from unregistered accounts.

5. Foreign Drafts
You may make payments by issuing a draft drawn on a Registered Account within the Danske Bank Group.

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

Issued drafts are regarded as banker's drafts, and the amounts are debited from the accounts on the date of issue. You may have the proceeds of uncashed drafts

deposited in Registered Accounts. If the proceeds from uncashed drafts are to be credited to your or a third-party's account, you or the third party must covenant to indemnify the Bank if a draft is subsequently presented.

6. Requests

A request by you or your Users for a transaction in Business eBanking, for example a payment, is called an electronic request.

6.1. **Submission of requests**

When a User submits an electronic request on your behalf and/or on behalf of a third party, we send an electronic receipt. The moment we have confirmed receipt of the request, the risk in relation to it being carried out in accordance with the instructions passed to us.

If a payment is authorised on your behalf but provides an incorrect Unique Identifier to us to identify the payee, we will not be liable if we process the payment in accordance with that Unique Identifier, but we will make reasonable efforts to recover the funds involved however, you agree that we may charge for this.

If we refuse to execute a payment authorised on your behalf via our Business eBanking Service, we shall notify you of this refusal as soon as possible by telephone, in writing, by email, by fax or such other reasonable means we may select.

6.2. **Binding requests**

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

6.3. **Retention of requests**

We retain electronic requests for at least seven years. During this period, you and/or the third party whose account is debited may obtain a hardcopy of the request against payment of the fee charged by us for Administrative Assistance. Details of our current fees and charges can be found in our "**Clear & Simple: Business Fees & Charges Explained**" brochure.

7. Receipt of documents in eArchive

eArchive is both an archive and an electronic mailbox facility provided by the Bank via our Business eBanking service. eArchive is used to send correspondence from us to you (electronic mail) electronically and without the need for any paper copies of that electronic mail to be sent to you. As a Business eBanking customer you will be automatically registered for receipt of certain documents by electronic mail.

The type of electronic mail that we will send to you electronically can be changed from time to time and we reserve the right to send you mail in either electronic form only, paper form (via ordinary mail) only or both electronic and paper form.

7.1. On registration for eArchive, all future documents sent by us in electronic form will be sent to your eArchive. You agree that you will no longer receive these documents by ordinary mail in paper form. You also agree to receive electronic mail to your electronic mailbox from us to the same extent and with the same legal validity as paper-based mail. You must use our eBanking Service and have an electronic mailbox if you want to receive documents from us in electronic form under this Agreement. Accounts of a Third Party for which You have access rights will be treated in the same manner as Your own Accounts.

7.2. Documents that you receive in your electronic mailbox could include statements of account, confirmation notes, payment advices, various other statements (annual summaries, total summaries), payment statements and updates of terms and conditions. These are merely examples and the number of types and volume of documents you will receive in your eArchive will gradually increase. You will receive separate notification in your Business eBanking inbox each time a new type of document becomes accessible in your electronic mailbox which you will no longer receive by ordinary mail.

7.3. You may temporarily activate postal delivery of paper documents. These documents will however still be visible in eArchive. You agree that once you have requested this service you will then receive all documents sent by the Bank to you in paper form by ordinary mail as well as in digital format in your eArchive. We undertake to complete this activation within one week of receipt of your request to revert to paper delivery. If you wish to amend this service to receive your documents from us in electronic form only, you must contact us requesting the reactivation of the electronic only delivery service. We may take up to one week to reactivate this service. For the avoidance of doubt all documents previously sent to eArchive will remain stored in your eArchive.

7.4. Users with viewing access to an Account will have access to the documents relating to that Account in eArchive.

7.5. We store the contents of documents sent electronically in accordance with applicable legislation.

7.6. If you cease to be a Business eBanking customer you will lose access to the contents of your electronic mailbox and you should take such steps as you deem appropriate to retain copies of any electronic mail that we have sent to you. You should be aware that once you export information from a secure website it will no longer be secure.

7.7. You are responsible for opening and checking documents sent electronically from us. You should check the electronic documents carefully as you

would ordinary, paper-based documents. Your responsibility is the same as if the documents were paper-based and had been sent by ordinary mail.

