Annex 1 Terms and conditions for dedicated MitID for business use (separate MitID for business)

A. Introduction 2
B. Use of dedicated MitID 2
C. Binding actions 3
D. Rules for the use of MitID 3
D.1 Registration of information when creating a dedicated MitID 3
D.2 Choice of authenticator 3
D.3 Assurance levels 3
D.4 Storage of authenticators 4
D.5 Safety in use 5
D.6 Administration of your user profile in MitID Erhverv and selected authenticators 5
D.7 Suspension and Blocking of dedicated MitID 5
D.7.1 Duty to suspend or block dedicated MitID 5
D.7.2 Request for blocking 6
D.7.3 Other cases of suspension and blocking 6
D.8 Processing of personal data 7
D.8.1 Data responsibility 7
D.9 Changing the rules for using dedicated MitID 7
E. Support and additional information about MitID 8
E.1 Support 8
E.2 Additional information about dedicated MitID 8

Version 1.3

A. Introduction

The Terms and Conditions for MitID describe the rules you must comply with, when using a dedicated MitID issued to you as business user via a User Organisation connected to MitID Erhverv. Dedicated MitID for business use is also referred to as a separate MitID for business.

A dedicated MitID consists of a unique user ID (user name) and one or more associated authenticators.

A dedicated MitID is to be used for business purpose only and must be used in accordance with the user organisation's own rules. This includes rules for provisions of power and articles of association.

The terms and conditions are available on http://www.mitid-erhverv.dk

A dedicated MitID consists of a user ID to be used with one or more associated authenticators (MitID password, MitID app, MitID code display, MitID audio code reader, MitID chip) to confirm your identity in MitID Erhverv, when interacting with a digital self-service solution.

Your user organisation defines which authenticators you can utilise as a user of MitID Erhverv.

MitID Erhverv is made available by the Danish Agency for Digital Government in cooperation with public partners.

Nets DanID A/S handles the administration of the MitID solution.

The Danish Agency for Digital Government is data controller for the MitID Erhverv solution. Additional information on the processing of data and data processors can be found in the privacy policy for MitID Erhverv at www.mitid-erhverv.dk.

If you have questions about personal data, please contact the Danish Agency for Digital Government by email:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
CVR-nr.: 34 05 11 78
E-mail: digst@digst.dk

B. Use of dedicated MitID

You can use a dedicated MitID with selected digital services, which require that your identity is confirmed securely. Access to services and functionality can be limited by the privileges the service or your user organisation are able to use.

C. Binding actions

You establish, who you are, when you log in or approve a transaction using a dedicated MitID – or when you use your dedicated MitID in the signature service Underskrift (digital signature). The use of dedicated MitID for electronic signature service requires the acceptance of separate terms and conditions prior to issuing the signature.

D. Rules for the use of MitID

D.1 Registration of information when creating a dedicated MitID

The process of creating a dedicated MitID will make use of the information your user organisation already has registered about you. If this information is not correct, you are obliged to discontinue the use of your dedicated MitID and update the information with your user organisation.

D.2 Choice of authenticator

Your authenticator is chosen by your user organisation when creating the dedicated MitID. These terms may therefore address other authenticators, than what you have access to use.

D.3 Assurance levels

You are set up in MitID Erhverv user at a given assurance level (Substantial or High).

You can log in with your dedicated MitID at three different assurance levels, if you are registered in MitID at the corresponding level:

- **Low** - With some digital services, you can simply use your MitID user ID together with at least one means of identification, e.g., MitID password
- **Substantial** – Most digital services require that, in addition to your MitID user ID, you use two different authenticators from separate categories, for example MitID app with corresponding PIN code.
- **High** – With selected digital self-service solutions, which require a very high level of security: Two authenticators are required from separate categories, and the two authenticators must, among other things, be extra secured against copying and manipulation, e.g., MitID password combined with MitID chip (this is extra secure against copying and manipulation).

