Danske Bank

Regulamin użytkowania systemu Business Online
Terms and Conditions for Business Online

Spis treści:

List of contents:

I. Postanowienia ogólne

§ 1. Zakres

1. Niniejszy Regulamin użytkowania systemu Business Online („Regulamin") wydany przez Danske Bank A/S, spółkę z kapitałem akcyjnym w wysokości 10.086.200.000,00 DKK, w pełni opłaconym, działającą poprzez centralę przy Holmens Kanal 2, DK-1092 Kopenhaga K, Dania i/lub, odpowiednio, Danske Bank A/S S.A. Oddział w Polsce, ul. Emilii Plater 28, 00-688 Warszawa, zarejestrowaną przez Sąd Rejonowy dla miasta Warszawy, XII Wydział Gospodarczy, pod numerem KRS 0000250684, NIP: 107-000-49-37 („Bank") reguluje zakres współpracy, jak również prawa i obowiązki stron w odniesieniu do systemu bankowości elektronicznej Banku, dostępnego za pośrednictwem sieci internetowej, który zapewnia dostęp do informacji o rachunku, umożliwia wykonywanie płatności i pozostałych transakcji bankowych przez klientów Banku.

2. Treść niniejszego Regulaminu została podzielona na następujące części:
Business Online – Opis ogólny – omówienie dostępnych opcji w systemie Business Online i wskazówki w zakresie korzystania z systemu;
Business Online – Systemy zabezpieczeń – opis wymogów bezpieczeństwa dotyczących systemu Business Online i jego Użytkowników;
Business Online – Aspekty dotyczące postanowień umownych - opis praw i obowiązków stron w zakresie łączenia się z systemem Business Online.

3. Niniejszy Regulamin wchodzi w życie z dniem 1 listopada 2013 roku.

§ 2. Definicje

„Umowa Dostępu" oznacza umowę pomiędzy Bankiem a jego klientem („Spółka") w zakresie użytkowania systemu Business Online;

„Autoryzacja/Upoważnienie/Pełnomocnictwo" oznacza Upoważnienie Użytkownika w systemie Business Online, Pełnomocnictwo do dysponowania rachunkami dla przedsiebiorców, Pełnomocnictwo do rachunku w systemie Business Online lub jakiekolwiek inne pełnomocnictwo obowiązujące w Banku upoważniające do korzystania z systemu Business Online;

„Osoba autoryzowana/Pełnomocnik" oznacza jednego lub więcej zarejestrowanych pełnomocników lub jedną lub więcej osób autoryzowanych i/lub osób fizycznych, którym udzielono autoryzacji/pełnomocnictwa;

„Dni Robocze" oznaczają wszystkie dni poza sobotami i niedzielami, jak również wszystkimi polskimi świętami państwowymi określonymi w przepisach szczególnych;

„Business Online" to termin zbiorczy określający internetowy system transakcyjny i informacyjny Banku dla klientów korporacyjnych;

„Płatności poufne" oznaczają płatności (takie jak wynagrodzenia), które mogą zostać wyświetlone lub zrealizowane jedynie przez Użytkowników posiadających szczególne

I. General Provisions

§ 1. Scope

1. These Terms and Conditions for Business Online (the "**Terms and Conditions**") issued by Danske Bank A/S, registered and paid in share capital DKK 10,086,200,000, acting through its principal office at Holmens Kanal 2, DK-1092 Copenhagen K, Denmark and/or, respectively, Danske Bank A/S S.A. Branch in Poland, ul. Emilii Plater 28, 00-688 Warsaw, registered by the District Court for the City of Warsaw, XII Commercial Division KRS 0000250684, tax identification number (NIP): 107-000-49-37 (the "**Bank**") shall govern the scope of co-operation as well as the rights and the obligations of the parties with respect to the Bank's internet-based office-banking system, which provides access to account information, payments and other banking transactions as requested by its customers.

2. These Terms and Conditions are divided into:
Business Online - general description - defining the options available in Business Online sytem and directions how to use it;
Business Online – Security systems - describing the security requirements for Business Online system and its Users;
Business Online – contractual aspects - describing rights and obligations of the parties with regard to connecting to Business Online system.

3. These Terms and Conditions shall come into effect on 1st November 2013.

§ 2. Definitions

"Access Agreement" is an agreement between the Bank and the customer (the "Company") concerning the use of Business Online;

"Authorisation/mandate" is either User Authorisation for Business Online, Mandate to operate accounts for entrepreneurs, or one of the Bank's other mandate forms for Business Online;

"Authorisation/mandate holder" is one or more registered mandates or authorisations and/or physical persons who have been granted authorisations/mandates;

"Banking days" are all days except Saturdays and Sundays as well as all Polish public holidays as defined in specific regulations;

"Business Online" is the collective term for the Bank's internet-based payment and information system for corporate customers;

"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

uprawnienia. Płatności zaliczone do Płatności Poufnych mogą być realizowane jedynie przez Użytkowników posiadających takie uprawnienia;	can only be processed by Users with these privileges;
„Płatności transgraniczne" lub odpowiednio „Płatności zagraniczne" oznaczają płatności przekraczające granicę państwową lub płatności wyrażone w walucie zagranicznej (innej niż PLN). Dotyczy to płatności pomiędzy zarejestrowanymi rachunkami, jak również płatności na rachunki niezarejestrowane. W krajach, gdzie obecna jest grupa finansowa Banku, płatności pomiędzy rachunkami w granicach tego samego kraju nie są traktowane jako płatności transgraniczne. Płatności wykonywane za pośrednictwem systemu SWIFT także nie należą do tej kategorii;	**"Cross-border payments"** or respectively **"Foreign payments"** are payments crossing a national border or expressed in foreign currency (i.e. other then PLN). This applies to payments between registered accounts as well as payments to unregistered accounts. In the countries where the Bank's financial group is represented, payments between accounts in the same country are not considered as cross-border payments. Payments managed via SWIFT are not included in this category either;
„Wsparcie Spółki" oznacza jednostkę organizacyjną w Banku świadczącą usługi wsparcia technicznego przez telefon dla Użytkowników Business Online;	**"Company support"** is a function at the Bank offering technical support or support for Business Online Users by telephone;
„Pakiet danych" oznacza transfer danych pomiędzy Spółką a Bankiem. Przykładowo pakiet danych może zawierać dyspozycje płatnicze;	**"Data delivery"** is transfer of data between Company and the Bank. For example, a data delivery may contain payment instructions;
„Podpis cyfrowy" oznacza podpis elektroniczny za pomocą którego autoryzuje się wiążące transakcje, np. płatności, i który wykorzystywany jest w chwili uzyskiwania połączenia z Bankiem;	**"Digital signature"** is an electronic signature appended to binding transactions, e.g. payments, and used when linking to the Bank;
„Urządzenie eSafeID" oznacza urządzenie osobiste, które występuje w rozmaitych postaciach. Wspólną ich cechą jest to, że urządzenia te wyświetlają kod bezpieczeństwa, który jest wykorzystywany przy logowaniu się do systemu Business Online za pośrednictwem systemu zabezpieczeń eSafeID;	**"eSafeID device"** is a personal device, which can come in various formats. A common feature is that it shows a security code to be used when logging on to Business Online with the eSafeID security system;
„eSafeID" oznacza system zabezpieczeń sieciowych służący do logowania się do systemu Business Online. eSafeID to dwuczynnikowy system uwierzytelniania składający się z informacji znanej Użytkownikowi („Hasło", zgodnie z podaną niżej definicją) i urządzenia eSafeID generującego kody bezpieczeństwa;	"**eSafeID**" is a web-based security system to log on to Business Online. eSafeID is a two-factor authentication system consisting of a piece of information the User knows (the "Password", as defiend below) and the eSafeID device that generates security codes;
„EDISec" oznacza system zabezpieczeń wykorzystywany przez rozwiązania zintegrowane do łączenia z systemem Business Online;	**"EDISec"** is a security system used for integrated solutions to connect to Business Online;
„Klucze szyfrujące" to klucze wykorzystywane na potrzeby systemów zabezpieczeń e-Safekey i EDISec. Każdy Użytkownik generuje klucz szyfrujący, który składa się z pary kluczy, tj. klucza prywatnego do tworzenia podpisów cyfrowych i klucza publicznego do potwierdzania podpisu cyfrowego i szyfrowania danych przesyłanych z Banku do Spółki. Każdy Użytkownik posiada tajny klucz szyfrujący w celu generowania unikalnych osobistych podpisów cyfrowych. Dostęp do klucza szyfrującego jest chroniony hasłem osobistym Użytkownika. Klucz szyfrujący jest przechowywany w środowisku informatycznym Spółki;	**"Encryption keys"** are used for the e-Safekey and EDISec security systems. Each User generates an encryption key that comprises a pair of keys: a private key to create digital signatures and a public key to confirm the digital signature and encrypt data from the Bank to the Company. Each User has a secret encryption key in order to create unique, personal digital signatures. Access to the encryption key is protected by the User's personal password. The encryption key is stored in the Company's IT environment;
„e-Safekey" oznacza system zabezpieczeń wykorzystywany przez rozwiązania zintegrowane do łączenia się z systemem Business Online;	"**e-Safekey**" is a security system used for integrated solutions to connect to Business Online;
„Dyspozycja" oznacza złożony w Banku wniosek elektroniczny, pisemny lub ustny o wprowadzenie zmian do Umowy, realizację transakcji itp.;	**"Instruction"** is an electronic, written or oral request to the Bank to carry out changes to the Agreement, transactions, etc.;
„Dane podstawowe" oznaczają: imię, drugie imię (jeśli dotyczy), nazwisko, nazwę Użytkownika, numer klienta, numer/przypisany numer klienta i właściwy adres	**"Master Data"** is the first name, middle name (if any), surname, User's name, customer number, number/assigned customer number and related Company's

siedziby Spółki;

„Umowa modułowa" oznacza umowę zawierającą postanowienia dotyczące poszczególnych modułów, np. usługi Trade Finance czy Windykacji;

„Opis modułu" oznacza opis w punktach funkcjonalności poszczególnych modułów zarejestrowanych w ramach danej Umowy;

„Wsparcie na miejscu" oznacza szkolenie, pomoc techniczną lub inną pomoc zapewniane przez Bank w siedzibie Spółki;

„Hasło" oznacza kod chroniący klucz prywatny Użytkownika, który służy do tworzenia (elektronicznych) podpisów cyfrowych;

„Rachunki płatnicze" oznaczają rachunki otwarte w celu realizacji transakcji płatniczych;

„Płatności pomiędzy zarejestrowanymi rachunkami" oznaczają płatności pomiędzy zarejestrowanymi rachunkami w tym samym kraju w ramach Grupy Danske Bank;

„Kod bezpieczeństwa" oznacza kod wykorzystywany łącznie z ID Użytkownika i hasłem osobistym do logowania do Business Online za pośrednictwem systemu zabezpieczeń eSafeID;

„Rejestracja bezpieczeństwa" oznacza proces rejestracji, który każdy Użytkownik musi pomyślnie przejść przed zalogowaniem się po raz pierwszy do systemu Business Online;

„Hasło tymczasowe" oznacza hasło wygenerowane przez Bank i przesłane do indywidualnego(-ych) Użytkownika(-ów) wskazanych przez Spółkę. Hasło składa się z czterech bądź ośmiu znaków i jest wykorzystywane przez Użytkownika(-ów) Spółki do rejestrowania się w systemie Business Online;

„Transakcje" oznaczają płatności, uznania oraz pozostałe operacje i zapytania w systemie Business Online, zgodnie z podaną niżej definicją;

„Użytkownik" oznacza osobę (na przykład pracownika), która została upoważniona przez Spółkę do działania w jej imieniu za pośrednictwem systemu Business Online. Jeżeli systemy informatyczne Spółki i Banku są bezpośrednio zintegrowane, Użytkownikiem może być również komputer bądź system informatyczny Spółki;

„Upoważnienie Użytkownika" oznacza autoryzację przez Spółkę konkretnego Użytkownika z wyszczególnieniem zakresu usług, rachunków, upoważnień i uprawnień, do których dany Użytkownik ma dostęp; oraz

„ID Użytkownika" oznacza sześciocyfrowy numer przydzielony konkretnemu Użytkownikowi systemu Business Online. ID Użytkownika jest podane w Upoważnieniu Użytkownika.

address;

"Module Agreement" is an agreement containing provisions about the individual module, e.g. Trade Finance or Collection Service;

"Module Description" is a bulleted description of the functionality of the individual modules registered under the particular Agreement;

"On-site Support" is training, technical assistance or other assistance provided by the Bank at the cCmpany's premises;

"Password" is a code to protect a User's private key that is used to create digital (electronic) signatures;

"Payment Accounts" are accounts opened with a view to completing payment transactions;

"Payments Between Registered Accounts" are payments between registered accounts in the same country within the Danske Bank Group;

"Security Code" is used together with the User ID and the personal password for logging on to Business Online with the eSafeID security system;

"Security Registration" is the registration process that a User must go through before using Business Online for the first time;

"Temporary Password" is generated by the Bank and sent to the individual User(s) indicated by the Company. The password consists of four or eight characters and is used by the Company's User(s) for registering in Business Online;

"Transactions" are payments, collections, other operations and other queries in Business Online, as defined herebelow;

"User" is a person (for example an employee) who has been authorised by the Company to act on its behalf via Business Online. If Company's and the Bank's IT systems are directly integrated, a User may also be a computer or system located within the Company;

"User Authorisation" is the Company's authorisation of a particular User, specifying the scope of services, accounts, authorisations and privileges to which the individual User has access;

"User ID" is a six-digit number assigned to the individual Business Online User. The User ID is stated in the User Authorisation.