7.8. If you do not have access to Business eBanking for a certain period of time, you must notify us immediately whether you wish to terminate your Agreement and receive paper-based documents by ordinary mail in future, or want to continue receiving the documents electronically. You may also temporarily suspend the delivery of electronic mail (see clause 7.3).

7.9. We reserve the right to send to you documents (which you would normally receive electronically as a result of this Agreement) in paper-based form by ordinary mail.

7.10. We may terminate this agreement in accordance with the Special Terms and Conditions applicable to our Business eBanking.

8. User Authorisations for Business eBanking

All Users performing transactions in Business eBanking on your behalf or a third party must be duly authorised to do so by you. This authorisation is created via the User Authorisation in Business eBanking.

Where the Access Agreement states that You have accepted the Administration Module the User Authorisation will also specify whether the User has been granted Administration privileges. The User Authorisation will specify what those Administration Privileges are. Condition 8.1 describes the different types of Administration privileges that may be specified on the User Authorisation. The Bank may from time to time update and increase the types of administration privileges available. Any new or additional types of administration privileges will be governed by these terms and conditions. You will receive separate notification of any such changes via Business eBanking or otherwise. Where a User has been granted Administration rights then references to you in these Special Terms and Conditions should be construed accordingly so that anything which an Administrator does under the terms of the User Authorisation shall be treated as if it was done by you.

If a third party has signed a mandate in favour of you, you may delegate this mandate to a User. This is done via the User Authorisation in Business eBanking.

When creating a User Authorisation for Business eBanking, you must obtain the User's consent before passing on his or her personal data to the Bank.

If a User needs to have manual access to Accounts, e.g. to carry out transactions at a post office or sign cheques, you must sign an account mandate form (which you can obtain from us) authorising the User to do so.

8.1. **Administrator Privileges**

Where you have access to the Administrator Module you must consider whether you will grant a User Administrator privileges. The following is a non-exhaustive list of Administrator privileges which may be granted. A comprehensive list is available in Business eBanking.

- Agreement Administrator
- User Administrator
- Agreement Information
- Log-on and Blocking
- Payment Limit – account
- Cards Administrator
- Markets Online Administrator
- Corporate Notifications Administrator
- Trade Finance Administrator

For Users granted Agreement and/or User Administrator privileges, you must also decide the level of authority that User will have i.e. whether the user shall be granted:

- Separate authorisation
- Two persons jointly (A authorisation)

The various authorisations granted by the Bank are described in Clause 11.

A User granted Agreement and User Administration privileges must have the same approval rights for both privileges.

8.2. **Agreement Administrator**

A User who is granted Agreement Administrator privileges is authorised to perform the following on behalf of the company:

- request that users be granted Agreement Administrator privileges or that such privileges be modified
- delete Agreement Administrator privileges
- create, modify and delete User Administrator privileges – see section 8.2.1
- create and delete Agreement Information privileges – see section 8.2.2
- create and delete user privileges in relation to Log-ons and blocking – see section 8.2.3
- request that Users be granted privileges, or that such privileges be modified, in relation to the setting of Payment Limits on any of the registered accounts – see section 9.1.2

In addition Agreement Administrators may grant these privileges to themselves and others.

Requests for Agreement Administrator privileges to be allocated to a User must always be confirmed in writing to the Bank and such confirmation must be signed by persons legally authorised to sign on your behalf. When a User with Agreement Administrator privileges has requested the creation or modification of a User Authorisation with Agreement Administrator privileges, a User Authorisation with a signature field is generated in Business eBanking and delivered to your eArchive.

This pre-populated User Authorisation will be accessible to Users with Agreement Information privileges who can then print the User Authorisation and arrange for it to be signed as above and sent to the Bank.

In other cases, the User accepts and signs using his or her digital signature. Users with Agreement Administrator privileges will also have User Administrator privileges automatically.

8.2.1. **User Administrator**

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

- create and modify users, including giving Users access to the required modules, accounts, authorisations and transactions types
- create and modify User master data
- delete all User details, including master data

Note: User Administrators can grant these privileges to themselves and others.

8.2.2. **Agreement Information**

Via a User overview, Users with Agreement Information privileges can search currently registered Users and view their individual privileges (including master data, modules, Administrator privileges, access to Accounts and the ability to make payment instructions).

Users have access to the User overview and selected documents shown in Business eBanking.

