Danske Bank

# *Special Terms & Conditions – Online Banking*

Effective date: 14th September 2019

**These special terms and conditions have been amended to reflect the requirements of the Regulatory Technical Standards (RTS) under the Payment Services Regulations and are effective from 14 September 2019 (the "Effective Date").**

**Special Terms and Conditions**

**Corporates & Institutions (Online Banking Channel)**

**14 September 2019**

The General Terms and Conditions – Corporates & Institutions (the "General Terms and Conditions") and these Special Terms and Conditions apply to the Online Banking Channel.

Unless otherwise stated, where there is any inconsistency between these Special Terms and Conditions and the General Terms and Conditions in relation to the Online Banking Channel, these Special Terms and Conditions will prevail.

## Part 1-Online Banking Channel - general description

### Introduction

Danske Bank's Online Banking Channel provides access to account information, payments and other banking transactions requested by our business customers such as you. These Special Terms and Conditions for our Online Banking Channel include a description of how the Online Banking Channel operates.

These Special Terms and Conditions are divided into the following parts:

**Part 1:** sets out certain definitions used in, and certain rules of interpretation applicable to, these Special Terms and Conditions;

**Part 2:** describes the options available in our Online Banking Channel and how to use the system;

**Part 3:** describes the security requirements for Online Banking Channel users;

**Part 4:** sets out some contractual aspects for connecting to our Online Banking Channel.

### 1. Definitions and Interpretation

**Definitions**
Defined terms used in these Special Terms and Conditions shall have the meanings given to them in the General Terms and Conditions, unless otherwise defined herein. In these Special Terms and Conditions:

**Access Agreement:** means the agreement between you and us concerning the use of the Online Banking Channel;

**Account Information Services:** means services of the type described in clauses 7.2 and 8;

**Administrator:** means, in respect of a Customer, a User who is entitled pursuant to the Administration Module to amend access rights or other rights or authorities of Users within that Customer in respect of the Online Banking Channel;

**Administrator Privileges:** means the administrator privileges as described at clause 13.5, a full list of which is available on our Online Banking Channel;

**Administration:** means the change, amendment or alteration of a User's rights in relation to the Online Banking Channel;

**Agreement:** means an agreement in relation to the Online Banking Channel;

**Application Programme Interface:** has the meaning given to such term in the Payment Service Regulations;

**Authorisation/mandate:** means any User Authorisation for the Online Banking Channel, account mandate, the Online Banking Channel account mandate or one of our other mandate forms for the Online Banking Channel;

**Authorisation/mandate holder:** means one or more natural persons who have been granted any Authorisation/mandate;

**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);

**Card Based Payments:** mean payments out of your Account made using a card which has been

issued by a Third Party Provider. Such payments do not include payments made using a debit card issued on your Account or any credit card that we have issued to you.

**Confidential payments:** means 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 viewed and approved by Users with these privileges;

**Cross-border payment:** means a payment that crosses a national border in any currency. 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:** means the function at our offices offering technical support or support for the Online Banking Channel users by telephone or email;

**Customer or Account holder:** means the Customer or Customers who has or have entered into an Agreement and includes each and every person nominated by you on any mandate, through the Administration Module in the Online Banking Channel or other document provided by you in connection with your Agreement;

**Data delivery:** means the 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:** means an electronic signature generated by a Customer or User using his or her User ID, Personal Password and (where relevant) Security Code, appended or to be appended to binding transactions via the Online Banking Channel, e.g. payments, and used when linking to us;

**Domestic Payments:** means a payment to a beneficiary domiciled in the country within the Danske Bank Group where the sending account is registered;

**eArchive:** means the electronic mailbox facility accessed via the Online Banking Channel;

**EDISec:** means a security system used for integrated solutions to enable Data delivery between the Bank and the Customer or any User;

**Encryption Keys:** means the encryption key generated by a User for use for the EDISec security systems. and which 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 the Bank to the Customer or User;

**eSafeID** is a three-factor authentication system consisting of something the User knows (the User ID and Password) and something the User has (the Token);

**Module Agreement:** means a separate agreement pertaining to a particular module or modules within the Online Banking Channel;

**Module Description:** means the bullet-listed description of the functionality of the individual modules registered under the Agreement;

**Notification Module:** means a module in the Online Banking Channel which allows a User to request that he/she is sent an unencrypted email or text message when a specified action/event occurs;

**Online Banking Channel:** is the collective term used to describe our business systems, comprising:

(i) **Online Banking Channel:** an internet-based payment and information system;

(ii) **Business Mobile App:** an app-based version of our online Banking Channel.