II. Business Online – Opis ogólny

§ 3. Moduły i usługi

System Business Online składa się z niezależnych modułów i usług. Opis systemu obejmuje moduły i usługi zawarte w wybranej wersji Business Online i/lub odrębne moduły i usługi.

§ 4. Transakcje

Business Online umożliwia Spółce między innymi tworzenie zleceń pobrania, dokonywanie płatności oraz śledzenie sald i operacji na rachunkach zarejestrowanych w systemie Business Online zgodnie z Umową Dostępu, otwieranie lokat terminowych, zarządzanie środkami pieniężnymi i płynnością czy składanie wniosków o produkty Trade Finance i zarządzanie takimi produktami. Płatności, pobrania oraz sprawdzanie sald i operacji na rachunkach będą dalej zbiorczo zwane Transakcjami.

§ 5. Rachunki zarejestrowane

Rachunki muszą zostać zarejestrowane w systemie Business Online, zanim Spółka będzie mogła realizować Transakcje za pośrednictwem Business Online, w szczególności zaś:

1. **Rachunki zarejestrowane w ramach Grupy Danske Bank**

   Na mocy Umowy Dostępu rachunki mogą być otwierane w dowolnej jednostce Banku bądź jego podmiotach powiązanych i innych jednostkach organizacyjnych (zwanych dalej „Podmiotami z Danske Bank").

   Następujące rodzaje rachunków mogą zostać zarejestrowane w systemie Business Online:

   - rachunki otwarte w imieniu Spółki i utrzymywane przez Spółkę;
   - rachunki, których posiadaczami są osoby trzecie, w tym spółki zależne pod warunkiem, że dana osoba trzecia lub spółka zależna udzieliła Spółce niezależnego pełnomocnictwa do działania w imieniu takiej osoby trzeciej czy spółki zależnej;

   Rachunki zarejestrowane w dowolnym Podmiocie Danske Bank mogą być również zarządzane za pośrednictwem SWIFT MT101 lub MT940/942; w celu uzyskania bardziej szczegółowych informacji zob. ust. 3.2.

2. **Rachunki zarejestrowane zarządzane za pośrednictwem SWIFT**

   Rachunki otwarte w innych bankach i rachunki prowadzone w dowolnym Podmiocie Danske Bank, co do których Spółka postanowi, że będzie je wykorzystywać do realizacji transakcji za pośrednictwem SWIFT MT101 lub MT940/942, mogą również zostać zarejestrowane w Business Online na mocy Umowy Dostępu. Spółka może zarejestrować zarówno własne Rachunki, jak i rachunki osób trzecich. W tym celu Spółka bądź osoba trzecia musi zawrzeć umowę z bankiem prowadzącym rachunek w sprawie zleceń płatniczych za pośrednictwem MT101 bądź umowę o zgłaszanie sald za pośrednictwem MT940; w celu uzyskania bardziej szczegółowych informacji zob. ust. 8.9

II. Business Online - general description

§ 3. Modules and services

Business Online comprises separate modules and services. The module description outlines the modules and services contained in the chosen version of Business Online and/or the separate modules and services.

§ 4. Transactions

Business Online allows the Company to, for example, create collections, make payments and view balances and movements in accounts registered in Business Online via the Access Agreement, to open term deposits, to do cash and liquidity management or apply for and manage Trade Finance instruments. Payments, collections and the checking of account balances and movements are jointly referred to as Transactions.

§ 5. Registered accounts

Accounts must be registered in Business Online before the Company can make Transactions via Business Online, and in particular:

1. **Registered accounts within the Danske Bank Group**

   Under this Agreement, accounts may be opened with any unit of the Bank or its affiliates and divisions (hereinafter referred to as "**Danske Bank Entity**").

   The following types of accounts can be registered in Business Online:

   - accounts opened in the name of and held by the Company;
   - accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate authorizing the Company to act on behalf of such third party or subsidiary;

   Registered accounts within any Danske Bank Entity can also be managed via SWIFT MT101 or MT940/942; for further details see Section 3.2.

2. **Registered accounts managed via SWIFT**

   Accounts opened with other banks, and accounts within any Danske Bank Entity which the Company decides to use for transactions via SWIFT MT101 or MT940/942, can also be registered in Business Online via the Access Agreement. The Company may register both its own accounts and third-party accounts. To this effect the Company 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; for further details see Section 8.9.

§ 6. Rachunki niezarejestrowane

Jeżeli rachunek posiadany przez Spółkę i/lub osobę trzecią nie został zarejestrowany w systemie Business Online, możliwe jest dokonywanie wpłat jedynie na te rachunki (przy czym nie jest możliwe dokonywanie płatności z tych rachunków bądź kierowanie zapytań dotyczących tego rachunku).

§ 7. Zlecenia elektroniczne

Zlecenie realizacji Transakcji, składane przez Spółkę lub jej Użytkowników w systemie Business Online, np. płatność, zwane jest zleceniem elektronicznym.

1. **Składanie i odwoływanie zleceń**

   Gdy Użytkownik składa zlecenie elektroniczne w imieniu i/lub osoby trzeciej, Bank potwierdza przyjęcie zlecenia w systemie Business Online.

   Zlecenia płatnicze mogą zostać odwołane do dnia poprzedzającego Dzień Roboczy, w którym zlecenie ma zostać zrealizowane włącznie.

   W celu uzyskania informacji na temat terminów dokonywania zmian w zleceniach płatniczych bądź odwoływania zleceń należy zapoznać się z następującymi dokumentami:

   - Regulamin Otwierania i Prowadzenia Rachunków Bankowych dla Przedsiębiorców;
   - Godziny graniczne przyjmowania zleceń i stosowane daty waluty.

2. **Wiążące zlecenia**

   Zlecenia realizowane zgodnie z dyspozycjami zawartymi w formularzu zlecenia elektronicznego są wiążące dla Spółki. Stąd Bank nie ma możliwości anulowania płatności, transakcji handlowych na rynku walutowym ani innych transakcji zrealizowanych zgodnie z treścią zlecenia.

§ 8. Automatyczna rejestracja na potrzeby otrzymywania dokumentów z Banku za pośrednictwem funkcjonalności eArchive

Z chwilą zawarcia Umowy o korzystanie z systemu Business Online Spółka zostaje automatycznie zarejestrowana do otrzymywania dokumentów elektronicznych z Banku. Dokumenty te są przechowywane w eArchive systemu Business Online.

Spółka otrzymuje dokumenty z Banku w postaci elektronicznej. Dokumenty te mają taką samą moc prawną jak oryginalne dokumenty przesłane pocztą.

Wszelkie takie dokumenty (w szczególności potwierdzenia wykonania przelewów i wyciągi z rachunków) uznaje się za sporządzone w oparciu o zapisy art. 7 ustawy z dnia 29 sierpnia 1997 r. Prawo Bankowe (Dz. U. 2002 nr 72 poz. 665, z późn. zm.) i nie wymagające podpisów ani pieczęci ze strony Banku.

W tym względzie rachunki osób trzecich objęte Umową użytkowania systemu Business Online są traktowane jako rachunki własne.

1. **Dokumenty otrzymywane w postaci elektronicznej**

   Spółka niniejszym potwierdza otrzymanie wszystkich dokumentów, w szczególności zaś: wyciągów z rachunków bankowych, zestawień depozytów, wypłat itp. umieszczanych drogą elektroniczną przez Bank w eArchive. W wyjątkowych okolicznościach Bank może,

§ 6. Unregistered accounts

If an account held by the Company and/or a third party is not registered in Business Online, it is only possible to make payments into these accounts (and not to make payments from or inquire about the said account).

§ 7. Electronic requests

A request by the Company or its Users for a Transaction in Business Online, for example a payment, is called an electronic request.

1. **Submitting and revoking requests**

   When a User submits an electronic request on behalf of the Company and/or a third party, the Bank confirms the receipt of the request in the Business Online system.

   The payment requests may be revoked up until and including the day before the Business Day on which the request is to be executed.

   With regard to deadlines for change or revocation of payment requests, please see:

   - Terms and Conditions for Opening and Maintaining Bank Accounts for Entrepreneurs;
   - Cut-off Times and Value Dates.

2. **Binding requests**

   Requests carried out in accordance with the instructions in the electronic request format are binding on the Company. Consequently, the Bank cannot reverse payments, trades in foreign exchange or other transactions finalised in accordance with the request.

§ 8. Automatic registration for receipt of documents from the Bank in eArchive

Upon entering into a Business Online agreement, the Company is automatically registered for receipt of electronic documents from the Bank. The documents are filed in the eArchive folder in Business Online.

The Company receives the documents from the Bank in electronic form with the same legal effect as ordinary mail in hardcopy.

All such documents (in particular confirmation of executed transfers and account statements) shall be considered to be prepared based on art 7 of the Banking Law dated 29 of August 1997 (Journal of Laws from 2002 No. 72, item 665, as amended) and do neither require Bank's signatures nor a stamp.

Third-party accounts comprised by the Business Online agreement are treated as own accounts with this respect.

1. **Documents received in electronic form**

   The Company hereby accepts receipt of all documents, in particular: account statements, lists of deposits, withdrawals etc. placed electronically by the Bank in eArchive. In special circumstances the Bank may, at a separate, justified request send

na indywidualny i uzasadniony wniosek, przesłać takie dokumenty w wersji papierowej, za pośrednictwem zwykłej poczty.

Jeżeli Spółka jest klientem jednego bądź więcej Podmiotów Danske Bank i otrzymuje dokumenty drogą elektroniczną od tych podmiotów, Spółka może również otrzymywać takie dokumenty za pośrednictwem systemu Business Online.

Bank może w dowolnej chwili rozszerzyć wybór i zwiększyć liczbę dokumentów elektronicznych dostępnych w eArchive, o czym Spółka zostanie osobno powiadomiona w systemie Business Online.

2. Dostęp do dokumentów w eArchive

Prawa i upoważnienia udzielone poszczególnym Użytkownikom określają zakres dokumentów, w które Użytkownik może mieć wgląd. Przykładowo Użytkownik będzie zawsze miał możliwość wglądu do własnego indywidualnego Upoważnienia Użytkownika w systemie Business Online. Użytkownikom z dostępem do danych/dostępem do obsługi rachunku zapewniany jest wgląd do dokumentów dotyczących danego rachunku w eArchive.