8.2.3. **Log-on and Blocking**

A User who is granted Log-on and blocking privileges is empowered to perform the following on behalf of the company:

- order temporary Pins for Users
- order eSafeID device
- block and unblock User access

This privilege can only be granted as a separate authorisation.

8.2.4. **Payment limit – account**

A User who is granted Payment limit – account privileges is authorised to perform the following on behalf of the Customer - create, edit and delete payment limits on the accounts which the User has been granted access to.

For Users granted Payment limit – account privileges, the User Authorisation will specify the extent of the User's authority to access and use the Service. This will include whether the User has been granted:

- separate authorisation
- two persons jointly [A Authorisation]
- two persons jointly [B Authorisation]
- two persons jointly [C Authorisation]

8.2.5. **Cancellation of the Administration module**

If the Customer cancels the Administration module, then the Payment Limits which have been authorised will continue to be applicable to the Agreement. In respect of any accounts which are opened after the date of cancellation of the Administration module, Payment Limits on Accounts will not apply but Payment Limits on Users will continue to apply. The Customer must contact the Bank in writing if he wishes to amend or cancel any Payment Limits which have been authorised.

After cancellation of the Administration module any Users who have been granted automatic access to future accounts will not have automatic access to any future accounts opened.

8.2.6. **Collect ion Service SEPA Direct Debit authorisation in Business eBanking**

To be able to create SEPA Direct Debit collections the Customer must register the User for the Collection Service - SEPA Direct Debit module. This will give the User access to:

- Collections
- Reimbursements
- Refunds

8.2.7. **Card Administrator**

A User who is granted Cards Administrator privileges is authorised to perform the following on behalf of the Customer:

- Block a card;
- Re-order a card
- Order and re-order a PIN for a card
- Change a card limit
- View card information
- Update Cardholder Information
- It is not currently possible for Users to order a new card. However it is intended that this functionality will be introduced shortly and You will be notified in Business eBanking once this functionality becomes available.

To view transactions on a card account a User must hold viewing rights for the Account in question.

The Customer and each cardholder will need to enter into separate documentation with the Bank. This document will confirm among other things that; (i) the cardholder has read and accepted the terms and conditions for use of the relevant card now published and up-dated from time to time on the Bank's website, and; (ii) that the Bank exchanges information with business partners for the establishment and administration of additional benefits of the card – and for the processing of any claims. The Customer warrants that it will have the cardholder sign this document prior to the issue of the card and agrees that it will also be required to

forward such documentation to the Bank on their demand.

8.2.8 **Markets Online Administrator**

A User who is granted Markets Online Administrator privileges is authorised to perform the following on behalf of the Customer - Create, edit and delete user authorizations relating to the trading in securities or foreign exchange via Business eBanking or viewing trades via Business eBanking.

In order to trade securities or enter into foreign exchange contracts on behalf of a Customer must execute the applicable mandate in writing for that User.

8.2.9 **Corporate Notifications Administrator**

A User who is granted Corporate Notifications Administrator privileges is authorised to perform the following on behalf of the Customer:

- create notification subscriptions for Users
- read notifications received
- manage User information
- delete subscriptions for Corporate Notifications created by Users

The Bank may charge a fee for notifications sent to Users. Such fees will be notified to you in Business eBanking. Where you grant a User Corporate Notification Rights you acknowledge and agree to pay to the Bank any fees associated with notifications created using the Corporate Notifications Administration privileges.

8.2.10 **Trade Finance Administrator**

A User who is granted Trade Finance Administrator privileges is authorised on behalf of the Customer to create, modify or delete user authorisations relating to trade finance instructions provided to the Bank using the Trade Finance Module as set out in Clause 10.3 below.

The various types of authorisations are described in Clause 11 below.

9. Viewing documents

A User may view a number of documents in eArchive in Business eBanking.

The rights and authorisations granted to the individual User determine which documents the User can view in Business eBanking.

A User will, for instance, be able to view his or her individual User Authorisation in Business eBanking.

9.1.1 **Access to accounts**

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

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 us are described in Clause 11 below.

Note that the authorisation granted at account level is reflected in all Business eBanking Agreements under which the account is registered.