**On-site support:** means training, technical assistance or other assistance provided by us at your premises;

**Payment Initiation Services:** means services of the type described in clause 7.2;

**Password:** means, when using eSafe ID, the password which you have created to replace the Temporary PIN;

**Payments between Registered Accounts:** means Payments between your own Registered Accounts on the Online Banking Channel in the same country within the Danske Bank Group;

**Payment Services Regulations** means the European Union (Payment Services) Regulations 2018 (S.I 6 of 2018) which implemented the Payment Services Directive 2 into Irish law, and any other implementing or supplementary legislation from time to time;

**Registered Accounts:** means any account registered in the Online Banking Channel in accordance with the Agreement;

**Screen-scraping:** means a computer based programme which copies data from your computer, such as the information on your Online Banking Channel, and translates it so that the information can be displayed to you in a different format;

**Security Code** means a code used together with the User ID and the Password for logging on to the Online Banking Channel with the eSafeID security system;

**Strong Customer Authentication:** means authentication based on two or more elements that are independent such as (a) something that you know (b) something that you possess and (c) something that is inherent to you. A full definition is set out in the Payment Services Regulations;

**SWIFT MT101** means a request for a payment transfer sent via the SWIFT network;

**SWIFT MT940** means an electronic account statement received via the SWIFT network;

**Temporary PIN:** means a code issued and sent by the Bank to your User(s) which consists of four or eight characters and is used by your User(s) to register in the Online Banking Channel/Business PC security system;

**Third Party Provider (TPP)** means an independent provider of services which can offer Account Information Services or Payment Initiation Services to you;

**Token:** means the eSafe ID device that generates security codes for the use of eSafe ID;

**Transactions:** Payments, payment requests and queries in the Online Banking Channel;

**User:** means a person (for example an employee) who has been authorised by you to act on your behalf via the Online Banking Channel. If your and our IT systems are directly integrated, a user may also be a computer or system located within your organisation;

**User Authorisation:** means your authorisation of a User, specifying the services, accounts, authorisations and/or privileges to which the individual User has access; and

**User ID:** means a six-digit number assigned to the individual Online Banking Channel User which is stated in the User Authorisation.

**In these Special Terms and Conditions:**

where you/the account holder comprises more than one person, these Special 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; and

**"you"** shall mean "you" the Customer and/or "you" the User as the context shall require.

## Part 2 – Modules and Services

### 2. Modules and services on the Online Banking Channel and Business Mobile Banking App

2.1 The Online Banking Channel comprises separate modules and services. The Module Descriptions comprise a description of the modules and services available via your Access Agreement.

2.2 The Notification Module is provided automatically and will be available to all Users unless the Customer has informed the Bank that it does not want any User to receive notifications. The Notification Module allows a User to request that he/she is sent an unencrypted email or text message when a specified action/event occurs.

2.3 When a Customer selects certain Modules it may be necessary for a Module Agreement to be entered into. Where this applies, the Access Agreement will refer to the Module

Agreement. By way of example a separate Module Agreement will be required where the Customer selects the SEPA Direct Debit Collection Service IRL Module.

2.4 The Access Agreement will also specify the types of Transactions which can be carried out or created on the Registered Accounts. The Customer can then authorise Users to carry out Transactions of the types specified.

## 3 Logging In to Online Banking Channel and Business Online Banking App

3.1 A User may be required to insert all 3 component parts of that User's Digital Signature when using that User's Online Banking Channel or the Business Mobile Banking App.

3.2 A User who allows the system to sit idle for a period when using the Online Banking Channel may be prompted to reinsert certain elements of that User's Digital Signature in order to continue to use the Online Banking Channel.

3.3 It is important that you, the Customer, 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).

## 4 Transactions and Transaction Data on Online Banking Channel and Business Mobile Banking App

4.1 Our Online Banking Channel allows you to make payments and queries on balances on, and movements between, accounts registered in our Online Banking Channel via the Access Agreement.

4.2 Use of your Digital Signature shall be your authorisation of and consent to payments through the Online Banking Channel 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 [to have] entered into a separate agreement with the Bank.

4.3 Our Business Mobile Banking App allows you to avail of certain services and carry out certain activities possible via our Online Banking Channel as further set out at clause 16 below. You accept that by using a Device to access the Online Banking Channel, you will only have access to a reduced range of services, full details of which can be viewed on our website.

4.4 Use of your Digital Signature shall be your authorisation of and consent to all services and activities available via the Business Mobile Banking App.