3. Archiwizacja

Bank przechowuje zlecenia elektroniczne i wszelkie dokumenty w eArchive za bieżący rok oraz przynajmniej za pięć lat wstecz. W przypadku wygaśnięcia Umowy użytkowania systemu Business Online lub zmiany numeru klienta lub wyrejestrowania dowolnego rachunku bądź też utraty przez Spółkę dostępu do systemu Business Online z dowolnej przyczyny, Spółka nie będzie mogła otrzymywać dokumentów w postaci elektronicznej w eArchive, a dokumenty te zostaną usunięte. W takich przypadkach zaleca się uprzednie sporządzenie przez Spółkę kopii wszystkich dokumentów.

W przypadku, gdy zachodzi konieczność składowania dokumentów przez okres dłuższy niż możliwy w ramach systemu Business Online, Spółka będzie zobowiązana zapewnić przechowywanie wszystkich wymaganych dokumentów we własnym zakresie.

4. Wyrejestrowanie eArchive

W sytuacji, gdy Spółka nie jest zainteresowana otrzymywaniem dokumentów w eArchive, jest ona zobowiązana wyraźnie poinformować Bank o swojej decyzji. Na indywidualny wniosek Spółki Bank może przesyłać dokumenty w wersji papierowej odpłatnie, przy czym wysokość opłaty zostanie uzgodniona odrębnie.

§ 9. Upoważninie Użytkowników na potrzeby systemu Business Online

Wszyscy Użytkownicy przeprowadzający transakcje w systemie Business Online w imieniu Spółki bądź osoby trzeciej muszą zostać należycie upoważnieni do tych czynności przez Spółkę. Stosowne upoważnienie może zostać utworzone na podstawie dokumentu Upoważnienie Użytkownika do systemu Business Online.

W przypadku, gdy osoba trzecia udzieli Spółce pełnomocnictwa, Spółka może delegować takie pełnomocnictwo na własnych Użytkowników w drodze udzielenia szczególnego Upoważnienia Użytkownika w systemie Business Online.

Przed stworzeniem Upoważnienia Użytkownika na potrzeby systemu Business Online, konieczne jest uzyskanie zgody Użytkownika na przekazywanie jego danych osobowych Bankowi w formie i treści wymaganej przez Bank. W celu dokonania dowolnych innych transakcji (np. przy stanowisku kasowym itp.), konieczne jest sporządzenie innych pełnomocnictw zgodnie z praktyką obowiązującą w Banku.

such documents in hardcopies by ordinary mail.

If the Company is a customer of one or more Danske Bank Entities, and the Company receives documents electronically from these companies, the Company can also receive such documents in Business Online.

The Bank can at any time increas the types and number of electronic documents accessible in eArchive, of which the Company will be separately notified in Business Online.

2. Access to the documents in eArchive

The rights and authorisations granted to the individual User determine which documents the User can view. A User will, for instance, always be able to view his/her individual User Authorisation in Business Online. Users with query access/access to operate an account are granted access to view the documents relating to the account in question in eArchive.

3. Archiving

The Bank stores the electronic requests and all documents in eArchive for the current year plus five years as a minimum. In case the Business Online agreement terminates, or the customer number changes, or any of the accounts is deregistered, or the Company no longer has access to Business Online for any other reason, the Company will not be able to receive documents in electronic form in eArchive and they will be deleted. In such cases it is advised that the Company makes copies of all documents, beforehand.

In case the documents are required to be stored for a longer period than possible via Business Online, the Company is obliged to assure storage of all required documents in own files.

4. Deregistering eArchive

In case the Company is not interested in receiving the documents in eArchive, it must specifically inform the Bank about it. At a separate request of the Company, the Bank may deliver documents in hardcopies against a fee to be agreed upon separately.

§ 9. User Authorisations for Business Online

All Users performing transactions in Business Online on behalf of the Company or a third party must be duly authorised to do so by the Company. The appropriate authorization can be created via the Bank's User Authorisation in Business Online.

If a third party has granted a mandate to the Company, the Company may delegate this mandate to its own Users, by way of effecting the special User Authorisation in Business Online.

Before the User Authorisation for Business Online is created, the User's consent to pass on his/her personal data to the Bank must be obtained in form and content required by the Bank.For effecting of any other transactions (e.g. via the cashier's desk, etc.), other mandates must be effected in accordance with binding Bank’s practice.

1. Prawa i autoryzacje Użytkowników

Zakres praw Użytkownika musi zostać określony dla każdego Użytkownika i obejmować w szczególności:

- przelewy pomiędzy rachunkami zarejestrowanymi w tym samym kraju prowadzonymi przez wszystkie Podmioty Danske Bank;
- zlecenia płatnicze za pośrednictwem SWIFT MT101;
- przelewy na niezarejestrowane rachunki pomiędzy Podmiotami Danske Bank i poza nimi;
- przelewy transgraniczne na rachunki zarejestrowane i niezarejestrowane pomiędzy Podmiotami Danske Bank i poza nimi; oraz
- inne produkty i usługi uzgodnione odrębnie.

Ponadto konieczne jest wskazanie, które rodzaje autoryzacji mają zostać przyznane danemu Użytkownikowi dla poszczególnych uprawnień Użytkownika, spośród tych wyszczególnionych poniżej:

- do podglądu;
- do tworzenia płatności/dokonywania ustawień;
- do zatwierdzania przez dwie osoby łącznie; oraz
- do zatwierdzania jednoosobowego.

Wybrany sposób autoryzacji będzie stosowany względem wszystkich płatności w ramach transakcji danego rodzaju. W przypadku wyboru bardziej restrykcyjnej metody autoryzacji na poziomie rachunku (dostęp do rachunków został opisany w ust. 7.2), taka autoryzacja zostanie zastosowana względem przelewów na rachunki niezarejestrowane i przelewów transgranicznych. W przypadku nieudzielenia autoryzacji Użytkownikowi na poziomie rachunku taki brak autoryzacji będzie traktowany jako ograniczenie i oznaczać będzie, że Użytkownik posiada jedynie prawo do podglądu.

2. Dostęp do rachunków

W przypadku, gdy Użytkownik został upoważniony do dokonywania przelewów na rachunki niezarejestrowane i przelewów transgranicznych, Użytkownik musi posiadać autoryzację na poziomie rachunku.

W odniesieniu do każdego rachunku, do którego Użytkownikowi udzielono dostępu na poziomie rachunku, Spółka musi wskazać rodzaj autoryzacji, której udzielono Użytkownikowi, spomiędzy wymienionych poniżej:

- osobna autoryzacja (Autoryzacja typu E);
- dwie osoby działające łącznie (Autoryzacja typu A);
- dwie osoby działające łącznie (Autoryzacja typu B);
- dwie osoby działające łącznie (Autoryzacja typu C).

Wszystkie rodzaje autoryzacji na poziomie rachunku stosowane przez Bank w systemie Business Online zostały opisane w ust. 8.

Metoda autoryzacji wybrana na poziomie rachunku znajduje zastosowanie do wszystkich Umów uzytkowania systemu Business Online, na mocy których dokonano rejestracji rachunku.

1. User rights and authorizations

The scope of User's rights must be defined for each particular User, embracing, in particular:

- payments between registered accounts in the same country within all Danske Bank Entities;
- payment requests via SWIFT MT101;
- payments to unregistered accounts between or outside the Danske Bank Entities;
- cross-border payments to registered and unregistered accounts between or outside the Danske Bank Entities;
- other products and services, as may be separately agreed.

Furthermore, it must be stated which authorisations a particular User is to be granted for each User right, from those listed below:

- view;
- create/set-up;
- approve two persons jointly;
- approve singly.

The selected authorisation is used for all payments within each transaction type. If a more restrictive authorisation at account level is selected (access to accounts is described in section 7.2), this authorisation is used for payments to unregistered accounts and cross-border payments. If no authorisation is granted to the User at an account level, it will be regarded as a restriction and means that the User has query (view) access only.

2. Access to accounts

In case a User is authorised to make payments to unregistered accounts and cross-border payments, he/she must have an authorisation at the account level.

For each account to which the User is granted access at the account level, the Company must state the type of authorisation which the User is granted, being any of:

- separate authorisation (E authorisation) ;
- two persons jointly (A authorisation);
- two persons jointly (B authorisation);
- two persons jointly (C authorisation).

All the account authorisation types used by the Bank in Business Online are described in section 8.

The authorisation chosen at the account level will apply to all Business Online agreements under which the account is registered.

3. Płatności poufne	**3. Confidential payments**
Spółka musi określić, czy dany Użytkownik jest upoważniony do dokonywania płatności poufnych. Płatności poufne obejmują płatności takie jak wynagrodzenia, w stosunku do których prawo podglądu oraz tworzenia i zatwierdzania płatności posiadają jedynie Użytkownicy ze specjalnymi uprawnieniami.	The Company must stipulate whether the particular 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 special privileges.
Użytkownicy są upoważnieni do dokonywania płatności poufnych w ramach rodzajów transakcji, do których przyznano im dostęp.	Users are authorised to make confidential payments within the transaction types, to which they have been granted access.
Nie ma rozróżnienia pomiędzy płatnościami poufnymi a niepoufnymi w kontekście zapytań dotyczących rachunków.	No distinction is made between confidential and non-confidential payments in connection with account queries.
4. Uprawnienia Administratora	**4. Administrator privileges**
Jeżeli zgodnie z postanowieniami Umowy użytkowania systemu Business Online powołany zostanie Administrator, Spółka musi określić które z poniższych rodzajów uprawnień administratora powinny zostać przyznane Użytkownikowi i w jakim zakresie:	If in accordance with the Business Online agreement an Administrator will be appointed, the Company must consider whether and which User will be granted administrator privileges in the form of:
• czynności Administratora Umowy;	• Agreement Administrator;
• czynności Administratora Użytkowników;	• Users Administrator;
• Informacje dotyczące Umowy;	• Agreement Information;
• logowanie i ustanawiania blokad; oraz	• Log-on and Blocking;
• ustanawianie limitów płatniczych na rachunkach.	• Payment Limit-Account.
W przypadku Użytkowników, którym udzielone zostaną uprawnienia Administratora Umowy i/lub Administratora Użytkowników, Spółka musi określić, które z poniższych rodzajów autoryzacji powinny zostać przyznane Użytkownikowi:	For Users, to whom an Agreement and/or Users Administrator privileges are granted, the Company must state which of the following authorisations should be granted to the User:
• do tworzenia płatności/dokonywania ustawień;	• create/set-up;
• do dokonywania odrębnej autoryzacji;	• separate authorisation;
• do dokonywania autoryzacji przez dwie osoby działające łącznie.	• two persons jointly authorisation.
Uprawnienia: „Informacje dotyczące Umowy" i "Logowania i ustanawiania blokad" mogą zostać udzielone jedynie w postaci osobnych autoryzacji.	The privileges: "Agreement Information" and "Log-on and Blocking" may be granted only as separate authorisations.
4.1. Autoryzacja w zakresie Umowy	**4.1. Agreement authorisation**
Użytkownik, któremu przyznane zostaną uprawnienia Administratora Umowy („Administrator Umowy"), jest upoważniony do dokonywania następujących czynności w imieniu Spółki:	A User to whom Agreement Administrator privileges are granted (the "Agreement Administrator") is authorised to perform the following actions on behalf of the Company:
• wnioskowanie o przyznanie bądź modyfikację przyznanych Użytkownikom uprawnień Administratora Umowy;	• request that Users are to be granted the Agreement Administrator privileges or that such privileges are modified;
• odbieranie uprawnień Administratora Umowy;	• delete Agreement Administrator privileges;
• tworzenie, modyfikowanie i odbieranie uprawnień Administratora Użytkowników – zob. ust. 9.4.2.;	• create, modify and delete User Administrator privileges - see section 9.4.2.;
• tworzenie i odbieranie uprawnień w zakresie Informacji o Umowie - zob. ust. 9.4.3;	• create and delete Agreement Information privileges- see section 9.4.3;
• tworzenie i odbieranie uprawnień użytkowników w zakresie logowania i ustanawiania blokad - zob. ust. 9.4.4.	• create and delete user privileges in relation to Logon and blocking - see section 9.4.4.
• tworzenie, edytowanie i odbieranie uprawnień w zakresie ustanawiania Limitów Płatniczych na rachunkach – zob. ust. 9.4.5.	• create, edit and delete Payment Limit – Account privileges - see section 9.4.5.
Spółka musi określić, czy Administrator Umowy ma zostać upoważniony do dokonywania	The Company must state whether the Agreement Administrator is to be authorised to

modyfikacji pod własnym ID Użytkownika.