The assurance level determines which actions you are allowed to complete with MitID and depends on which authenticator you use.

The following explains which authenticators and their combinations that can be used at the various security levels:

- **Assurance level low** (is sufficient for a small number of primarily private digital services)
  - The assurance level can be achieved by using the MitID app, MitID password or MitID chip
- **Assurance level Substantial** (required by the majority of public and private digital services)
  - The assurance level can be achieved by using the MitID app or a combination of MitID password and MitID code display or a combination of MitID password and MitID Chip
  - Blind or visually impaired individuals can achieve this assurance level by combining the MitID password with the MitID audio code reader
- **Assurance level High** (required for selected public and private digital services)
  - The assurance level can be achieved by using the MitID app installed on a device with a built-in microprocessor chip which can store sensitive data and start applications protected from malware, or by combining the MitID password with the MitID chip or combining the MitID app with the MitID chip.

D.4 Storage of authenticators

You must protect your dedicated authenticator, so it can't be used by others. Therefore you must be aware that you

- must protect your authenticator, so it cannot be used by others. You are not in any way to physically write down your password or your PIN code to your MitID app;
- must not inform any other person about your MitID user ID. However, you are allowed to inform your user administrator in MitID Erhverv or MitID Erhvervs support, if you initiate the contact;
- must not inform any other person about your MitID password and other codes;
- must not store your MitID password or other codes unencrypted on any device;
- must not store your MitID password together with your MitID code display, MitID audio code reader or MitID chip or save your MitID password on the same device, where the MitID app is installed;
- must not write your MitID password on your MitID code display, MitID audio code reader and MitID chip;
- may only install your MitID app on devices that you control either privately or for business use;
- in addition, you must follow the instructions that your user organisation has issued.

D.5 Safety in use

General rules for using MitID can be found in the security guide for MitID authenticators, which you can find at MitID.dk.

You need to make sure that

- your user ID and authenticator are only used by you in a secure and responsible manner and in accordance with these Terms and Conditions for dedicated MitID for business use;
- other individuals do not have the opportunity to read or otherwise gain insight into your MitID password or PIN code for the MitID app, when you enter these;
- you use MitID on a device, where the operating system, internet browser and other programs are continuously updated with the latest security updates.

You must continuously check that:

- you have not lost your MitID code reader, MitID audio code reader, MitID chip or devices, with your MitID app is installed;
- MitID has not been misused, e.g., by logging into the MitID Erhverv solution

D.6 Administration of your user profile in MitID Erhverv and selected authenticators

Administration of your user profile and authenticators can be handled by yourself or a user administrator in MitID Erhverv.

You can check the event log of to see your usage of your dedicated MitID and the digital services you have been logged in to. In this way, you can continuously check that your dedicated MitID has only been used with digital services, you have visited.

D.7 Suspension and Blocking of dedicated MitID

Suspension is a temporary state that can be reopened, whereas blocking is a permanent state similar to decommissioning.

D.7.1 Duty to suspend or block dedicated MitID

You must immediately via MitID Erhverv, user administrator or via MitID Erhverv support:

- suspend your dedicated MitID Business user ID (username), if you suspect that it has been misused or compromised;
- block your dedicated MitID code reader, MitID audio code reader or MitID chip, if you have lost one or more of these;
- block your MitID app, if you have lost a device on which your MitID app is installed, or if you suspect that unauthorized persons have access to your MitID app or know your PIN code;

- change your dedicated MitID password, if you suspect that unauthorized persons have obtained or may have obtained knowledge of it, and if this cannot be done, block your MitID password;
- block your MitID code reader, MitID audio code reader or MitID chip, if the device is broken.

D.7.2 Request for blocking

You can block your dedicated MitID in the following way:

- Via MitID Erhverv self-service and your user profile
- Via a User Administrator in MitID Erhverv
- Via MitID Erhverv support on phone +45 33980021

Further information about support can be accessed via www.mitid-erhverv.dk/support.