9.1.2. **Payment Limits**

Where You have included the Administration module in your Business eBanking Agreement, you may control the value of payment orders created and/or approved through Business eBanking either at an account level which applies to all Users [knows as Payment limit - account] or on individual Users [known as Payment limit - user]. It is your responsibility to create Payment Limits suitable for his requirements. If a Payment Limit is exceeded, payments may not be processed until appropriate action is taken by you. [Please refer to our Getting Started Guide on Administration – Payment Limits for more information]

In exceptional circumstances the Bank may, at its discretion, agree to create a Payment Limit on your behalf on receipt of written instructions.

9.2. **Transaction types**

For each User, you must state which transaction types the User is to have access to:

- Payments between accounts registered under the Agreement in the same country within the Danske Bank Group
- Payment requests via SWIFT MT101
- Euro payments into accounts in SEPA countries not registered on Business eBanking within or outside the Danske Bank Group - including payment by drafts
- Cross-border payments to registered and unregistered accounts within or outside the Danske Bank Group.

Furthermore, you 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:

- Separate authorisation
- Two persons jointly (A authorisation)

The various authorisations granted by us are described in Clause 9.

In general, the selected authorisation is used for all payments within each payment type. If you have 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.

9.3. **Exchange Rates**

Cross-border payments to registered and unregistered accounts within or outside the Danske Bank Group can be processed:

- Without exchange – where no exchange is required. For example, the payment is being made in the same currency as the beneficiary account;
- Bank's fixing rate – We will use our published rate of exchange [known as the "Danske Bank Exchange Rate (IRL)"] for the relevant currency on the applicable day at such time as we may select. For transactions over €50,000 the rate of exchange will usually be at least equal to the published rate, if not better;
- Bank's Spot Rate – no longer available for Electronic Payments;
- Agreed Rate – A rate agreed in advance with the Bank for the specific payment. An Agreement number must be held by you to use this rate;
- Forward Rate – A rate agreed in respect of a Forward Contract agreed between us. A Forward Contract number must be held by you to use this rate

9.4. **Confidential payments**

You 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.

9.5. **Corporate Notifications**

A User may subscribe for different Corporate Notifications in the Notification Centre in Business eBanking.

The rights and authorisations granted to a User determine the notifications which the User can subscribe for in the notification centre.

The Bank may charge a fee for notifications sent to Users. Such fees will be notified to you in Business eBanking. Where a User has access to Corporate Notification you acknowledge and agree to pay to the Bank any fees associated with notifications created by those Users.

9.6. **Changing Business eBanking User Authorisations**

If you wish to extend or limit a User's access to Business eBanking, a new User Authorisation for Business eBanking must be signed (physically or using your Digital Signature on Business eBanking where applicable), replacing the previous one.
If the change relates to the User's authorisations at account level, you and/or the relevant third party must also sign an account mandate.
Note that a User's authorisation in Business eBanking may be affected if you issue an account mandate form.

9.7. **Revoking Business eBanking User Authorisations**

User Authorisations for Business eBanking remain in force until revoked by you in writing - physically or using your Digital Signature on Business eBanking where applicable.

When we have received notice of revocation, we will send written confirmation that the User number and Key(s) have been deleted in our systems.
If you terminate the Agreement, we will construe this as revocation of all User Authorisations granted under the Agreement.
If you and/or a third party have granted the User an account mandate, this mandate must be revoked separately. It is not sufficient for you merely to revoke the User Authorisation.

10. Other mandates in Business eBanking

10.1. **Third-party mandates granted to you**

If you wish to make transactions on third-party accounts with the Danske Bank Group, the third party must sign our third-party mandate form.

If account queries should be possible using SWIFT MT940 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) shall first be submitted to us.

If you should make payments from the third party's accounts outside the Danske Bank Group using SWIFT MT101, an agreement stating that you may send payment instructions to the third party's bank(s) via the Danske Bank Group shall first be submitted to us.

The Bank registers the third-party accounts in Business eBanking via your Access Agreement.

10.2. Authorisation to buy/sell foreign exchange and securities

If a User should have access to information, be able to view trade positions and buy and sell foreign exchange spot and forward, the User must have access to one or more 'Markets Online' modules. Access to buy and sell foreign exchange spot and forward also requires that you grant the user currency trading and/or securities trading

authorisations. These authorisations only authorise the User to perform transactions on your behalf via 'Markets Online'.
All transactions relating to the purchase and sale of foreign exchange spot and forward are subject to the provisions of the separate framework agreement on netting and final settlement of trades concluded between you and us.