4.5 If you are making payments between your own Accounts using the Online Banking Channel you may be prompted to insert 2 of the 3 component parts of your Digital Signature before doing so.

4.6 If you are making payments between your own Accounts using the Business Mobile Banking App, you may be prompted to insert 2 out of the 3 component parts of your Digital Signature before doing so.

4.7 If when using payment services or inquiring about transaction data on the Online Banking Channel you allow the system to sit idle for more than 5 minutes, you may be prompted to reinsert 2 out of the 3 component parts of your Digital Signature to continue using the Online Banking Channel services.

4.8 If when using payment services or inquiring about transaction data on the Business Mobile Banking App, you allow the system to sit idle for more than 5 minutes, you may be prompted to reinsert 2 out of the 3 component parts of your Digital Signature to continue using Business Mobile Banking App.

## 5 Registered accounts

5.1 Accounts must be registered in the Online Banking Channel before you can make transactions via the Online Banking Channel. Accounts are registered via the Access Agreement.

5.2 The following accounts can be registered in the Online Banking Channel: (a) Accounts held by you and opened in your name with the Bank and affiliates and divisions of the Danske Bank Group, and (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.

5.3 Registered Accounts within the Danske Bank Group can also be managed via SWIFT MT101 or MT940; see clause 5.4 for further details.

5.4 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 SWIFT MT940, can also be registered in the Online Banking Channel via an 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 SWIFT MT101 or an agreement on balance reporting via MT940.

## 6 Unregistered accounts

If Accounts held by you and/or a third party are not registered in our Online Banking Channel, it is only possible to make payments into those accounts. It is not possible to enquire about or make payments from unregistered Accounts.

## 7 TPPs – general

7.1 You can use TPP services to aggregate your account information, make payments out of your Account and to make confirmation of funds requests, if you are registered for the Online Banking Channel and have a Digital Signature. All references to you in this clause include any User with a Digital Signature authorised to access your Account. You must have a Digital Signature that allows you to make payments out of your Account to use Payment Initiation Services and Card Based Payment services.

7.2 TPPs are independent providers of services. If we provide you with a TPP service then we will make that clear to you at the time. TPP services can be used to access any of your Accounts which are accessible online. Your Account will be accessible online unless the terms and conditions for your Account state otherwise. The following types of services are offered by TPPs:

(i) Account Information Services – these services allow Customers to consolidate information about different payment accounts which they have with one or more banks to review their overall aggregated financial position. Some TPPs may also offer a range of associated services such as budgeting and financial planning tools. Further information is set out below.

(ii) Payment Initiation Services – these services help Customers to make a range of Credit Transfers out of their Account.

(iii) Card Base Payment instrument issuers – some TPPs may issue instruments for making Card Based Payments out of your Account. These TPPs may ask us to confirm whether an amount needed for a payment using a card they have issued is available on your Account. Further information about how we respond to such requests is set out below.

7.3 If you use a TPP to make a payment from your Account, then you will need to confirm the details of the payment including the sort

code and account number or, where applicable, the BIC and IBAN of the Payee and also the amount of the payment. When you confirm these details, we will process the payment as set out in our Corporates & Institutions - Fees & Charges brochure. The Corporates & Institutions - Fees & Charges brochure includes information about the processing times that apply to payments initiated by a TPP. In particular, you should note that payments initiated by a TPP which require authorization by more than one user (for example, where an authorised user has a joint mandate to approve payments) will only be deemed to have been received by us when we receive the final authorization from an appropriate user and will be processed in accordance with the times set out in the Corporates & Institutions - Fees & Charges brochure thereafter. Any payment from your Account using the services of a Third Party Provider will be made from the Account as a Credit Transfer even if the Account is one on which one of our Cards has been issued. Further information on how this may impact on the protections that you have is set out below.

7.4 TPPs may provide their services in different ways. Some TPPs use the Open Banking APIs to access your Account whilst others use a technique known as Screen-scraping. The way in which a TPP accesses your Account is important because this will affect how these Special Terms and Conditions apply to you when using the TPP services.

7.5 If you consent to a TPP accessing your Account using the Open Banking APIs, we will ask you to authenticate any TPP requests that we receive by entering your Digital Signature on a secure Danske Bank page – this will not be the Online Banking Channel log on page. By entering your Digital Signature, you give us your consent to provide information to that TPP, make a payment that they have initiated or to respond to a confirmation of funds request, whichever applies. The TPP will only be able to view the information that you specifically authorise it to view or to debit the specific payment that you authorise.