Jeżeli Administrator Umowy podlega ograniczeniom w zakresie posługiwania się własnym ID Użytkownika, Administrator Umowy nie będzie mógł udzielić sobie autoryzacji, o których mowa powyżej, ani tworzyć czy zatwierdzać zleceń płatniczych. Powyższe dotyczy również uprawnień takiego Użytkownika z uprawnieniami Administratora Umowy jako Administratora Użytkowników.

Wnioski o udzielenie uprawnień Administratora Umowy muszą być zawsze podpisane przez osoby upoważnione zgodnie z prawem do reprezentowania Spółki. W przypadku, gdy Użytkownik posiadający uprawnienia Administratora Umowy złoży wniosek o utworzenie lub modyfikację Upoważnienia Użytkownika z uprawnieniami Administratora Umowy, Upoważnienie Użytkownika w systemie Business Online z polem podpisu zostanie wygenerowana w eArchive systemu Business Online. Upoważnienie Użytkownika jest dostępne dla wszystkich Użytkowników z uprawnieniami w zakresie Informacji o Umowie. Upoważnienie Użytkownika musi zostać podpisana w trybie określonym powyżej i przesłana Bankowi. W pozostałych przypadkach Użytkownik wykonuje czynności posługując się posiadanym podpisem cyfrowym.

Użytkownicy z uprawnieniami Administratora Umowy muszą posiadać również uprawnienia Administratora Użytkowników.

4.2. Administrator Użytkowników

Użytkownik, któremu przyznane zostaną uprawnienia Administratora Użytkowników („Administrator Użytkowników"), jest upoważniony do dokonywania następujących czynności w imieniu Spółki:

- tworzenie i modyfikowanie Użytkowników, w tym udzielanie Użytkownikom dostępu do wymaganych autoryzacji i rodzajów transakcji, modułów i rachunków zarejestrowanych na mocy Umowy w dowolnym czasie;
- tworzenie i modyfikowanie Danych Podstawowych Użytkowników;
- usuwanie wszystkich szczegółowych danych Użytkowników, w tym Danych Podstawowych.

Spółka musi określić, czy Administrator Użytkowników ma zostać upoważniony do dokonywania modyfikacji pod własnym ID Użytkownika.

Jeżeli Administrator Użytkowników podlega ograniczeniom w zakresie posługiwania się własnym ID Użytkownika, taki Administrator Użytkowników nie będzie mógł nadawać wymienionych wyżej uprawnień sobie samemu ani tworzyć czy zatwierdzać zleceń płatniczych. Powyższe dotyczy również uprawnień Użytkownika jako Administratora Umowy.

4.3. Informacje o Umowie

Dzięki funkcji „User overview" Użytkownicy, którym nadano uprawnienia w zakresie Informacji o Umowie mogą wyszukiwać Użytkowników Umowy i uzyskiwać wgląd w ich indywidualne uprawnienia (w tym w Dane Podstawowe, moduły, uprawnienia Administratora, dostęp do rachunków i płatności).

Użytkownicy mają dostęp do funkcji „User overview" i wybranych dokumentów przechowywanych w systemie Business Online.

4.4. Logowanie oraz blokowanie Użytkowników

Użytkownik, któremu nadane zostaną uprawnienia w zakresie logowania oraz blokowania Użytkowników, jest upoważniony do dokonywania następujących czynności w imieniu Spółki:

make modifications under his/her own User ID.

If an Agreement Administrator is subject to restricted use under his/her own User ID, the Agreement Administrator will neither be able to grant himself/herself the authorisations stated above nor to create and approve payment requests. The aforementioned also applies to this Agreement Administrator user's privileges as User Administrator.

Requests for granting of the Agreement Administrator privileges must always be signed by persons legally authorised to represent the Company. When a User having Agreement Administrator privileges has requested the creation or modification of a User Authorisation with Agreement Administrator privileges, a User Authorisation Business Online with a signature field is generated in the Business Online eArchive. The User Authorisation is accessible to all Users with Agreement Information privileges. The User Authorisation must be signed as stated above and sent to the Bank. In all other cases, the User takes actions using his/her digital signature.

Users with Agreement Administrator privileges must also have User Administrator privileges.

4.2. User Administrator

A User to whom the User Administrator privileges are granted (the "User Administrator") is authorised to perform the following actions on behalf of the Company:

- create and modify the Users, including giving Users the access to the required uthorisations and transaction types, modules and accounts registered under the Agreement at any time;
- create and modify User Master Data;
- delete all User's details, including Master Data.

The Company must decide whether the User Administrator is to be authorised to make modifications under his/her own User ID.

If a User Administrator is subject to restricted use under his/her own User ID, he/she will neither be able to grant the above privileges to once self nor will the User Administrator be able to create and approve payment requests. The aforementioned also applies to the User's privileges as Agreement Administrator.

4.3. Agreement Information

Via a User overview, Users to whom Agreement Information privileges are granted can search by Agreement Users and view their individual privileges (including Master Data, modules, Administrator privileges, access to accounts and payment access).

Users have access to the User overview and selected documents stored in Business Online.

4.4. Log-on and Blocking

A User to whom the Log-on and Blocking privileges are granted is authorised to perform the following actions on behalf of the Company:

- zamawianie tymczasowych kodów PIN dla Użytkowników;
- zamawianie urządzeń eSafeID; oraz
- blokowanie i odblokowywanie Użytkowników.

4.5. Ustanawianie limitów płatniczych na rachunkach

Użytkownik, któremu nadane zostaną uprawnienia w zakresie ustanawiania limitów płatniczych na rachunkach, jest upoważniony do dokonywania następujących czynności w imieniu Spółki:

- tworzenie, edytowanie i usuwanie limitów płatniczych na rachunkach, którymi Użytkownik może w dowolnym czasie dysponować na mocy Umowy.

Spółka musi określić, które z poniższych rodzajów autoryzacji powinny zostać udzielone Użytkownikom posiadającym uprawnienia w zakresie ustanawiania limitów płatniczych na rachunkach:

- samodzielna autoryzacja (Autoryzacja E);
- dwie osoby działające łącznie (Autoryzacja A);
- dwie osoby działające łącznie (Autoryzacja B);
- dwie osoby działające łącznie (Autoryzacja C).

Rodzaje autoryzacji na poziomie rachunków zostały opisane w ust. 8.

5. Zmiana Autoryzacji Użytkowników w systemie Business Online

W celu zwiększenia lub ograniczenia dostępu konkretnego Użytkownika do systemu Business Online konieczne jest podpisanie nowego Upoważnienia Użytkownika dla systemu Business Online zastępującej poprzednie Upoważnienie. W przypadku, gdy zmiana dotyczy Upoważnienia Użytkownika na poziomie rachunku, Spółka jest zobowiązana również podpisać Pełnomocnictwo do dysponowania rachunkami dla przedsiębiorców, a w uzasadnionych przypadkach osoba trzecia jest zobowiązana podpisać nowe upoważnienie dla osoby trzeciej.

W przypadku, gdy zmiany są dokonywane za pośrednictwem modułu Administracji systemu Business Online przez Administratora Umowy i/lub Użytkowników umowy, zmiany są zatwierdzane przy użyciu podpisu cyfrowego. Jeśli zmiana obejmuje również uprawnienia Administratora Umowy, Upoważnienie Użytkownika musi zostać podpisana zgodnie z wewnętrznymi regulacjami Spółki w zakresie składania oświadczeń woli.

Na zakres upoważnień do działania wynikający z Upoważnienia Użytkownika w systemie Business Online może mieć wpływ udzielenie przez Spółkę Pełnomocnictwa do dysponowania rachunkiem dla przedsiębiorców.

6. Odwoływanie Upoważnień Użytkowników w systemie Business Online

Upoważnienie Użytkownika w systemie Business Online zachowuje moc obowiązującą do czasu jej odwołania przez Spółkę, z zachowaniem formy pisemnej lub przy użyciu podpisu elektronicznego, w zależności od sytuacji. W wyjątkowych okolicznościach autoryzacje mogą również zostać odwołane telefonicznie. Jednakże takie telefoniczne odwołanie autoryzacji musi zostać każdorazowo niezwłocznie potwierdzone na piśmie. Z chwilą otrzymania wspomnianego wyżej zawiadomienia przez telefon uprawnienia Użytkownika do działania w imieniu Spółki za pośrednictwem systemu Business Online zostają zablokowane.

W przypadku otrzymania przez Bank zawiadomienia o odwołaniu, Bank prześle pisemne potwierdzenie usunięcia ID i klucza Użytkownika z systemów.

- order temporary PINs for Users;
- order eSafeID device;
- block and unblock Users.

4.5. Payment Limit – Account

A User to whom Payment Limit - Account privileges are granted is authorised to perform the following actions, on behalf of the Company:

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

The Company must state which of the following authorisations should be granted to Users with Payment Limit - Account privileges:

- separate authorisation (E authorisation);
- Two persons jointly (A authorisation);
- Two persons jointly (B authorisation);
- Two persons jointly (C authorisation).

The account authorisation types are described in section 8.

5. Changing Business Online User Authorisations

In order to extend or limit a particular User's access to Business Online, a new User Authorisation for Business Online must be signed, replacing the previous one. If the change relates to the User's authorisations at account level, the Company must also sign a Mandate to operate accounts for entrepreneurs, and, where applicable, the third party must sign a new third party authorisation.

If the changes are made via Business Online Administration by the Agreement and/or User Administrator of the agreement, the changes are approved by using digital signature. If the change also comprises Agreement Administrator privileges, User Authorisation must be signed in accordance with internal Company's signing regulations.

A User's authorisation in Business Online may be affected if the Company issues a Mandate to operate accounts for entrepreneurs.

6. Revoking Business Online User Authorisations

User Authorisation for Business Online remain in force until it is revoked by the Company, either in writing or using an electronic signature where applicable. Exceptionally, authorisations may also be revoked by telephone, however this must always be followed up by immediate written confirmation. The User's access to act on behalf on the Company via Business Online is blocked after such a notification was received by phone.

In case the Bank has received notice of revocation, the written confirmation that the user ID and key have been deleted from the systems will be sent.

W przypadku wygaśnięcia całej Umowy Dostępu do systemu Business Online Bank uzna to za równoważne z odwołaniem wszystkich Upoważnień Użytkowników przyznanych na mocy takiej Umowy.

Jeżeli Spółka i/lub osoba trzecia udzieliły Użytkownikowi pełnomocnictwa do działania na rachunku, pełnomocnictwo to musi zostać odwołane w odrębnym trybie. W takim przypadku odwołanie samego Upoważnienia Użytkownika w systemie Business Online nie jest wystarczające.

7. Transakcje z udziałem rachunków osób trzecich w systemie Business Online

W sytuacji, gdy Spółka rozważa przeprowadzanie transakcji na rachunkach osób trzecich prowadzonych w dowolnym Podmiocie Danske Bank, dana osoba trzecia jest zobowiązana podpisać przygotowany przez Bank formularz pełnomocnictwa dla osób trzecich.

Jeżeli istnieje potrzeba zapewnienia możliwości składania zapytań dotyczących rachunków osób trzecich poza Bankiem, konieczne jest zawarcie specjalnej umowy z Bankiem, zważywszy, że takie zapytania muszą być kierowane za pośrednictwem systemu SWIFT i przy użyciu MT940. Ponadto osoba trzecia musi zawrzeć umowę z bankiem prowadzącym rachunek wskazując, że Bank może otrzymywać dane dotyczące rachunków zewnętrznych osoby trzeciej.