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

10.3. **Trade Finance Authorisation in Business eBanking**

If a User should be able to issue letters of credit, collect debt and/or issue guarantees, you must register the User for the 'Trade Finance' module and sign the 'Connection to/Modification of the Trade Finance Module' in the Access Agreement or grant the user authorisation to the Trade Finance Module using the Administration Module within Business eBanking . In this regard, you must state whether the User shall have access to:

- letters of credit (exports and/or imports)
- debt collection (exports and/or imports)
- guarantees

Furthermore, you must state whether the User shall have access to:

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

11. 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 you to specify which Users may, separately or jointly, approve a payment or request. The authorisations are described below.

11.1. **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.

11.2. **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.

11.3. **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.

11.4. **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.

12. Business Mobile Banking App

12.1. To be eligible to access Business eBanking through the Business Mobile Banking App you must have completed and signed an Access Agreement and you together with each User must be registered for the Bank's Business eBanking service, have a Device and otherwise comply with any requirements set down by the relevant software application distributor.

12.2. When a User downloads the Business Mobile Banking App to a Device you accept that these conditions apply in relation to the use of Business eBanking by you or that User via the Business Mobile Banking App. In addition, the use of the Business Mobile Banking App is subject to the terms and conditions of the licence under which it may be downloaded from the App Store and Google Play and any other relevant software application distributor.

12.3. The Business Mobile Banking App currently gives access to the following content and Account services:

- View Balances;
- View Transactions;
- View history of transactions;

The Bank may from time to time update, extend or reduce the Business eBanking services offered via the Business Mobile Banking App from time to time. The bank may extend the scope of the Business eBanking services offered via the Business Mobile Banking App without notice and add new services to the Business Mobile Banking App without advance notice and without obtaining new signatures from you, provided that the new services are advantageous to you, whereas one month's notice is required prior to any reduction in the scope and/or content (unless we are required by

law, regulation or regulatory requirement to give you a longer notice period, in which case we will give you such longer notice period).

12.4. **Security**

In addition to any other obligations or responsibilities you may have under these Terms and Conditions, you and each User must take all reasonable steps to maintain the confidentiality of any information shown or stored on the Device in connection with your use of the Business Mobile Banking App. You are solely responsible for the safety and security of your Device.

You and each User should as a minimum take the following steps to protect your Account information:

- Set a PIN on the Device, change it regularly and keep your keypad locked;
- Ensure that you and each User logs-off from any Business Mobile Banking App session as soon as you have finished availing of the relevant service(s); and
- Keep the Device in your possession at all times and do not leave your Device unattended where it may be accessed by unauthorised persons.

12.5. The Business Mobile Banking App is currently free of charges from the Bank, however you should refer to your network service provider for any additional charges that could be imposed by them. If you use Mobile Banking

Certain services on the Business Mobile Banking App, use location data sent from a Device which can be turned off by you or a User at any time if you wish. If you use these services you consent to collection and processing of this location data.

13. Cookies

By using Business eBanking you consent to the use of cookies which are required to enable Business eBanking to operate effectively. Full details of our policy in relation to cookies can be found on our website.

14. Customer support

The Bank provides support and service to you. Support and service includes:

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

User administration often includes establishment of Access Agreements for new clients and authorisations, adjustment of your and your 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 our office-banking system, as well as related troubleshooting. Troubleshooting may result in adaptation and/or modification of the computer setup. Installation and troubleshooting take place in cooperation with your IT department and at your risk.

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 Business eBanking is provided in cooperation with your IT department and at your risk.

Internet-based support may include training, User instruction, troubleshooting assistance and guidance in relation to modifications. Internet-based support is provided in cooperation with your IT department and at your risk.

Part 2 - Business eBanking - security system

15. Technical issues

15.1. **Transmission and access**

In order to use Business eBanking, you must establish a data communication link with us. You must establish and bear the costs related to the link and must purchase, install, set up and maintain the required IT equipment.

Likewise, you must ensure the necessary adaptations to your IT equipment in order to use the link and ensure continuity of operations.

We may at any time and without notice modify our 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 your equipment in order to retain the link and access by giving one month's written notice via Business eBanking or in such other manner as we shall determine.