7.6 If you consent to a TPP accessing your Account using Screen-scraping then you give us your consent to provide information or make payments using that TPP by providing them with your Digital Signature. A TPP accessing your account using Screen-scraping will be able to access all of your Accounts, including being able to access all the information that you can access in the Online Banking Channel and make payments from your Account in the same way that you can. The TPP may ask you for your Digital Signature on its own website or it may instead redirect you to the Online Banking Channel log on page with the Danske Bank website and ask for the information there.

7.7 Where the TPP uses Screen-scraping techniques it may not be clear to us that the services of a TPP are being used. In these circumstances, you must provide us with the details of the TPP on request.

7.8 You will be able to revoke TPP access to your Account either: (i) directly with the TPP by following its procedures, (ii) in our Online Business Channel under 'Contact and help' or (iii) by contacting the branch. You can also obtain a full list of TPPs who you have authorised to access your Account by contacting us. We can only provide this service where the TPP uses the Open Banking APIs to access your Account. You can revoke TPP access to your Account directly with the TPP using its own procedures, where the TPP is using Screen-scraping techniques to access your Account.

7.9 Where you tell us that you want to withdraw a TPP's ability to access to your Account we will comply with that request but it will not act as a revocation of consent to a payment that has already been debited from your Account or to information that has already been provided to a TPP in response to a confirmation of funds request or for Account Information Services.

7.10 We will only otherwise revoke a TPP's access to your Account if we believe its access is unauthorised or fraudulent or if

we become aware that it is no longer authorised or regulated by an appropriate authority.

## 8 TPPs – Account Information Services

8.1 A TPP will only be able to get information about your Account if it is accessible online. Your Account is accessible online unless the terms and conditions for your Account state otherwise. All references to you in this clause include any User who has a Digital Signature and is authorised to access your Account. All Users with a Digital Signature and are authorised to access your Account can use Account Information Services.

8.2 The TPP will ask you to give your explicit consent before it can access your Account. This means that the TPP should make available to you the information that you need to make an informed decision so that you understand what you are consenting to.

8.3 If the TPP accesses your Account using the Open Banking APIs the TPP will only receive the specific information that you have explicitly consented to be provided. When the TPP uses this method you will be redirected to a Danske Bank webpage where you will be asked to provide your Digital Signature. By entering the Digital Signature you are giving us your consent to provide the information to the TPP for a specified period of time. Only certain accounts are accessible in this way (for example accounts which are not payment accounts are not accessible). Information about your Accounts will be available as "data clusters" – this means that we will group certain information into a data set (a cluster). When you confirm your consent all of the information in the data cluster will be made available to the TPP.

8.4 If the TPP accesses your Account using Screen-scraping the TPP will be able to access and download all of the information that is available within our Online Business Channel and we will not be able to limit or restrict this. By giving the TPP your Digital Signature you are giving us your consent to provide the information to the TPP. Unless the TPP has taken steps to identify itself to us we may think that the request is being made directly by you. A TPP which uses Screen-scraping techniques will be able to access both payment and non-payment Accounts. A non-payment Account would include any loan accounts that you have with us.

8.5 We recommend that you check that the TPP is authorised and regulated by the Central Bank of Ireland or another European Regulator before using its services. If the TPP is authorised and regulated by the Central Bank of Ireland then it will be subject to the Payment Services Regulations. This means that it is obliged to ensure that any personalised security credentials are not available to any unauthorised person and that it uses safe and efficient channels in providing its services to you.

8.6 A TPP should not request more information than is absolutely necessary to provide the specific service it is offering to you.

8.7 A TPP which provides an Account Information Service may use the User's personalised security credentials if it is necessary to provide the Account Information Service. We will treat a request from an Account Information Service TPP in the same way as we treat a request received from you. We will release information about all parties to any joint accounts. Any information that you have recorded on your Account about any third party will not be released. We will not provide your Digital Signature to a TPP.

8.8 You will be able to revoke TPP access to your Account either directly with the TPP by following its procedures, in our Online Business Channel under 'Contact and help' or by contacting the branch. You can also obtain a full list of TPPs whom you have authorised to access your Account by contacting us. We can only provide this service where the TPP uses the Open Banking APIs to access your Account. You can revoke TPP access to your Account directly with the TPP using its own procedures, where the TPP is using Screen-

scraping techniques to access your Account.

8.9 Where you tell us that you want to withdraw access to a TPP being able to access your Account we will comply with that request but it will not act as a revocation of consent where information has already been provided to a TPP which provides Account Information Services.

