Energimyndigheten

Terms of use for account representatives in the Swedish part of the Union Registry

In order to be a representative in the Swedish part of the Union Registry, it is required that you approve and, as long as you act as a representative, comply with the terms of use. The terms of use are approved when you enter your authorization key when you log in for the first time in the Union Registry.

Unless otherwise stated, the term device refers to the computer, tablet, phone or any other device used to connect to the union registry

These common minimum security requirements are:

1. Devices used to connect to the union registry

- To connect to the Union Registry, users must use a device provided by their organisation and/or their own device (if authorised by their organisation's security policy).

2. Patches, versions

- Operating System (OS) and other software installed on the device should be updated with the latest security patches released by their software editor.
- Mobile Operating System (mobile OS) where the EU Login mobile app is installed should be updated with the latest security patches released by its software editor.
- The EU Login mobile app should always be updated to the latest version available in relevant (Google or Apple) application store.

3. Administrators[1] privileges restriction

- Administrator accounts should only be used by trusted people and only to install authorised and trusted programs (see point 7 below). In general the device should be as-well-protected-as-possible.
- To connect to the Union Registry and to the Internet, the users must use a device where they log in as a “user”, never as an “administrator”.

4. Antimalware / Antivirus policy

- It is an obligation of the user to use and update anti-virus software and firewall software regularly, as a minimum on a weekly basis.

[1] The term "administrators" in this section refers to IT system administrators and not to National Administrators in the meaning of the Registry Regulations.

- Full and in depth scanning for malicious virus/spyware check must be configured so that it is performed automatically at least every two weeks using up to date antivirus- and antimalware software.

5. System lock-down

- Computers shall have a lockscreen configured, so that, after no more than 15 minutes of inactivity the workstation shall be locked down. A policy shall also apply of not leaving a computer unattended without applying a lockscreen – this ensures that a lockscreen is always applied when a user is not at their desk.

6. Removable media control

- The users should connect to their PC only USB devices provided or authorised by their organisation.
- Computers shall be configured to deactivate the use of USB port. At least they shall monitor and log when a non-authorised USB device has been connected.

7. Application White Listing

- It is recommended that an exhaustive list of authorised software installed on users' computers be defined.
- It is recommended that administrators make sure that no other software is installed on the user's computer, by carrying out monitoring or scanning.
- It is recommended that any unauthorised software be removed.

8. Audit and Logging

- External access, computer access events should be logged and analysed frequently by the administrators. Every anomaly, even basic, should lead to an investigation.

9. Secure Internet Connection

- Any use of the Union Registry shall be done through a secure Internet connection.
- The secure connection shall include logical (firewall based) protection between the internal network where the user computer is located and Internet including an Intrusion Detection System at the Network and the Host (HIDS) level, and an antivirus capability.
- The secure Internet connection shall restrict access to Internet using whitelisting/blacklisting functionalities.

10. User education

- Users shall be trained to use the Union Registry and made aware of information security issues.
- The users shall avoid sharing the computer used to connect to the Union Registry with other people.
- Links in emails to access the Union Registry shall never be used.

- The Commission, the central administrator, the national administrator or the national administration Helpdesk will never ask the users for their password and / or any kind of software.
- The users shall avoid to open attachments to emails that do not come from a known source and, if absolutely necessary, to open it after careful consideration of their source and content, and never open any attachments with e.g. in Microsoft Windows a .com, .bat, .vbs, .wsh or .exe extension on the filename.
- If the users have any cause for suspicion regarding received emails, they shall contact the national administration Helpdesk.
- On the users' devices where Soft token mobile app is installed, they should maintain appropriate level of security and mobile device hygiene.
- The Registry helpdesk sends all emails from utslappshandel(at)energimyndigheten.se.
- If the users have any cause for suspicion, they shall immediately contact the national administration Helpdesk.
- National administration Helpdesk contact: Email: utslappshandel(at)energimyndigheten.se; Phone (Mon - Thu. 9.00 – 11.00 & 13.00 – 15.00): [+46 16 544 2300].

11. Users device configuration

- Computers shall be configured so that the "auto log-in" function is not used. After OS boot or software start, the log in password for the service should always be asked.
- Browsers shall be configured so that credentials are not stored by the browser and all temporary stored navigation information (such as history, passwords, cookies) are automatically deleted when closing the browser.
- Booting from CD/DVD and/or USB devices (by BIOS configuration) shall be avoided. Users must not be able to access BIOS set-up configurator (locked by a strong password and different from the log in password).
- Computers shall be configured so that no resources can be shared with external entities outside of the end user's organisation (e.g. using file sharing software such as BitTorrent) in the PC used to connect to the Union Registry.
- Computer shall be configured so that the user is not connecting to the Internet having "administrator" privileges but restricted rights. Users must not have the possibility to install software using the account with which they are connecting to the Internet and the Union Registry.

12. Union Registry usage

- Password for logging in to the Union Registry is strictly personal. Any action in the Union Registry performed with a given email address and password is deemed under the liability of the user of this email address and password.

- Password for logging in to the Union Registry is strictly personal. Any action in the Union Registry performed with a given username and password is deemed under the liability of the user of this username and password.
- All authorised users of the Union Registry shall ensure that the email address password, the SMS one-time login codes and the codes generated while authenticating with Soft Token do not become known to other people, including other account holders in the Union Registry. National administrators or the helpdesk may only ask users to communicate their email address by phone but neither the Commission nor national administrators will ever ask end-users to communicate their password.
- To access the Union Registry website, it is recommended to always type the website directly into the address box of the browser. For the Union Regisry, this is

  https://unionregistry.ec.europa.eu/euregistry/SE/index.xhtml. If the users do not type the address, each time they connect, they shall check that the SSL connection is set ("https" and not "http" appears in the browser's address bar) and that the SSL certificate which appears when clicking on the lock icon of the browser:

  - Is issued by "GlobalSign Extended Validation CA – SHA 256 – G2" to "*.unionregistry.ec.europa.eu",
  - Is valid until 2 October 2021 and
  - has the following fingerprint (SHA-256 algorithm value): " "7F:E5:54:B2:F2:4F:65:D0:A1:7F:54:D1:8F:43:50:AC:23:6F:47 :7F:83:85:F7:52:8A:E7:A5:16:AF:64:6F:8E”

- When leaving their computer, the users shall log out of the Union Registry so that unauthorised persons cannot gain access to their account in the Union Registry.
- The users shall take reasonable precautions to prevent the unauthorised use of the mobile devices, the numbers of which are used in Registry communication.
- The mobile device that receives the SMS one-time login codes and/or the mobile device where the Soft token mobile app is installed must not be used for transactions on the Internet at the same time.