15.2. **Distribution, control and storage of software**

We distribute the programs required to install Business eBanking. You must download the programs from the Internet.

If we send CD-ROMs, they are sealed, and you must check that the seal is unbroken. If it has been broken, the program may have been tampered with and should not be installed. You must contact us immediately for a new set.

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

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

15.3. **Data security**

eSafeID,and EDISec are the general security systems used in Business eBanking. Using systems ensures that:

- data is kept confidential (encrypted) during transmission to us
- data is not modified during transmission to us
- the sender is always identified
- a Digital Signature is appended to all financially binding transactions.

A User's Digital Signature is created using a combination of the individual's User ID, a Password and a Security Code generated by the eSafeID device.

We reserve the right to block the your or a User's access to Business eBanking for objectively justified reasons relating to the security of the Business eBanking service or if we register attempts at misuse. If access is blocked, you will be notified immediately by telephone, in writing, by email, by fax or other such reasonable means we may choose and we will unblock access to Business eBanking if the reasons for blocking cease to exist.

If you wish to apply for unblocking of your access to Business eBanking please contact the Business eBanking helpdesk, your Relationship Manager or by phoning 1890 866 860.

You must implement effective security procedures to prevent unauthorised use of Business eBanking and unauthorised access to User Keys.

16. Acquiring a User ID, temporary password and eSafeID device

When a user is to be created in Business eBanking with the eSafeID or EDISec security system, we give the user an individual user ID, a temporary PIN and an eSafeID device. Together with the eSafeID device, the temporary PIN is used for first-time identification when the user is registered in the security system.

The temporary PIN is system-generated and printed electronically without anybody seeing the combination. If the letter containing the temporary PIN and/or the letter containing the eSafeID device has been opened or is not intact, the user must contact us to order a new temporary PIN and/or a new eSafeID device. For security reasons, the letters containing the temporary PIN and the eSafeID device are not sent at the same time.

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

On registering in the security system, the user chooses a personal Password and must subsequently destroy the temporary one.

Once the user has selected a Password, he or she will be required to create a one-off Security Code using the eSafeID device.

16.1. **Storing the user ID, Password and eSafeID device**

The following rules apply to the use of eSafeIDand EDISec:

- Only the user may use the user ID, Password and eSafeID device
- The User ID, Password and eSafeID device are strictly personal and must not be shared with any third parties
- The User ID, Password and eSafeID device may be used only when communicating with Danske Bank
- The Password must not be written down and stored together with the eSafeID device

16.2. **Password**

The User should select a Password that is as difficult as possible to guess – for example using upper and lower-case letters, numbers and symbols.

The User must ensure that other users do not know the Password and must store it in a suitable and safe manner, see Clause 14.3.

16.3. **Changing the Password**

You must prepare guidelines to ensure that the User regularly changes his or her Password. It is your responsibility to ensure that the guidelines are observed.

For further information, read the security recommendations under the 'Security' menu in Business eBanking on the Website and any other guidelines provided or made available to you from time to time.

16.4. **Deregistering Users**

You must inform us if Users should be deleted. You are responsible for all transactions performed by a User until we are requested to delete or block the User.

16.5. **Misuse or risk of misuse**

You or the user must immediately contact Danske Bank in order to block user access if

- either of them suspects that their Password, or the eSafeID device has been misused or that others have had access to the Password, or have gained possession of the eSafeID device

17. Ban on encryption

You should be aware that local, national legislation in the country where Business eBanking is used may include a general ban or limitations on encryption. Therefore, national legislation should always be checked.

Part 3 - Contractual aspects

18. For business purposes only

Business eBanking is to be used for business purposes only. The information made available to you, including price information, is solely for your own use. You may not pass on the information to others, except by written permission from us.

19. Changing Business eBanking

Business eBanking gives access to the services offered by us at any time.

We may at any time extend the scope of Business eBanking without advance notice, whereas one month's notice is required prior to any reduction in the scope and/or content (unless we are required by law, regulation or regulatory requirement to give you a longer notice period, in which case we will give you such longer notice period). We shall provide written information of any changes via Business eBanking or otherwise.

20. Changes to service and support

We may change the scope and content of our service and support at any time by giving one month's written notice via Business eBanking or otherwise. The list of fees attached to these Special Terms and Conditions shows the fees charged for the various services and support functions.