8.10 We will only otherwise revoke a TPP's access to your Account if we believe its access is unauthorised or fraudulent or if we become aware that it is no longer authorised or regulated by an appropriate authority.

8.11 If you experience detriment caused by your Account Information Service provider (AISP) other than in relation to an unauthorised payment you should contact the AISP in the first instance. If you believe that we have breached any of our obligations in relation to a TPP having accessed your Account for the purposes of provision of Account Information Services then you should contact us. We will be liable for any loss that you have suffered as a result of us having breached any of our obligations. We are not responsible to you under this clause where any failure on our part was due to (i) abnormal or unforeseeable circumstances beyond our control, the consequences of which would have been unavoidable despite all of our efforts to the contrary or (ii) our obligations to comply with any other provision of applicable laws.

## 9 TPPs – Card Based Payments

9.1 All references to you in this clause include any User with a separate authorisation to make payments out of your Account.

9.2 We will confirm whether an amount needed for a Card Based Payment out of your Account is available when this information is requested by the card issuer if:

(i) your Account is accessible online at the time we receive the request; or

(ii) you have given us your consent to do so.

9.3 When we receive the first confirmation of funds request from a card issuer, we will ask you to authenticate the request. We will then show you all the information relating to the request, including who has made it, the Account it relates to and the date on which consent for us to respond to such requests from the TPP expires, if any.

9.4 We will then ask you to confirm your consent before we respond to the request. We will only respond with a "yes/no" answer about the availability of funds in a particular account to cover the amount in the request. We will not provide details of your account balance or block funds on your Account for payment. We will continue to respond to confirmation of funds requests made by that particular card issuer until either your consent expires or you revoke it, whichever is earlier.

9.5 You can view your confirmation of funds history and revoke your consent to us responding to further confirmation of funds requests in the Online Banking Channel or by otherwise contacting us to communicate this.

## 10 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 SWIFT 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.

## 11 Requests

11.1 A request by you or any of your Users for a transaction in the Online Banking Channel, for example a payment, is called an electronic request.

11.2 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 instruction passes to us.

11.3 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.

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

11.5 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 issuances, finalised in accordance with the electronic request.

11.6 We retain electronic requests for 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 such fee as may be charged by us for administrative assistance (separate rules will apply where the information is requested by a Data Subject and is Personal Data – see our Data Privacy Notice on our website Data Privacy Notice). Details of our current fees and charges can be found in our Corporates & Institutions - Fees & Charges brochure on our website www.danskebank.ie.

## 12 Receipt of documents in eArchive

12.1 eArchive is both an archive and an electronic mailbox facility provided by the Bank via our Online Banking Channel service. eArchive is used to send correspondence from us to you electronically (electronic mail) and without the need for any paper copies of that electronic mail to be sent to you. As an Online Banking Channel 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 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. Where you request a document to be sent by paper which is available electronically, a fee may apply.

12.2 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 Online Banking Channel and have an electronic mailbox if you want to receive documents from us in electronic form under the Agreement. Accounts of a third party for which you have access rights will be treated in the same manner as your own Accounts.

12.3 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 advices 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 may increase. You will receive separate notification each time a new type of

document becomes accessible in your electronic mailbox which you will no longer receive by ordinary mail.

12.4 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. If you wish to amend this service to receive your documents in electronic form once more, please get in touch with your relationship manager.

## 13 User Authorisations for the Online Banking Channel

13.1 All Users performing transactions in the Online Banking Channel 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 the Online Banking Channel.

13.2 Where the Access Agreement states that you have accepted the Administration Module, the User Authorisation will also specify whether the User has been granted Administrator Privileges. The User Authorisation will specify what those Administrator Privileges are. Clause 13.5 describes the different types of Administrator Privileges that may be specified on the User Authorisation.

13.3 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 Special Terms and Conditions. You will receive separate notification of any such changes via the Online Banking Channel or otherwise. Where a User has been granted Administration privileges 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 the Online Banking Channel.

13.4 When you provide us with Personal Data for a User, you warrant that you are entitled to disclose such Personal Data to us. In addition, you confirm you will promptly ensure that the Data Subject has been informed where to find information about our processing of Personal Data, which is set out in the Purposes. If a User needs to have manual access to Accounts, e.g. to carry out transactions at An Post branches or sign cheques, you must sign an account mandate form (which you can obtain from us) authorising the User to do so.