W sytuacji, gdy Spółka rozważa dokonywanie płatności z rachunków osoby trzeciej na rachunki inne niż prowadzone przez Podmioty Danske Bank, konieczne jest zawarcie z Bankiem specjalnej umowy w tym celu. Ponadto osoba trzecia jest zobowiązana zawrzeć umowę z bankiem prowadzącym rachunek wskazując, że Podmioty Danske Bank mogą wysyłać dyspozycje płatnicze do banku(-ów) osoby trzeciej.

Danske Bank rejestruje rachunki osób trzecich w systemie Business Online w ramach Umowy Dostępu zawartej ze Spółką.

8. Upoważnienie do zawierania transakcji walutowych

W celu zapewnienia możliwości podglądu do sald rozliczeń walutowych i zawierania walutowych transakcji spot i transakcji terminowych Użytkownik musi posiadać dostęp do jednego bądź więcej modułów Markets Online. Dostęp do opcji zawierania walutowych transakcji spot i transakcji terminowych wymaga również udzielenia przez Spółkę Użytkownikowi specjalnych autoryzacji w zakresie realizacji transakcji na rynku walutowym. Wspomniane autoryzacje upoważniają Użytkownika jedynie do wykonywania transakcji w imieniu Spółki za pośrednictwem modułów Markets Online.

Wszystkie transakcje dotyczące zawierania walutowych transakcji spot i transakcji terminowych podlegają postanowieniom umowy ramowej w zakresie nettingu i ostatecznego rozliczania transakcji zawieranych pomiędzy Spółką a właściwym Podmiotem Danske Bank.

9. Upoważnienie do zawierania transakcji Trade Finance w systemie Business Online

W sytuacji, gdy Użytkownik jest upoważniony do wystawiania akredytyw, windykowania wierzytelności i/lub wystawiania gwarancji, Spółka jest zobowiązana zarejestrować takiego Użytkownika w module dotyczącym usług Trade Finance i podpisać zgodę na Podłączenia do/Modyfikacji modułu Trade Finance w Umowie o dostęp do systemu Business Online. W tym celu Spółka musi określić, czy Użytkownik powinien mieć dostęp do:

- akredytyw (eksportowych i/lub importowych);
- inkasa wierzytelności (eksportowych i/lub importowych); oraz

In case the entire Business Online Access Agreement is terminated, the Bank shall consider this as revocation of all User Authorisations granted under the Agreement.

If the Company and/or a third party have granted the User a mandate to operate the account, this mandate must be revoked separately. It is not sufficient just to revoke the Business Online User Authorisation.

7. Transactions involving third party accounts in Business Online

If the Company contemplates making transactions on third-party accounts with any of Danske Bank Entities, the third party must sign the Bank's third-party mandate form.

If account queries are to be possible on third-party accounts outside the Bank, a special agreement with the Bank must be concluded, since such queries must be made through SWIFT and by using MT940. Furthermore, the third party must conclude an agreement with the account-holding bank, stating that the Bank may receive data about the third party's external accounts.

If the Company considers making payments from the third party's accounts to outside the Danske Bank Entities, a special agreement to this effect must be concluded with the Bank. Furthermore, the third party must conclude an agreement with the account-holding bank, stating that the Danske Bank Entities may send payment instructions to the third party's bank(s).

Danske Bank registers third-party accounts in Business Online via the Company's Access Agreement.

8. Authorisation to enter into foreign exchange transactions

In order to be able to view trade positions and enter into foreign exchange spot and forward transactions, the User must have access to one or more Markets Online modules. Access to enter into foreign exchange spot and forward transactions also requires that the Company grants the User a special Currency trading authorisations. These authorisations only authorise the User to perform transactions on behalf of the Company via Markets Online.

All transactions relating to concluding foreign exchange spot and forward transactions are subject to the provisions of the framework agreement on netting and final settlement of trades concluded between the Company and the relevant Danske Bank Entity.

9. Trade Finance Authorisation in Business Online

If a User is to be authorized 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 Business Online Agreement. For this purpose, the Company must state whether the User should have access to:

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

- gwarancji.

Ponadto Spółka musi wskazać, czy Użytkownik powinien posiadać uprawnienia do:

- tworzenia i składania zapytań;
- tworzenia i zatwierdzania – przez dwie osoby działające łącznie; lub
- tworzenia i zatwierdzania – osobna autoryzacja.

§ 10. Rodzaje autoryzacji

Bank wykorzystuje następujące rodzaje autoryzacji:

- samodzielna autoryzacja (Autoryzacja typu E);
- dwie osoby działające łącznie (Autoryzacja typu A);
- dwie osoby działające łącznie (Autoryzacja typu B);
- dwie osoby działające łącznie (Autoryzacja typu C).

Powyższe autoryzacje umożliwiają Spółce wskazanie, którzy Użytkownicy mogą, samodzielnie bądź łącznie, zatwierdzać płatności bądź zlecenia. Poniżej przedstawiono szczegółowy opis poszczególnych rodzajów autoryzacji.

1. **Samodzielna autoryzacja**

   W sytuacji, gdy zlecenia czy płatności są tworzone bądź zmieniane przez Użytkownika w ramach tej autoryzacji, są one automatycznie traktowane jako zatwierdzone przez tego Użytkownika. Użytkownicy posiadający ten rodzaj autoryzacji mogą również zatwierdzać zlecenia czy płatności wprowadzane przez Użytkowników posiadających wszelkie inne rodzaje autoryzacji.

2. **Autoryzacja przez dwie osoby działające łącznie**

   W sytuacji, gdy Użytkownik posiadający autoryzację dwuosobową (dokonywaną przez dwie osoby działające łącznie) tworzy zlecenie płatnicze bądź dokonuje płatności, wymagana jest autoryzacja (druga autoryzacja) dokonana przez innego Użytkownika.

3. **Autoryzacja przez dwie osoby działające łącznie (Autoryzacja typu A)**

   W sytuacji, gdy zlecenia lub płatności są tworzone przez Użytkownika posiadającego Autoryzację typu A, są one automatycznie zatwierdzane przez tego Użytkownika (pierwsza zgoda). Następnie wymagane jest uzyskanie kolejnej zgody (druga zgoda) ze strony Użytkownika posiadającego samodzielną autoryzację lub Autoryzację typu A, B lub C. Użytkownicy posiadający Autoryzację typu A posiadają ten sam poziom uprawnień. Stąd kolejność uzyskiwania zgód nie ma znaczenia.

4. **Autoryzacja przez dwie osoby działające łącznie (Autoryzacja typu B)**

   W sytuacji, gdy zlecenia lub płatności są tworzone przez Użytkownika posiadającego Autoryzację typu B, są one automatycznie zatwierdzane przez tego Użytkownika (pierwsza zgoda). Następnie wymagane jest uzyskanie kolejnej zgody (druga zgoda) ze strony Użytkownika posiadającego samodzielną autoryzację, Autoryzację typu A lub C. Dwóch Użytkowników posiadających Autoryzację typu B nie może łącznie zatwierdzić żadnej płatności.

5. **Autoryzacja przez dwie osoby działające łącznie (Autoryzacja typu C)**

   W sytuacji, gdy zlecenia lub płatności są tworzone przez Użytkownika posiadającego Autoryzacja typu C, są one automatycznie zatwierdzane przez tego Użytkownika

Furthermore, the Company must state whether the User should have access to:

- create and inquire;
- create and approve - two persons jointly or;
- create and approve - separately.

§ 10. Authorisation types

Danske Bank operates with the following authorisation types:

- Separate authorisation (E 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 as follows.

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.

2. **Two persons jointly**

   When a User with a two persons-jointly-authorisation creates a payment request or a payment, the authorisation (2nd authorisation) from another User is required.

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.

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.

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

(pierwsza zgoda). Następnie wymagane jest uzyskanie kolejnej zgody (druga zgoda) ze strony Użytkownika posiadającego samodzialną autoryzację, Autoryzację typu A lub B. Dwóch Użytkowników posiadających Autoryzację typu C nie może łącznie zatwierdzić żadnej płatności.

.

§ 11. Wsparcie klientów

Bank zapewnia wsparcie i obsługę Spółkom w formie:

- administrowania Użytkownikami;
- wsparcia telefonicznego, w tym blokowania obsługi w systemie Business Online;
- wsparcia za pośrednictwem Internetu; oraz
- wsparcia na miejscu.

Administrowanie Użytkownikami często obejmuje zawieranie Umów Dostępu i ustanawianie autoryzacji, korektę dostępu Spółki (i Użytkowników działających w jej imieniu) do różnego rodzaju funkcji wsparcia i obsługi, usuwanie i blokowanie Użytkowników, zamawianie tymczasowych kodów PIN i rejestrowanie zmian do autoryzacji, itp.

Wsparcie telefoniczne może obejmować szkolenie, instruktaż dla Użytkowników, pomoc w rozwiązywaniu problemów, wytyczne w zakresie wprowadzania zmian oraz opcję blokowania systemu Business Online. Wsparcie telefoniczne w związku z instalacją, ustawieniem, szkoleniem i rozwiązywaniem problemów itp. w systemie Business Online jest zapewniane we współpracy z Działem IT Spółki i na ryzyko Spółki.

Wsparcie za pośrednictwem Internetu może obejmować szkolenie, instruktaż Użytkowników, pomoc w rozwiązywaniu problemów oraz wytyczne w zakresie wprowadzania zmian. Wsparcie za pośrednictwem Internetu jest zapewniane we współpracy z Działem IT Spółki i na ryzyko Spółki.

Wsparcie na miejscu może obejmować instalację systemu bankowości biurowej Banku i szkolenie z zakresu jego użytkowania, jak również rozwiązywanie problemów. Rozwiązywanie problemów może skutkować dostosowaniem i/lub modyfikacją ustawień komputerów i systemów informatycznych Spółki, modyfikacją baz rejestrowanych danych, instalacją ruterów, zapór sieciowych i serwerów proxy, wewnętrznych systemów zabezpieczeń oraz innych modyfikacji oprogramowania i sprzętu komputerowego. Usługi instalacji i rozwiązywania problemów są zapewniane we współpracy z Działem IT Spółki i na ryzyko Spółki.

III. Business Online – Systemy zabezpieczeń

§ 12. Kwestie techniczne

1. **Transmisja danych oraz dostęp**

Spółka jest zobowiązana ustanowić łącze komunikacyjne do przesyłania danych z Bankiem w celu uzyskania możliwości użytkowania systemu Business Online. Wszelkie koszty związane z ustanowieniem łącza, zakupem, instalacją, ustawieniami i utrzymaniem wymaganego wyposażenia IT ponosi Spółka.

Zważywszy na fakt, że stale wdrażane są nowe wersje systemu Business Online, Spółka

cannot jointly approve a payment.

.

§ 11. Customer suport

The Bank provides support and service to the Company in the form of:

- User administration;
- telephone support, including blocking service in Business Online;
- internet-based support;
- on-site support.

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

Telephone support may include training, User's instruction, troubleshooting assistance, guidance in relation to modifications, and an option to block Business Online. Telephone support in connection with installation, set-up, training and troubleshooting etc. of Business Online is provided in cooperation with the Company's IT department and at the risk of the Company.

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

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

III. Business Online – Security systems

§ 12. Technical Issues

1. **Transmission and access**

The Company must establish a data communication link with the Bank to be able to use Business Online. All costs related to the link, purchase, installation, set up and maintaining the required IT equipment will be borne by the Company.

Since Business Online is constantly upgraded, the Company must ensure that the necessary adaptations to the IT equipment - in order to be able to use the link and ensure continuity of operations are in place.

jest zobowiązana zadbać o dokonywanie na bieżąco koniecznych aktualizacji posiadanego wyposażenia IT w celu zapewnienia możliwości korzystania z łącza i ciągłości działania.

Bank może w każdej chwili bez uprzedzenia dokonać modyfikacji w posiadanym wyposażeniu, podstawowym oprogramowaniu i właściwych procedurach w celu optymalizacji działalności operacyjnej i poziomu obsługi. Bank poinformuje Spółkę o wszelkich zmianach wymagających aktualizacji wyposażenia Spółki w celu utrzymania łącza i dostępu, z zachowaniem 30-dniowego okresu pisemnego powiadomienia, za pośrednictwem systemu Business Online bądź w inny sposób.