21. Responsibilities and liability

21.1 **Your responsibilities**

You use Business eBanking at your own responsibility and risk.

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

- sending information to us, 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 Business eBanking

You cannot hold us liable for any consequences thereof.

It is your responsibility to:

- check that the content of User Authorisations always matches the authorisations given to the User by you and any third party
- ensure that the content of the User Authorisation is in accordance with your wishes
- ensure that the content of the User Authorisation is in accordance with the User's wishes
- inform us as soon as possible if you find that the statement of any registered account includes any item authorised via Business eBanking which seems to be incorrect. On becoming aware of an unauthorised amount having been debited to such an account, you should telephone Danske Bank on 1890 866 860 or your Relationship Manager as soon as possible and, in any event, no later than thirteen months after the debit date in which case you will be able to obtain a refund from us, subject to all applicable laws and if a prompt investigation by us demonstrates that the transaction was, in fact, unauthorised. You should confirm such telephone call in writing to Danske Bank or your Relationship Manager within seven days.

Furthermore, it is your responsibility to ensure that Users are aware of the Special Terms and Conditions for our Business eBanking Services, and that all Users observe them, and that they comply with the on-screen Help requirements.

You are responsible for:

- all operations and transactions made using your 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 Users' Keys in your IT environment to prevent unauthorised access to the Keys
- any incorrect use or misuse of Business eBanking by registered Users

In the event that any Password or Digital Signature or Key relating to your access to our Business eBanking Service has been misappropriated or used in an unauthorised manner, you must notify us by telephoning Danske Bank on 1890 866 860 or your Relationship Manager. You should confirm your notice by writing within seven days to Danske Bank or your Relationship Manager.

Subject to any applicable laws, you cannot make any claims on us in respect of errors and omissions resulting from you circumstances, including non-observance of your safety and control procedures.

21.2 **Our responsibilities**

We will be liable for damages if, through errors or neglect, we are late in performing our obligations under the Agreement or perform our obligations inadequately.

However, we are not liable for errors and omissions resulting from:

- errors and omissions in third-party software which is part of the Business eBanking security system
- a User's disclosure of the Temporary PIN and/or the Password
- modifications to the security system (not performed by us)
- the security system's integration with other systems or software not supplied by us.
- In areas that are subject to stricter liability, we 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 we operate the systems itself or has outsourced operations
- telecommunication or power failures at our offices, 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 us or our organisation and irrespective of the cause of the conflict. This also applies if the conflict affects only parts of our organisation
- any other circumstances beyond our control.

Our exemption from liability does not apply if:

- we 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 us liable for the cause of the loss.

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

22. Other terms and conditions

22.1 **Structure of the Business eBanking agreement**

An agreement in relation to Business eBanking (an "**Agreement**") is comprised of the following:

- the Access Agreement
- all User Authorisation(s)
- all Module Descriptions
- these Special Terms and Conditions to each of which our General Terms and Conditions for Business also apply
- our "Clear & Simple: Business Fees & Charges Explained" brochure.
- the "Getting Started" user guide on the Business eBanking website and onscreen Help as well as other sets of rules applying at any time, as stated in the individual module agreements or the Access Agreement

By signing the Access Agreement for Business eBanking you also acknowledge having read and accepted all parts of the Agreement.

22.2 **Prices**

We may at any time change our prices by giving one month's written notice via Business eBanking or otherwise (save where we are required by applicable law, regulation or regulatory requirement to provide you with a longer notice period, in which case we will do so). We will debit various fees and charges from the account(s) specified as fee account(s). Details of our current fees and charges can be found in our "Clear & Simple: Business Fees & Charges Explained" brochure.

22.3 **Assignment, transfer and third parties**

Your Agreement has been concluded by us on behalf of the Danske Bank Group. This means that any member of the Danske Bank Group is entitled to fulfil and enforce your Agreement. It also means that we may transfer our rights and obligations there under to another member of the Danske Bank Group at any time.

We are entitled to transfer the performance under your Agreement to subcontractors. Such transfer shall not affect our responsibilities under your Agreement.

23. Termination and breach

You may terminate the Access Agreement without notice - provided that you do so in writing. Requests and agreements made before the time of termination will be carried out. Paid subscription fees will not be refunded.