13.5 Administrator Privileges

Where you have access to the Administrator Module you must consider whether you will grant to a User Administrator Privileges. The following is a non-exhaustive list of Administrator Privileges which may be granted (a comprehensive list is available in our Online Banking Channel):

- 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 Adminstrator and/or User Administrator Privileges, you must also decide the level of authority that the 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 17. A User granted Agreement Adminstrator and User Administrator Privileges must have the same approval rights for both privileges.

13.6 Agreement Administrator

A User who is granted Agreement Adminstrator Privileges is authorised to perform the following on behalf of the Customer:

- 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
- create and delete Agreement Information privileges
- create and delete User privileges in relation to Log-ons and blocking
- 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.

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 person(s) 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 the Online Banking Channel 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. Agreement Administrator Privileges will not be granted until the Bank has approved the User Authorisation.

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.

13.7 User Administrator

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

- 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.

13.8Agreement 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 the Online Banking Channel.

13.9Log-on and Blocking

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

- order temporary Pins for Users
- order Tokens
- block and unblock User access.

This privilege can only be granted as a separate authorisation.

13.10 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].

13.11 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 this 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 that Customer 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.

13.12 Collection Service SEPA Direct Debit authorisation in the Online Banking Channel

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

13.13 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

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 documentation 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 he or she 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 its demand.

13.14 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 authorisations relating to the trading in securities or foreign exchange via the Online Banking Channel or viewing trades via the Online Banking Channel.

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

13.15 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 the Online Banking Channel. 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.

13.16 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 16.3 below. The various types of authorisations are described in clause 17 below.

## 14 Viewing documents

A User may view a number of documents in eArchive in the Online Banking Channel. The rights and authorisations granted to the individual User determine which documents the User can view in our Online Banking Channel. A User will, for instance, be able to view his or her individual User Authorisation in the Online Banking Channel.

## 15 Access to Accounts

15.1 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 below. Note that the authorisation granted at account level is reflected in all Online Banking Channel agreements under which the Account is registered.

15.2 Payment Limits

Where you have included the Administration module in your Online Banking Channel Agreement, you may control the value of requests created and/or approved through the Online Banking Channel either at an Account level which applies to all Users [known as Payment Limit - account] or on individual Users [known as Payment Limit - user]. It is your responsibility to create Payment Limits suitable for your requirements. If a Payment Limit – account or Payment Limit - user 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.

15.3 Transaction types

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

- Payments between accounts registered under this Agreement in the same country within the Danske Bank Group
- Payment requests via SWIFT MT101
- Euro payments to accounts in Ireland or within the Single Euro Payments Area (SEPA)
- 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 both to 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

The various authorisations granted by us are described in clause 17.1. 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.

15.4 Exchange Rates

(i) Cross-border payments to registered and unregistered Accounts within or outside the Danske Bank Group may be processed:

- Without exchange - where no exchange is required. For example, the payment is being made in the same currency as the beneficiary account;
- at the relevant Fixing Rate;
- Bank's Spot Rate - a currency exchange rate based off the prevailing market rate at that time and at or within the spreads on our rates displayed on our Website;
- 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.

(ii) Domestic Payments from one currency and another to registered and unregistered Accounts within or outside the Danske Bank Group will be processed at the relevant Fixing Rate.

(iii) The relevant Fixing Rate may be subject to change in respect of Foreign Payments for an amount in excess of €50,000 (or its equivalent in euro).

15.5 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.

15.6 Corporate Notifications

A User may subscribe for different [Corporate Notifications] in the [Notification Centre] in our Online Banking Channel.

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 the Online Banking Channel or on our website. Where a User has access to[ Corporate Notifications] you acknowledge and agree to pay to the Bank any fees associated with notifications created by those Users.

15.7 Changing your Online Banking Channel User Authorisations

If you wish to extend or limit a User's access to the Online Banking Channel, a new User Authorisation for the Online Banking Channel must be signed physically or using your Digital Signature on your Online Banking Channel 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 the Online Banking Channel may be affected if you issue an account mandate form.

Revoking the Online Banking Channel User Authorisations

User Authorisations for the Online Banking Channel remain in force until revoked by you in writing - physically or using your Digital Signature in the Online Banking Channel where applicable. When we have received notice of revocation, we will send written confirmation that the User number and Encryption Key(s) have been deleted in our systems. If you terminate this Agreement, we will construe this as revocation of all User Authorisations granted under this 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.

## 16 Other mandates in the Online Banking Channel

16.1 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 the Online Banking Channel via your Access Agreement.

16.2 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.

16.3 Trade Finance Authorisation in the Online Banking Channel

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 the Online Banking Channel. 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).