Spółka nie może stosować specjalnego oprogramowania tzw. nakładek ani podobnych rodzajów oprogramowania przy uzyskiwaniu dostępu do systemu Business Online. Użytkownicy są zobowiązani obsługiwać system bezpośrednio przez interfejs Użytkownika i przy użyciu oprogramowania dostarczonego przez Bank.

2. Dystrybucja oprogramowania, jego kontrola i przechowywanie

Bank prowadzi dystrybucję programów wymaganych do zainstalowania/aktualizowania systemu Business Online. Programy te można pobrać z Internetu.

Przy pobieraniu programów z Internetu Spółka lub dany Użytkownik są zobowiązani sprawdzić, czy pobranie programu zostało potwierdzone/podpisane przez Bank drogą elektroniczną (cyfrowo).

Powodem, dla którego programy nie zostały elektronicznie (cyfrowo) potwierdzone/podpisane przez Bank, może być to, że ktoś w nie ingerował lub to, że nie pochodzą od Banku. Podpis może zostać następnie zweryfikowany poprzez sprawdzenie właściwości pobranego(-ych) pliku(-ów) z programem. W przypadku, gdy podany podpis elektroniczny nie pochodzi od Banku, nie należy instalować pobranego programu.

3. Bezpieczeństwo danych

Spółka wyraża zgodę na to, aby Bank używał danych osobowych Użytkowników, w chwili rejestrowania ich jako Użytkowników systemu Business Online zgodnie z właściwymi przepisami o przetwarzaniu danych osobowych. Bankowi przysługuje prawo, za pośrednictwem systemu Business Online do zbierania danych dotyczących adresów IP Użytkowników oraz czasu logowania, zakresu informacji wymienianych w trakcie komunikacji pomiędzy Użytkownikami i Bankiem oraz innych danych i nformacji, które w ocenie Bank są niezbędne do należytego funkcjonowania systemu Business Online.

Funkcjonowanie system Business Online może być oparte o świadecznie przez Bank usług za pośrednictwem serwerów będących własnością osób trzecich, zgodnie z obowiązującymi przepisami o ochronie danych osobowych oraz przepisami innych właściwych regulacji.

eSafeID, e-Safekey and EDISec stanowią kompleksowe systemy zabezpieczeń stosowane w ramach serwisu Business Online.

eSafeID jest systemem zabezpieczeń sieciowych Banku służącym do logowania się do serwisu Business Online. Natomiast eSafeID jest dwustopniowym systemem uwierzytelniania, co oznacza, że uwierzytelnianie Użytkowników jest przeprowadzane w oparciu o element znany Użytkownikowi (jego hasło osobiste) i element znajdujący się w posiadaniu Użytkownika (urządzenie eSafeID generujące kody bezpieczeństwa). Kod bezpieczeństwa generowany przez urządzenie eSafeID jest tymczasowo zapisywany w sesji przeglądarki, w czasie gdy Użytkownik loguje się do systemu Business Online.

e-Safekey i EDISec są systemami zabezpieczeń Banku przeznaczonymi dla klientów, którzy postanowili wymieniać informacje z Bankiem drogą elektroniczną bezpośrednio z wykorzystaniem posiadanych systemów biznesowych. e-Safekey i EDISec bazują na

The Bank may at any time and without notice modify its own equipment, basic software and related procedures in order to optimise operations and service levels. The Bank will notify the Company of any modifications requiring adaptation of the Company's equipment in order to retain the link and access, by giving 30 days' written notice via Business Online or otherwise.

The Company may not use special software such as "overlay services" or similar types of software when accessing the Business Online system. Users must operate the system directly via the User interface and the software provided by the Bank.

2. Distribution, control and storage of software

The Bank distributes the programs required to install/upgrade Business Online. You can download the programs from the Internet.

When programs are downloaded from the Internet, the Company or a particular User must check that the program delivery has been electronically (digitally) confirmed/signed by the Bank.

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

3. Data and data security

The Company accepts that the Bank will use personal data on the Users when registering them as Users of Business Online in accordance with applicable law on processing of personal data. The Bank may, through Business Online, collect data about a user's IP address and time of log-in, the business communication between the Users and the Bank and other data that the Bank considers relevant to ensure the appropriate operation of Business Online.

Functionalities of Business Online may be carried out by the Bank using 3. party server solutions in accordance with applicable law on the processing of personal data and other applicable regulations.

eSafeID, e-Safekey and EDISec are the general security systems used in Business Online.

eSafeID is the Bank's web-based security system to log on to Business Online. The eSafeID is a two-level authentication system, which means that it is based on something the User knows (his/her personal password) and something the User has (his/her eSafeID device that generates security codes). The security code generated by the eSafeID device is saved temporarily in the browser session while the User is logging on to Business Online.

e-Safekey and EDISec are the Bank's security systems for the customers who want to exchange information with the Bank electronically directly through their own business systems. e-Safekey and EDISec are built on a password (digital signature) and use permanent encryption keys stored in the Company's IT environment.

zastosowaniu haseł (podpisów cyfrowych) i stosują stałe klucze szyfrujące przechowywane w środowisku informatycznym Spółki.

Korzystanie z tych systemów zabezpieczeń daje pewność, że dane są właściwie szyfrowane przed ich przesłaniem do Banku i że nie są przedmiotem ingerencji w trakcie przesyłania. Ponadto autentyczność podpisu cyfrowego nadawcy jest zawsze sprawdzana, a wszystkie transakcje rodzące skutki finansowe są opatrzone podpisem cyfrowym. Bank jest uprawniony do zablokowania dostępu Spółki lub Użytkownika do systemu Business Online w przypadku odnotowania nie mniej niż 3 prób wykorzystania dostępu niezgodnie z przeznaczeniem. Spółka zostanie niezwłocznie powiadomiona o zablokowaniu dostępu do systemu Business Online.

Spółka jest zobowiązana wdrożyć skuteczne procedury bezpieczeństwa w celu zapobieżenia nieuprawnionemu wykorzystywaniu systemu Business Online i dostępowi osób nieuprawnionych do kluczy Użytkownika i urządzenia eSafeID.

Bardziej szczegółowe informacje na temat zaleceń w zakresie bezpieczeństwa można znaleźć w folderze „Bezpieczeństwo" w systemie Business Online na stronie internetowej Banku oraz w innych wytycznych.

§ 13. Pobieranie ID Użytkownika, hasła tymczasowego i urządzenia eSafeID

W sytuacji, gdy profil Użytkownika ma zostać utworzony w systemie Business Online z systemem zabezpieczeń eSafeID, Bank przekazuje Użytkownikowi indywidualne ID Użytkownika, hasło tymczasowe i urządzenie eSafeID. Hasło tymczasowe jest wykorzystywane wraz z urządzeniem eSafeID do identyfikacji Użytkownika w czasie pierwszego logowania do systemu zabezpieczeń.

W sytuacji, gdy profil Użytkownika ma zostać utworzony w systemie Business Online z systemami zabezpieczeń e-Safekey lub EDISec, Bank przekazuje Użytkownikowi indywidualne ID Użytkownika i hasło tymczasowe. Hasło tymczasowe służy do identyfikacji Użytkownika podczas pierwszego logowania do systemu zabezpieczeń.

Hasło tymczasowe jest generowane przez system i drukowane elektronicznie bez możliwości przejęcia go przez kogokolwiek. W sytuacji, gdy koperta zawierająca pismo z hasłem tymczasowym i/lub pismo z urządzeniem eSafeID została otwarta lub nosi ślady ingerencji, Użytkownik jest zobowiązany skontaktować się z Bankiem w celu zamówienia nowego hasła tymczasowego i/lub nowego urządzenia eSafeID. Ze względów bezpieczeństwa pisma zawierające hasło tymczasowe i urządzenie eSafeID nie są nadawane w tym samym terminie.

W sytuacji, gdy Użytkownik nie otrzymał pisma z hasłem tymczasowym w terminie siedmiu dni roboczych od złożenia zamówienia, Użytkownik jest zobowiązany, ze względów bezpieczeństwa, skontaktować się z Bankiem w celu anulowania hasła i zamówienia kolejnego. W czasie rejestracji w systemie zabezpieczeń Użytkownik wybiera jasło osobiste i jest zobowiązany następnie zniszczyć hasło tymczasowe.

1. Przechowywanie ID Użytkownika, hasła osobistego i urządzenia eSafeID

Poniższe zasady regulują korzystanie z systemów eSafeID, e-Safekey i EDISec:

- Wyłącznie Użytkownik ma prawo posługiwać się ID Użytkownika, hasłem osobistym i urządzeniem eSafeID;
- Hasło, urządzenie eSafeID i kody bezpieczeństwa mają charakter ściśle osobisty i nie wolno ich ujawniać osobom trzecim;
- Hasło i kody bezpieczeństwa mogą być wykorzystywane wyłącznie na potrzeby

Using these security systems ensures that the data is properly encrypted before being transmitted to the Bank and is not tampered with during transmission. In addition, the authenticity of the sender's digital signature is always checked, and all financially binding transactions are provided with a digital signature. The Bank is entitled to block a Company's or any User's access to Business Online, if it registers numerous, not less then 3, attempts of misuse. If the access is blocked, the Company will be immediately notified about it.

The Company must implement effective security procedures to prevent unauthorised use of Business Online and unauthorised access to User keys and the eSafeID device.

Further information about security recommendations is available under the "Security" folder in Business Online on the Bank's website and in other guidelines.

§ 13. Acquiring a User ID, temporary password and eSafeID device

When a User is to be created in Business Online with the eSafeID security system, the Bank gives the User an individual User ID, a temporary password and an eSafeID device. Together with the eSafeID device, the temporary password is used for the first-time identification when the User logs-on to the security system.

When a User is to be created in Business Online with the e-Safekey or EDISec security systems, the Bank gives the User an individual User ID and a temporary password. The temporary password is used for first-time identification when the User logs-on to the security system.

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

If the User has not received the letter containing the temporary password within seven workdays of ordering, the User must, for security reasons, contact the Bank in order to cancel it and order a new one. While registering in the security system, the User chooses a personal password and must subsequently destroy the temporary one.

1. Storing the User ID, personal password and eSafeID device

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

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

komunikowania się z Bankiem;

- Hasła nie należy zapisywać ani przechowywać razem z urządzeniem eSafeID.

2. Zmiana hasła

Użytkownik jest zobowiązany regularnie zmieniać swoje hasło, a zadaniem Spółki jest dopilnować, żeby Użytkownik należycie wywiązywał się z tego obowiązku.

Bardziej szczegółowe informacje na temat zaleceń w zakresie bezpieczeństwa można znaleźć w folderze „Bezpieczeństwo" w systemie Business Online na stronie internetowej Banku oraz w innych wytycznych.

3. Wyrejestrowanie Użytkowników

Spółka jest zobowiązana powiadamiać Bank o konieczności usunięcia Użytkowników. Spółka ponosi odpowiedzialność za wszystkie transakcje realizowane przez Użytkownika do czasu złożenia w Banku należytego wniosku o usunięcie bądź zablokowanie autoryzacji udzielonych danemu Użytkownikowi. Spółka ponosi również odpowiedzialność za wszystkie przyszłe transakcje zrealizowane przez usuniętego i/lub zablokowanego Użytkownika przed należytym powiadomieniem Banku o konieczności usunięcia takich transakcji.

4. Niezgodne z przeznaczeniem użycie zabezpieczeń lub groźba takiego użycia

Spółka i/lub Użytkownik są zobowiązani niezwłocznie skontaktować się z Bankiem w celu zablokowania dostępu Użytkownika w sytuacji, gdy:

- którekolwiek z nich podejrzewa, że hasło osobiste, klucz szyfrujący lub urządzenie eSafeID Spółki bądź Użytkownika zostało użyte niezgodnie z przeznaczeniem; lub
- nieuprawnione osoby uzyskały dostęp do hasła osobistego lub osobistego klucza szyfrującego czy też weszły w posiadanie urządzenia eSafeID.