We may terminate the Access Agreement in writing by giving one month's notice (or such longer notice period as we may be required by law or regulatory requirement to give you).

We may, however, terminate the Access Agreement without notice if you are in breach of any part of your Agreement. You are in breach if you, for example, omit to pay as agreed in the Access Agreement, suspend your payments, are subject to bankruptcy proceedings or other insolvent administration of your estate, negotiates for a composition or are subject to an execution or attachment order.

24. Governing law

This Agreement is governed by Irish law and subject to the jurisdiction of the courts of Ireland.
If you are registered for a module that is solely intended to be used abroad, you accept – to the same extent as us – that you are subject to the legal rules and usage applying in the country where you operate.

25. Definitions

Defined terms used in these Special Terms and Conditions shall have the meanings given to them in the General Terms and Conditions for Business, unless otherwise defined herein.

Access Agreement: Agreement between you and us concerning the use of Business eBanking.
Agreement: Has the meaning given to it in Clause 21.1.
Authorisation/mandate: Any User Authorisation for Business eBanking, account mandate, Business eBanking account mandate or one of our other mandate forms for Business eBanking.
Authorisation/mandate holder: One or more registered mandates or authorisations and/or physical persons who have been granted authorisations/mandates.
Business eBanking: Collective term used about our business systems, comprising:
(i) **Business PC**: a PC-based payment and information system; and

(ii) **Business eBanking**: an Internet based payment and information system.
Business Mobile Banking App means the Danske Bank Business Mobile Banking App available from the Apple or Android online stores (or such other software application distributor as may offer a Danske Bank business mobile banking application from time to time) which enables the electronic receipt and transmission of information (including information in relation to an Account).
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.
Payments managed via SWIFT are not included in this category either.
Customer support: Function at our offices offering technical support or support for Business eBanking users by telephone.
Data delivery: Transfer of data between you and us. For example, a data delivery may contain payment instructions.
Device means an electronic device (such as a smartphone, tablet or mobile phone) which is capable of accessing the Internet or downloading the App to access Business Mobile Banking.
Digital signature: An electronic signature generated by a Customer or User using his or her User ID, Personal Password and (where relevant) Security Code, to be appended to binding transactions via Business eBanking, e.g. payments, and used when linking to us.
eArchive means the electronic mailbox facility accessed via Business eBanking
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 Business eBanking or Business Mobile Banking with the eSafeID security system.
eSafeID is a web-based security system to log on to Business eBanking. eSafeID is a three-factor authentication system consisting of something the user knows (the User ID and Password) and something the user has (the eSafeID device that generates security codes).
EDISec is a security system used for integrated solutions to connect to Business eBanking.
Encryption keys are used for the 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 and eSafeID.
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 us at your premises.
Password: means, when using eSafe ID, the Password which you have created to replace the Temporary PIN, as described in these Special Terms and Conditions.
Payments between Registered Accounts: Payments between your own Registered Accounts on Business eBanking in the same country within the Danske Bank Group.
Registered Accounts: any account registered in Business eBanking in accordance with the Agreement.
Security code is used together with the user ID and the personal password for logging on to Business eBanking with the eSafeID security system.
SWIFT MT101 means request for a payment transfer sent via the SWIFT network.
SWIFT MT940 means electronic account statement received via the SWIFT network.
Temporary PIN: A code issued and sent by the Bank to your User(s). The code consists of four or eight characters and is used by your User(s) to register in the Business eBanking/Business PC security system.
Transactions: Payments, payment requests and queries in Business eBanking.
User: A user is a person (for example an employee) who has been authorised by you to act on your behalf via Business eBanking. If your and our IT systems are directly integrated, a user may also be a computer or system located within your organisation.
User Authorisation: Your authorisation of a User, specifying the services, accounts, authorisations and privileges to which the individual User has access.
User ID: A six-digit number assigned to the individual Business eBanking User. The User ID is stated in the User Authorisation.
You, you, Customer or **Account holder** means the customer or customers who has or have entered into the Agreement and shall be construed accordingly. Such terms will also be construed as referring to each and every person nominated by you on any mandate, through the Administration Module in Business eBanking or other document provided by you in connection with your Agreement. Where you/the accountholder comprises more than one person, these Terms and Conditions will apply to such persons jointly and severally so that all such persons are liable together and also individually for their obligations to us.