When contacting MitID Erhverv support, you must state your MitID Erhverv user ID, your name and the name or CVR number of your user organisation, when you want to block your dedicated MitID.

A blocked dedicated MitID cannot be reopened. If your dedicated MitID is blocked, a user administrator will have to create a new one for you in the MitID Erhverv solution.

D.7.3 Other cases of suspension and blocking

You should be aware that blocking or suspension will also occur in the following situations. Suspension is a temporary condition. Blocking or suspension can be done automatically by the MitID or MitID Erhverv solution.

- your dedicated MitID password is blocked, if suspicion or knowledge exist that others have gained knowledge of this;
- your dedicated MitID password is suspended for a shorter period, if the password is entered incorrectly number of times. Your password will be blocked, if the password is entered incorrectly again a certain number of times after the suspension is lifted;
- your MitID app is blocked, if suspicion or knowledge exist that others know the PIN code for your MitID app;
- your MitID app is blocked if there suspicion or certainty exist that the device you are using has been compromised;
- your MitID app is suspended, if there suspicion or certainty exist that the device you are using has significant security gaps;
- your dedicated MitID is blocked, if it is known that you have not complied with the Terms and Conditions for MitID Erhverv;

- your dedicated MitID is suspended, if it is suspected that your dedicated MitID has been misused or compromised;
- your dedicated MitID is suspended upon the introduction of new Terms and Conditions for dedicated MitID, until you have accepted these;
- your MitID Erhverv identity and associated dedicated authenticators are blocked, if it is announced from the CPR register that you have passed away;
- your MitID Erhverv identity and associated authenticators are blocked, if your association with the User Organisation is terminated;
- your MitID Erhverv identity and associated dedicated authenticators may be suspended or blocked based on updates on the user organisation's business status from the CVR register

You can contact your user administrator in MitID Erhverv or read more at www.mitid-erhverv.dk.

D.8 Processing of personal data

You can read about what information the Danish Agency for Digital Government collects, stores and processes about you in connection with the issuance and administration of MitID in the Privacy Policy here: www.MitID.dk/juridisk/privatlivspolitik/.

You must, among other things, be aware that personal data about you is passed on to the service you use. You must also be aware that information about e.g., your name and company affiliation are part of the identity in MitID Erhverv, to which the dedicated authenticator is associated, and are therefore also passed on to the digital self-service solutions that you choose to log in to with the dedicated MitID. Which information is passed on depends on the specific authorization for processing which the self-service solution possesses.

D.8.1 Data responsibility

The Danish Agency for Digital Government is data controller for your personal data, which is processed in the MitID solution and MitID Erhverv. Nets DanID A/S is the data processor for the Danish Agency for Digital Government. If Nets DanID A/S uses a subcontractor who processes your personal data, then the subcontractor becomes a subprocessor of your personal data.

The processing of your personal data is subject to the data protection rules found in the Data Protection Regulation and the Data Protection Act, which you can find by following this link: https://www.retsinformation.dk/eli/lta/2018/502.

D.9 Changing the rules for using dedicated MitID

The Danish Agency for Digital Government has the right to change the rules in accordance with the agreement between the Danish Agency for Digital Government and your user organisation. You will be asked to accept updated terms and conditions, the first time you use your dedicated MitID after a terms and conditions update.

E. Support and additional information about MitID

E.1 Support

Your user organisation is responsible for providing support.

First, contact your user administrator in the user organisation, for which the dedicated authenticator was issued.

If you experience problems using a particular service, please contact it. Finally, for general technical problems related to dedicated MitID, you can contact MitID Erhverv support on phone +45 33980020 or via contact form http://www.mitid-erhverv.dk/kontakt.

E.2 Additional information about dedicated MitID

For additional information about dedicated MitID, contact the Danish Agency for Digital Government. You can also read more at MitID-erhverv.dk.