IV. Business Online – Aspekty postanowień umownych

§ 14. Przeznaczenie wyłącznie na potrzeby prowadzonej działalności gospodarczej

System transakcyjny Business Online jest przeznaczony wyłącznie do celów biznesowych. Informacje udostępniane Spółce, w tym informacje cenowe, nie mogą być ujawniane osobom nieuprawnionym. Spółce nie wolno przekazywać osobom trzecim uzyskanych informacji, chyba że ich przekazanie następuje za pisemną zgodą Banku.

§ 15. Zmiany usług i wsparcia związanych z systemem Business Online

System Business Online zapewnia dostęp do usług oferowanych przez Bank.

Bank może w dowolnym czasie rozszerzyć lub zawęzić zakres usług świadczonych za pośrednictwem systemu Business Online. Dodawanie nowych usług do aktualnie świadczonego zakresu w systemie Business Online nie wymaga akceptacji przez Spółkę pod warunkiem, że nowe usługi są dla Spółki korzystne i nie wiążą się ze znaczącym wzrostem kosztów. Ograniczenie zakresu usług oferowanych za pośrednictwem systemu Business Online może nastąpić wyłącznie z zachowaniem 14-dniowego okresu.

Bank może wprowadzać zmiany do treści niniejszego Regulaminu z zachowaniem 14-dniowego okresu powiadomienia, przy czym informacje dotyczące zmian będą przesyłane pocztą elektroniczną lub zwykłą. Ponadto obowiązująca wersja Regulaminu

device.

2. Changing the password

The User must change his/her password regularly, and it is the Company's responsibility to ensure that this is done diligently.

Further information about security recommendations is available under the "Security" folder in Business Online on the Bank's website and in other guidelines.

3. Deregistering Users

The Company must inform Bank if Users are to be deleted. The Company shall be responsible for all transactions performed by the User until the Bank was duly requested to delete or block the authorizations for a particular User. The Company shall also be responsible for all future transactions made to date by a deleted and/or blocked User until the Bank will have been duly notified that the transactions should be deleted.

4. Misuse or risk of misuse

The Company and/or the User are obliged to immediately contact the Bank in order to block the User access, in case when:

- either of them suspects that the personal password, the Company's or User's encryption key or the eSafeID device has been misused;
- unauthorized persons have had access to the personal password, the personal encryption key or have gained possession of the eSafeID device.

IV. Business Online – Contractual aspects

§ 14. For business purposes only

Business Online transaction system is designed to be used for business purposes only. The information made available to the Company, including price information, is not to be disclosed to any unauthorized persons. The Company may not pass on the information to others, except with written permission from the Bank.

§ 15. Changes to services and support relating to Business Online

Business Online gives access to the services offered by the Bank.

The Bank may at any time extend or reduce the scope of services offered via Business Online. Adding new services to the currently offered scope of the Business Online does not require any acceptance from the Company, provided that the new services are beneficial for the Company and not imply any material cost increase. Any reduction in the scope of services offered via Business Online may only be effected with 14 days' prior notice.

The Bank has a right to amend these Terms and Conditions subject to 14 days prior notification, and information on changes will be provided by email or ordinary mail. Additionally, the binding version of the Terms and Conditions is published on the Bank's website.

The amended Terms and Conditions will apply, unless the Company notifies the Bank in

zostanie podana do publicznej wiadomości na stronie internetowej Banku.

Zmieniony Regulamin wejdzie w życie, chyba że Spółka powiadomi Bank na piśmie, że nie akceptuje zmienionego Regulaminu. Wówczas podstawowy stosunek prawny łączący strony zostanie uznany za wypowiedziany z dniem wejścia w życie zmian do Regulaminu.

To samo dotyczyć będzie również zmiany cennika wchodzącego w skład Regulaminu.

§ 16. Obowiązki oraz zakres odpowiedzialności stron

1. Obowiązki Spółki

Użytkowanie systemu Business Online odbywa się na wyłączną odpowiedzialność i ryzyko Spółki.

Ryzyko ponoszone przez Spółkę obejmuje między innymi ryzyko związane z:

- przesyłaniem informacji do Banku, w szczególności zaś ryzyko zniszczenia, utraty, uszkodzenia, opóźnienia przesyłanych informacji lub wystąpienia w nich błędów bądź opuszczeń związanych z przesyłem, np. powstałych w trakcie pośredniego przekazywania lub przetwarzania treści danych;
- udostępnieniem informacji osobom trzecim w wyniku błędów bądź nieuprawnionego przejęcia danych w obrębie łącza służącego do transmisji danych;
- realizacją wszelkich czynności i transakcji przy użyciu klucza własnego Spółki lub kluczy zarejestrowanych Użytkowników;
- zapewnianiem przechowywania kluczy Użytkownika w środowisku informatycznym Spółki w celu zapobieżenia nieuprawnionemu dostępowi do kluczy;
- pilnowaniem, żeby Użytkownicy zabezpieczali swoje hasła, tak by nie zostały one ujawnione osobom nieuprawnionym; lub
- nieprawidłowym bądź niezgodnym z przeznaczeniem użytkowaniem systemu Business Online przez zarejestrowanych Użytkowników.

Bank nie ponosi odpowiedzialności za skutki wymienionych wyżej zdarzeń. Spółce również nie przysługują żadne roszczenia względem Banku z tytułu błędów i pominięć wynikających z okoliczności leżących po stronie Spółki, w tym nieprzestrzegania przez nią procedur bezpieczeństwa i kontroli.

Ponadto do obowiązków Spółki należy:

- uzyskanie zgody poszczególnych Użytkowników przed przekazaniem ich danych osobowych Bankowi;
- upewnienie się, że zawartość foldera Upoważnienie Użytkownika zawsze odpowiada zakresowi autoryzacji przyznanej danemu Użytkownikowi przez Spółkę i/lub osobę trzecią (w zależności od okoliczności) i jest z nim zgodna;
- zapewnienie poprawności wszystkich dokumentów elektronicznych przesyłanych przez Bank w stopniu odpowiadającym poprawności takich samych dokumentów przesyłanych w wersji papierowej zwykłą pocztą;
- niezwłoczne powiadamianie Banku w razie braku dostępności systemu Online przez jakikolwiek okres, a w razie braku dostępności systemu zwracanie się do Banku o przesłanie dokumentów elektronicznych w wersji papierowej zwykłą pocztą.

Ponadto obowiązkiem Spółki jest dopilnowanie, żeby Użytkownicy znali aktualną treść niniejszego Regulaminu użytkowania systemu Business Online i przestrzegali go, jak również stosowali się do wyświetlanych na ekranie i obowiązujących czasowo wskazówek w zakładce

writing that the Company is not accepting the amended Terms and Conditions and therefore the underlying contractual relationship will be considered terminated as from the effective date of the Terms and Conditions amendment.

The same also relates to the amendment of the price list forming a part of the Terms and Conditions.

§ 16. Responsibilities and liability

1. The Company's responsibilities

Use of Business Online is at the sole responsibility and risk of the Company.

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

- sending information to the Bank, and in particular 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;
- all operations and transactions made using the Company's own key or keys of registered Users;
- ensuring storage of User keys in the Company's IT- environment in order to prevent unauthorised access to the keys;
- ensuring that Users keep their passwords secure so that they are not disclosed to unauthorized persons;
- any incorrect use or misuse of Business Online by registered Users.

The Bank cannot be held liable for any consequences of the above enlisted occurrences. Neither the Company can make any claims on the Bank in respect of errors and omissions resulting from circumstances pertaining to the Company, including non-observance of safety and control procedures.

In addition, it is the Company's responsibility to:

- obtain the consent of each User before passing on his/her personal data to the Bank;
- ensure that the content of User Authorisation folder always matches and is in accordance with the contemplated scope of authorisation given to a particular User by the Company and/or any third party (as may be applicable);
- ensure the correctness of all electronic documents sent by the Bank , to the same extent as if the electronic documents had been sent in hardcopy by ordinary mail;
- notify the Bank immediately, in case Business Online is not accessible for a period of time and consequently the Company would like to receive electronic documents in hardcopy by ordinary mail.

Furthermore, it is the Company's responsibility to ensure that Users are aware of and comply with these Terms and Conditions for Business Online, , as may be amended, as well as the on-screen Help instructions, as may be applicable from time to time.

Help.

2. Obowiązki Banku

Bank ponosi odpowiedzialność odszkodowawczą w sytuacji, gdy, w wyniku błędu bądź zaniedbania dopuści się zwłoki w wykonaniu swoich obowiązków w ramach Umowy lub wykona swoje obowiązki w sposób nienależyty.

Jednakże Bank nie ponosi odpowiedzialności za błędy i/lub zaniechania będące wynikiem:

- nieprawidłowego działania oprogramowania stanowiącego własność osób trzecich, które wchodzi w skład systemu zabezpieczeń serwisu Business Online;
- ujawnienia przez Użytkownika tymczasowego kodu PIN i/lub hasła osobom nieuprawnionym;
- modyfikacji systemu zabezpieczeń przez osoby trzecie bez wiedzy Banku;
- integracji systemu zabezpieczeń z innymi systemami czy oprogramowaniem nie dostarczonym przez Bank; lub
- wykorzystania informacji i danych przekazanych przez osoby trzecie.

W każdym przypadku, a zwłaszcza w obszarach podlegających ściślejszym uregulowaniom w zakresie odpowiedzialności prawnej, Bank zrzeka się odpowiedzialności za straty będące wynikiem:

- awarii/przerw w pracy systemów informatycznych bądź zniekształcenia danych przechowywanych w tych systemach w wyniku wystąpienia zdarzeń wymienionych poniżej, niezależnie od tego, czy Bank eksploatuje systemy samodzielnie, czy też powierza podmiotom zewnętrznym eksploatację dowolnej części tych systemów;
- awarii łączy telekomunikacyjnych bądź braku zasilania w obiektach Banku, działań urzędów państwowych czy czynności administracyjnych, klęsk żywiołowych, działań wojennych, powstań, niepokojów społecznych, aktów sabotażu, zamachów terrorystycznych czy aktów wandalizmu (w tym stosowania wirusów komputerowych i włamywania się do systemów informatycznych);
- strajków, lokautów, bojkotów czy blokad, niezależnie od tego, czy dane działanie jest wymierzone w Bank bądź jego organizację lub przez Bank bądź jego organizację wywołane, i niezależnie od przyczyny powstania konfliktu. Dotyczy to również sytuacji, w której konflikt rzutuje na działalność jedynie niektórych jednostek organizacyjnych Banku; lub
- innych okoliczności pozostających poza kontrolą Banku.

Wyłączenie odpowiedzialności Banku nie znajduje zastosowania w sytuacji, gdy:

- Bank powinien był przewidzieć wystąpienie okoliczności skutkujących stratami w chwili zawierania Umowy bądź też powinien był zapobiec powstaniu strat bądź wyeliminować ich przyczynę; lub
- na mocy bezwzględnie obowiązujących przepisów prawa Bank uznaje się, niezależnie od okoliczności, za stronę odpowiedzialną za powstanie strat.

Bank ponosi odpowiedzialność jedynie za szkody bezpośrednie, a co za tym idzie, nie ponosi odpowiedzialności za żadne szkody pośrednie czy wtórne, niezależnie od tego, czy takie szkody są następstwem błędu czy zaniechania po stronie Banku.

Bank ponosi odpowiedzialność odszkodowawczą na mocy postanowień ust. 14.2 powyżej z uwzględnieniem właściwych przepisów Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2011 nr 199 poz. 1175, z późn. zm., „Ustawa o usługach płatniczych"), z wyłączeniem art. 144-146 tej Ustawy.

2. The Bank's responsibilities

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

However, the Bank will not be liable for errors and/or omissions resulting from:

- malfunctions of the third-party owned software which is part of the Business Online security system;
- a User's disclosure of the temporary PIN and/or the password to unauthorised persons;
- modifications to the security system effected by third parties without the Bank's knowledge;
- the security system's integration with other systems or software which were not delivered by the Bank;
- information and data provided by third parties.

