National Centre for Emissions Management
Institute of Environmental Protection
National Research Institute

Security requirements for users of the Union Registry IT system

1. Each Authorized Representative possesses an individual, confidential Password that allows the access to the secure section of the Registry Website and is used during the authorization of operations performed in the Registry. Password should consist of a minimum of 10 characters chosen from at least three of the following four character groups (spaces may be used): uppercase letters, lowercase letters, digits, special characters. Password cannot consist of the first name, last name, email address, or username of Authorized Representative.

2. It is recommended to change the Password at least once every 30 days. Changed Password must be different from the previously used Passwords.

3. Registry Administrator never requests the confidential Password used in the Registry.

4. Authorized Representatives are prohibited from sharing Passwords with other individuals, including representatives of the Registry Administrator.

5. Authorized Representatives are prohibited from sharing with other individuals their mobile phone or other mobile device with the EU Login application installed.

6. Authorized Representatives should ensure that while logging and performing operations in the Registry, they enter data according to the "*Union Registry User Manual*" provided by the Registry Administrator.

7. The Registry Website in the web browser should display a 'closed padlock' symbol indicating a page with a current security certificate (usually found in the lower right corner or in the address bar). Authorized Representatives should verify if the server's security certificate on which the Union Registry application operates is valid and correct. More information on the certificate verification process is available in the "*Union Registry User Manual*."

8. While logging into to the Registry the identification of Authorized Representatives is done by providing email address, correct Password, and Code generated in the EU Login mobile application based on the scanned QR Code.
Proper identification provides the access to the Account information, enables Authorised Representatives to initiate and approve Transactions, as well as to perform other operations through the Registry, to which they have been assigned based on an application submitted by the Account Holder.

9. If Authorized Representatives are asked to provide Password or email address not through the EU Login system, they should immediately contact the Registry Administrator.

10. After accessing the secure section of the Registry Website, Authorized Representatives should constantly verify whether they remain in the secure zone (using the https protocol along with the correct certificate). In case of session expiration before logging in again, the web browser should be completely closed.

11. Authorized Representatives should only use trusted workstations with current antivirus software and an active firewall installed during login to the Registry Website. Full and thorough scanning of the workstation with antivirus software should be performed at least once every two weeks.

12. Operating system along with other software installed on the workstation used to log into the Registry should be updated according to the latest security updates issued by the provider of that system.

13. Links to the Registry Website sent via email or found on untrusted websites should not be used.

14. Caution should be exercised while opening attachments in electronically delivered messages. In case of messages not originating from the Registry Administrator, the credibility of their source and content should be verified. For example, when using the Microsoft Windows operating system, attachments with file extensions such as .com, .bat, .vbs, .wsh, or .exe should not be opened.

15. When accessing the secure section of the Registry Website, Authorized Representative should use a profile with "user" permissions rather than "administrator" permissions. In addition, Authorized Representative may only use Registry functionalities for which they have permissions resulting from the Terms of use and RR.

16. Automatically logging systems or tools testing the Registry should never be used. Data sent to the server running the Registry application should not be manually modified.

17. The Authorized Representative should log out from the secure section of the Registry and the EU Login system before leaving the workstation in order to prevent unauthorized access to the Registry.

18. Workstation used to log into the Registry should not be used by individuals other than Authorized Representatives, as well as resources (such as folders, printers) should not be shared on it, servers (such as HTTP(S), ftp, etc.) should not be launched, and file sharing services should not be used. Additionally, USB devices from unknown sources should not be connected to the workstation.

19. In order to generate the Code used in the user authentication process or to authorize operations in the Union Registry system, the Authorized Representative should have a mobile phone or other mobile device with the EU Login application installed (provider - European Union). In emergency situations, in case of problems with the mobile application, users will log in using a mobile phone number and Code received via SMS, so it is necessary to provide the Administrator with the current mobile phone number. During the user authentication process in the Registry, mobile device used to generate or receive Codes should not be connected to the Internet.

Glossary of terms:

Password - confidential access password used for authorization in the EU Login system.

Code - a one-time code consisting of a sequence of digits, generated by the EU Login application installed on the mobile device of the Authorized Representative or a code consisting of a sequence of alphanumeric characters, sent via SMS to the mobile phone number.

RR - Commission Delegated Regulation (EU) 2019/1122 of 12 March 2019 supplementing Directive 2003/87/EC of the European Parliament and of the Council with regard to the functioning of the Union Registry (Official Journal of the EU L 177 of 2.7.2019, p. 3, as amended).

Workstation - a computer or other device with an installed web browser.

Registry Website - means the website serving as the interface of the Union Registry application for users.