## 17 Authorisation types

17.1 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.

17.2 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.

17.3 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.

17.4 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.

17.5 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.

## 18 Business Mobile Banking App

18.1 To be eligible to access the Online Banking Channel 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 Online Banking Channel service, have a Device and otherwise comply with any requirements set down by the relevant software application distributor.

18.2 When a User downloads the Business Mobile Banking App to a Device you accept that these conditions apply in relation to the use of the Online Banking Channel 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.

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

- View Balances;
- View Transactions;
- View history of transactions
- Create Domestic Payments and approve payments
- Administration

The Bank may from time to time update, extend or reduce the Online Banking Channel services offered via the Business Mobile Banking App from time to time. The Bank may extend the scope of the Online Banking Channel 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 not less than one month's notice is required prior to any reduction in its 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).

## 19 Security

In addition to any other obligations or responsibilities which you may have under these Special 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.

The Business Mobile Banking App is currently free of charge 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.

## 20 Cookies

By using our Online Banking Channel you consent to the use of cookies which are required

to enable the Online Banking Channel to operate effectively. Full details of our policy in relation to cookies can be found on our website.

## 21 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 you 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. We reserve the right to charge a fee for the provision of the training referred to above.

Troubleshooting may result in adaptation and/or modification of the computer setup. Installation and troubleshooting takes 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 the Online Banking Channel 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 3 - Online Banking Channel - security system

## 22 Technical issues

22.1 Transmission and access

In order to use our Online Banking Channel, 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 not less than one month's written notice via the Online Banking Channel or in such other manner as we shall determine.

22.2 Distribution, control and storage of software

We may distribute programs required to operate the Online Banking Channel. You must download the programs from the internet.

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.

22.3 Data security

eSafeID and EDISec are the general security systems used in our Online Banking Channel. Using these 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.

22.4 eSafeID security system

eSafeID is the Bank's web based security system to log-on to our Online Banking Channel. It is a two factor authentication system, which means that it is based on something you know (a User's Password) and something you have in your possession (the security code generated by your Token). The security code generated by the Token is saved temporarily in the browser session while the User is logged on to the Online Banking Channel.

22.5 Other security systems

e-Safekey, EDISec and OpenPGP Security are security systems supported by the Bank which allow Customers to exchange information electronically with the Bank directly using their own system. E-Safekey, EDISec and OpenPGP Security use permanent Encryption Keys stored in the Customer's IT environment.

22.6 E-Safekey

eSafekey is the security component in the Bank's Application Programme Interface solution. The Customer may download the e-Safekey security system software via the internet. When downloading via the internet, it is the duty of the Customer to ensure that the software has been supplied by the Bank. Guidance for this procedure is available on request. If the software has not been supplied by the Bank it must not be installed. The Customer agrees to follow the guidance provided regarding the installation of the e-Safekey security system. Registration in the e-Safekey security system takes place before the User starts using the Service. In this connection, a private [Encryption] Key is generated. A User's Digital Signature is created using a private [Encryption] Key stored in the Customer's IT environment. Access to the [Encryption] Key is protected by the User's Password.

22.7 EDISec

EDISec is a security system used for integrated solutions to connect to our Online Banking Channel via data communication channels.

22.8 OpenPGP Security

22.8.1 OpenPGP Security is a security system used for integrated solutions to connect to our Online Banking Channel via data communication channels. If an OpenPGP Security public certificate is issued by a third party issuer on behalf of a Customer, the Bank will recognise the Customer as owner of the key and thus the Customer will be 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.

22.8.2 EDISec Encryption Keys and OpenPGP Security Certificates. For EDISec and OpenPGP Security, it is the responsibility of the Customer to ensure usage of valid Encryption Keys at any time for securing data communication. To be more specific, the Customer must make sure that:

- The Bank has got a valid set of the Customer's Encryption Keys. When the Encryption Keys are about to expire then the Customer must update the customer system with new Encryption Keys (which will be provided by the Bank)
- The Customer is using a valid set of the Bank's Encryption Keys for securing the data communications. When these Encryption Keys are about to expire then the Customer must

renew the Encryption Key's and exchange them with the Bank.

- If Customer Encryption Keys are compromised or damaged, then they should be revoked by contacting the Bank.

When the Bank receives the Customer's EDISec Encryption Key or public OpenPGP Security certificates the Encryption Keys/ certificates will be stored in the Bank's systems in a secure way and will not be shared with anyone outside the Bank. It is the responsibility of the Bank to make sure that a valid set of the Bank's public EDISec Encryption Keys or OpenPGP Security certificates are always available to the Customer.