In any case, especially in areas which are subject to stricter regulations on liability, the Bank will not be liable for losses resulting from:

- IT-systems failure/downtime or corruption of data in these systems as a result of the events listed below, irrespective of whether the Bank operates the systems itself or has outsourced any of its operations;
- telecommunication lines or power failures at the Bank, statutory intervention or administrative acts, natural disasters, wars, rebellions, civil unrest, acts of sabotage, terrorism or vandalism (including computer viruses and hacking);
- strikes, lockouts, boycotts or blockades, irrespective of whether the conflict is targeted at or initiated by the Bank or its organisation and irrespective of the cause of the conflict. This also applies if the conflict affects only some organizational units of the Bank;
- any other circumstances beyond the Bank's control.

The Bank's exemption from liability does not apply, when:

- the Bank should have predicted the circumstances resulting in the loss at the time when the Agreement was concluded, or should have prevented or overcome the cause of the loss;
- under any absolutely binding provisions of law the Bank under any circumstances is designated as liable for the cause of the loss.

The Bank is only liable for direct losses and is therefore not liable for any indirect or consequential damage, regardless of whether such damage is due to errors or omissions on the part of the Bank or not.

The Bank is liable in damages according to section 14.2 above, provided that the respective provisions of the Law on payment services of 19 August 2011(Journal of Laws of 2011 No. 199, item 1175, as amended- the "Law on Paymnet Services") shall be applicable, with the exclusion however of articles 144-146 thereof.

§ 17. Postanowienia różne

1. Struktura Umowy o dostęp do systemu Business Online

Na Umowę użytkowania systemu Business Online składają się następujące dokumenty:

- Umowa Dostępu do systemu Business Online;
- Upoważnienie(-a) Użytkownika do systemu Business Online;
- Opis modułów systemu Business Online;
- Regulamin użytkowania systemu Business Online;
- Regulamin Otwierania i Prowadzenia Rachunków Bankowych dla Przedsiębiorców;
- Godziny graniczne przyjmowania zleceń i stosowane daty waluty obowiązujące w Danske Bank A/S S.A. Oddział w Polsce;
- Tabela opłat i prowizji obowiązująca w Danske Bank A/S S.A. Oddział w Polsce; oraz
- Help Dokumenty i programy –pomoc Użytkownikowi.

Wszystkie wymienione wyżej dokumenty stanowią integralną część Umowy Dostępu do systemu Business Online i wchodzą w życie z dniem zawarcia Umowy Dostępu przez Spółkę.

W przypadku ewentualnych rozbieżności pomiędzy dowolnymi wymienionymi wyżej dokumentami pierwszeństwo mają dokumenty umieszczone wyżej na liście.

Ponadto zastosowanie znajdują Regulamin i pozostałe obowiązujące dokumenty dotyczące Umów o korzystanie z poszczególnych Modułów oraz Umowa Dostępu.

Składając podpis pod Umową Dostępu do systemu Business Online, Spółka potwierdza również, że zapoznała się oraz akceptuje treść niniejszego Regulaminu i innych obowiązujących dokumentów składających się na Umowę użytkowania systemu Business Online.

Regulamin użytkowania systemu Business Online oraz pozostałe regulaminy są dostępne na stronie internetowej Banku.

2. Ceny oraz opłaty

Bank ma prawo w dowolnym czasie wprowadzić zmiany w wysokości opłat i prowizji z zachowaniem 14-dniowego okresu pisemnego powiadomienia za pośrednictwem poczty elektronicznej lub zwykłej poczty. Bank będzie obciążać opłatami i prowizjami rachunek/rachunki wyszczególnione jako rachunek/rachunki służący(-e) do regulowania opłat i prowizji, chyba że strony postanowią inaczej w odrębnym trybie (np. w regulaminie dotyczącym danego modułu).

Bank jest uprawniony do pobierania i naliczania opłat i prowizji po upływie więcej niż jednego miesiąca od realizacji transakcji, za którą pobierana jest taka opłata lub prowizja.

Bank jest uprawniony do naliczania opłaty z tytułu przekazywania informacji uzupełniających z większą częstotliwością niż przewidziana w Umowie o dostęp do systemu Business Online.

Bank może naliczać opłaty i prowizje od płatności zrealizowanych przez Spółkę z dowolnego rachunku, jak również z tytułu powiadomienia Spółki o wszelkich zrealizowanych płatnościach.

3. Cesja, przelew oraz osoby trzecie

Umowa Dostępu do systemu Business Online została zawarta przez Bank i dotyczy wszystkich Podmiotów Danske Bank. Oznacza to, że każdy z Podmiotów Danske Bank ma prawo wykonywać i egzekwować postanowienia tej Umowy. Oznacza to również,

§ 17. Other terms and conditions

1. Structure of the Business Online Agreement

A Business Online Agreement consists of the following documents:

- Business Online - Access Agreement;
- User Authorisation(s) for Business Online;
- Module Description for Business Online;
- Terms and Conditions for Business Online;
- Terms and Conditions for Opening and Maintaining Bank Accounts for Entrepreneurs;
- Cut-off times and value dates applicable at Danske Bank A/S S.A. Branch in Poland;
- Fees and Charges Table applicable at Danske Bank A/S S.A. Branch in Poland;
- Help documents and programs.

All of the aforementioned documents form an integral part of Business Online Agreement and become valid as from concluding of the Access Agreement by the Company.

In case of any discrepancy between any of the above referred to documents, the listed order of priority will apply.

Furthermore, the Terms and Conditions and other applicable documents, related to the individual Module Agreements or the Access Agreement shall apply.

By signing the Business Online Access Agreement, the Company also acknowledges having read and accepted these Terms and Conditions and other applicable documents forming part of the Business Online Agreement.

The Terms and Conditions for Business Online and other terms and conditions are accessible on the Bank's website.

2. Prices and fees

The Bank may at any time change the fees and charges by giving a 14 days' written notice via email or ordinary mail. The Bank will debit fees and charges to the account(s) specified as fee account(s), unless otherwise separately agreed (e.g. in the terms and conditions relating to each specific module).

The Bank is entitled to collect and debit fees later than one month after completion of the transaction for which a fee is charged.

The Bank is entitled to charge a fee for providing supplementary information more frequent than as agreed in the Business Online Agreement.

The Bank may charge fees for payments made by the Company from an account as well as for notifying the Company of any payments made.

3. Assignment, transfer and third parties

This Agreement has been concluded by the Bank and relate to all Danske Bank Entities. This means that any of the Danske Bank Entities is entitled to fulfil and enforce this Agreement. It also means that the Bank may transfer its rights and obligations to another Danske Bank

że Bank może przelać swoje prawa i obowiązki na inny Podmiot Danske Bank w dowolnym czasie.

Bank ma prawo powierzyć wykonanie Umowy podwykonawcom, zgodnie z właściwymi przepisami. Takie powierzenie wykonania Umowy nie będzie miało wpływu na zakres obowiązków Banku w ramach Umowy.

4. Postanowienia szczególne dotyczące rachunków płatniczych i usług płatniczych

W odniesieniu do rachunków płatniczych zastosowanie znajdują postanowienia Regulaminu Otwierania i Prowadzenia Rachunków Bankowych dla Przedsiębiorców obowiązującego w Danske Bank A/S S.A. Oddział w Polsce oraz zapisy Ustawy o usługach płatniczych.

Bank i Spółka niniejszym wspólnie zrzekają się prawa do stosowania przepisów o usługach płatniczych w zakresie, w jakim dopuszcza to obowiązujące prawo.

W przypadku, gdy Spółka dysponuje rachunkiem płatniczym w ramach specjalnego instrumentu płatniczego, takiego jak karta kredytowa, zapisy stosownego regulaminu dotyczącego użytkowania właściwego rachunku płatniczego będą regulowane osobno w treści umów dotyczących danych instrumentów płatniczych.

Na Spółce ciąży obowiązek bieżącego sprawdzenia wszystkich transakcji względem zapisów księgowych. Spółka jest zobowiązana powiadamić Bank niezwłocznie (nie później niż w terminie 14 dni od otrzymania wyciągu z rachunku dokumentującego daną transakcję) w przypadku wykrycia przez Spółkę transakcji, co do których zachodzi podejrzenie, że mogły zostać przeprowadzone w sposób oszukańczy przez osobę trzecią.

§ 18. Wypowiedzenie Umowy oraz naruszenie postanowień Umowy

Spółka ma prawo rozwiązać Umowę użytkowania systemu Business Online poprzez rozwiązanie Umowy Dostępu na piśmie bez uprzedzenia. Zlecenia i transakcje rozpoczęte przed datą rozwiązania Umowy zostaną zrealizowane.

Bank może rozwiązać Umowę użytkowania systemu Business Online poprzez rozwiązanie Umowy o dostęp z zachowaniem formy pisemnej i 14-dniowego okresu powiadomienia.

Bank może jednak rozwiązać Umowę o użytkowanie systemu Business Online bez uprzedzenia w sytuacji, gdy Spółka dopuści się naruszenia postanowień dowolnego spośród wymienionych dokumentów: Umowy użytkowania systemu Business Online, Umowy Dostępu czy Regulaminu użytkowania systemu Business Online, bądź innego dokumentu stanowiącego część Umowy użytkowaniq systemu Business Online, co ma miejsce na przykład wówczas, gdy Spółka zaniecha uregulowania wobec Banku należnych opłat i prowizji w trybie uzgodnionym w Umowie Dostępu, zawiesi realizację płatności, wszczęte wobec niej zostanie postępowanie naprawcze bądź likwidacyjne, lub też zajdą inne okoliczności o podobnym charakterze.

§ 19. Prawo właściwe

Postanowienia niniejszej Umowy podlegają przepisom prawa polskiego i jurysdykcji sądów polskich.

W sytuacji, gdy Spółka jest zarejestrowana w module, który przewidziany jest dla użytkowania w całości bądź częściowo poza granicami Polski, Spółka - podobnie jak i Bank - przyjmuje do wiadomości, że warunki realizacji takich transakcji określają regulaminy banków zagranicznych oraz przepisy prawa i zwyczaje obowiązujące w danym kraju.

Entity at any time.

The Bank is entitled to transfer the performance under this Agreement to subcontractors, in accordance with separate regulations. Such transfer will not affect the Bnak's responsibilities under the Agreement.

4. Special provisions concerning payment accounts and payment services

Rules and Regulations for Opening and Maintaining Bank Accounts for Entrepreneurs applicable at Danske Bank A/S S.A. Branch in Poland and further the Polish Law on Paymet Services shall apply in relation to payment accounts.

The Bank and the Company hereby unanimously waive the applicable regulations on payment services to the extent as it is possible in accordance with the applicable provisions of law.

In case the Company have the disposal of a payment account by way of a special payment instrument such as a credit card, the terms and conditions thereof are regulated separately in the agreements on the payment instruments concerned.

The Company is under an obligation to check all transactions in relation to the accounts on an ongoing basis. The Company is obliged to notify the Bank immediately (and not later than within 14 day from receiving the account statement, documenting the relevant transaction) in case when the Company discovers transactions that, may potentially be fraudulently performed by any third party.

§ 18. Termination and breach of the Busienss Online Agreement

The Company may terminate the Business Online Agreement by termination of the Access Agreement in writing without notice. Requests and trades initiated before the time of termination will be carried out.

The Bank may terminate the Business Online Agreement by termination of the Access Agreement in writing by giving 14 days' notice.

The Bank may, however, terminate the Business Online Agreement without notice if the Company is in breach of the any of the Business Online Agreement, Access Agreement or the Terms and Conditions for Business Online, or any other document forming part of the Business Online Agreement, which is the case, when the Company, for instance, omits to pay the Banks fees, as agreed in the Access Agreement, suspends its payments, is subject to restructuring or winding-up procedure or another situation of alike nature.

§ 19. Governing law

This Agreement is governed by Polish law and the legal venue is Poland.

If the Company is registered for a module that is wholly or partly intended to be used abroad, the Company accepts - like the Bank - that the terms and conditions of the foreign banks and the legal rules and usage apply for the completion of the transaction.