Appendix No 1

Security requirements for using the DDE platform by the Client and User

*For the safe use of the means of communication used by the Client/User when using the Platform [in particular, but not only: smartphone, computer (desktop/ laptop), tablet, including software and hardware elements and e-mail (hereinafter: **Device**)] to make valid electronic statements of will binding on the Client, including signing an agreement and using the Platform, as well as to preserve the Client's/User's personal data and the Client's bank secrets, the proper maintenance and security of these Devices will be essential and the continuous fulfillment of the following security requirements will be necessary, for which the Client and the User will be jointly responsible:*

- *the device is accessible only and exclusively after successful identification of the Client/User on the device, and the data used for identification is changed regularly and may not be easily guessed (PIN code — for smartphones/for tablets, password);*
- *the elements of the Device (operating system, firmware, browser, other applications) are regularly updated in accordance with the manufacturer's recommendations and are professionally and securely set up;*
- *the Device's network connections are set up securely using appropriate wireless network security procedures (e.g. encryption and authentication), restricting access to network devices;*
- *the display of the Device is visible only to the Client/User during the process;*
- *saving the username and password in the browser is not recommended;*
- *it is recommended to use a password that is at least 9 characters long, contains lower- and upper-case letters, numbers, special characters, does not contain meaningful words from the dictionary, the usage of a special password is recommended, and it is recommended that the Client/User avoids re-using passwords, used for other services, it is generally recommended to use a secure password store.*

In addition to the above, in respect of smartphones/tablets:

- *security mechanisms, the authorisation system and other subsystems of the operating system are not modified on the device (root - Android, jailbreak - iOS);*
- *SMS viewing is not allowed on lock screen;*
- *The PIN code does not contain data that can be easily known, e.g. date of birth, recurring characters, e.g. 111111.*

In respect of desktop/laptop, in addition to the above:

- *has a legitimate, up-to-date protection against malicious code (virus protection, anti-malware) – virus scanning is performed regularly and its scope extends to downloaded files, data carriers connected to the device, with modern security solutions (e.g. firewall).*

In addition, the Client/User guarantees that when using the Platform for the exchange of digital documents electronically, the communication tools used to make an electronic statement accessible only to the Client/User, and access by third parties is impossible.

The Bank reserves the right - but is not obliged - to limit the types of messages delivered without special notice, to pause or terminate the sending of messages, to suspend or limit the operation of the access provided by the Bank to the Platform on devices operating with an operating a system modified by the manufacturer or the Client/User in such a way that the Client/ User's access to the operating system or its subsystems is not limited (including, but not limited to: "jailbreak", "unlock", "root" and similar modifications) or the modification of the operating system may carry other data security risks - an outdated and vulnerable version of the browser or operating system is used. Browser-based systems and applications may contain software code to modify the operating system and/ or check the version of the browser and/or operating system, and information about the modified operating system may be forwarded by the application to the Bank.