The Bank accepts no liability for any ommissions or delays when Encryption Keys have not been renewed.

22.9 Creation of Digital Signature

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 Token.

22.10 Blocking User Access

22.10.1 We reserve the right to block your or a User's access to the Online Banking Channel for objectively justified reasons relating to the security of the Online Banking Channel 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 the Online Banking Channel if the reasons for blocking cease to exist.

22.10.2 If you wish to apply for unblocking of your access to Online Banking Channel please contact the Online Banking Channel helpdesk, your Relationship Manager or by phoning 1850 812 040. After unblocking a temporary PIN may be issued by [SMS] to a User where the User has registered a mobile telephone number with the Bank in accordance with the process prescribed by us at the time.

22.11 You must take all reasonable steps to prevent unauthorised use of the Service and unauthorised access to User Encryption Keys, Passwords or Tokens.

**23 Acquiring a User ID, temporary password and Token**

23.1 When a User is to be created in your Online Banking Channel with the eSafeID security system, we give the User an individual user ID, a temporary PIN and a Token. The Token must be activated upon receipt of it in order to make use of it, activation to be effected in accordance with our instructions in the letter sending you the Token. Together with the Token, the temporary PIN is used for first-time identification when the user is registered in the security system.

23.2 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 Token has been opened or is not intact, the user must contact us to order a new temporary PIN and/or a new Token. For security reasons, the letters containing the temporary PIN and the Token are not sent at the same time.

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

23.4 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 Token.

23.5 Storing the User ID, Password and Token.

The following rules apply to the use of eSafeID

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

23.6 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.

23.7 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.

23.8 Deregistering Users

Users can be deleted via the administration module of the Online Banking Channel. Users can also be deleted by the Bank and 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.

23.9 Misuse or risk of misuse

You or the User must immediately contact the Bank in order to block user access if you suspect or the User suspects that the Password, or the Token has been misused or that others have had access to the Password, or have gained possession of the Token.

Part 4 - Contractual aspects

24 For business purposes only

The Online Banking Channel 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 with written permission from us.

**25 Changing the Online Banking Channel**

Our Online Banking Channel gives access to the services offered by us at any time. We may at any time extend the scope of our Online Banking Channel without advance notice, whereas not less than one month's notice is required prior to any reduction in its 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 not less than such longer notice period). We shall provide written information of any changes via the Online Banking Channel or otherwise.

**26 Changes to service and support**

We may change the scope and content of our service and support at any time by giving not less than one month's written notice via our Online Banking Channel or otherwise.

**27 Responsibilities and liability**

27.1 Your responsibilities

You use our Online Banking Channel 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 the Online Banking Channel. 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 the Online Banking Channel which seems to be incorrect. On becoming aware of an unauthorised amount having been debited to such an account, you should telephone the Bank 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 the 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 Online Banking Channel 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 [Encryption] 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' [Encryption] Keys in your IT environment to prevent unauthorised access to the [Encryption] Keys
- any incorrect use or misuse of the Online Banking Channel by registered Users.

In the event that any Password or Digital Signature or Key relating to your access to our Online Banking Channel Service has been misappropriated or used in an unauthorised manner, you must notify us by telephoning the Bank or your Relationship Manager. You should confirm your notice by writing within seven days to the 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 your circumstances, including non-observance of your safety and control procedures.

27.2 Our responsibilities

We will be liable for damages if, through errors or neglect, we fail to perform our obligations or in any other circumstance where liability will attach as set out in the General Terms and Conditions. However, we are not liable for errors and omissions resulting from:

- errors and omissions in third-party software which is part of the Online Banking Channel security system
- a User's disclosure of that User's 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 system itself or have 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.

**28 Other terms and conditions**

28.1 Structure of the Online Banking Channel Agreement

The Agreement is comprised of the following:

- the Access Agreement
- all User Authorisation(s)
- all Module Descriptions
- these Special Terms and Conditions
- General Terms and Conditions
- Corporates & Institutions - Fees & Charges brochure

By signing the Access Agreement for our Online Banking Channel you also acknowledge having read and accepted all parts of the Agreement.

28.2 Prices

- We may at any time change our prices by giving not less than one month's written notice via the Online Banking Channel 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 the fee account(s). Details of our current fees and charges can be found in our Corporates & Institutions - Fees & Charges brochure.

**29 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 not less than one month's notice (or not less than such longer notice period as we may be required by law or regulatory requirement to give you).