SIKKER PÅLOGGING TIL KVOTEREGISTERET

Vedlegg til brukeravtalens avsnitt 7.

EU Kommisjonens krav til pålogging til kvoteregisteret gjelder for alle brukere, og for alle typer konti. Dokumentet er på engelsk, og det utarbeides/oppdateres av kommisjonen.

Miljødirektoratet er ikke ansvarlig for eventuelle feil om mangler i dokumentet.

Sist oppdatert **30. juni 2017**

Postadresse: Postboks 5672, Sluppen, 7485 Trondheim | **Telefon:** 03400/73 58 05 00 | **Faks:** 73 58 05 01
E-post: post@miljodir.no | **Internett:** www.miljødirektoratet.no | **Organisasjonsnummer:** 999 601 391
Besøksadresser: Brattørkaia 15, 7010 Trondheim | Grensesvingen 7, 0661 Oslo|

MILJØ-
DIREKTORATET

Common minimum security requirements to be imposed on the account holders of the Union Registry

The National Administrators must inform their account holders in the Union Registry of the minimum security requirements which they must fulfil, either by including them in their agreements with those account holders, in national Terms of Use or via another appropriate means depending on national practice.

1. Workstations

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

2. Patches

Operating System (OS) and other software installed in the machine should be updated with the latest security patches released by their software editor.

3. Administrators[1] privileges restriction

Administrator accounts should be used by trusted people, and only to install authorised and trusted programs (see point 6 below). In general, the machine should be as-well-protected-as-possible.
To connect to the Union Registry and to the Internet, the users must use a machine 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.

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.

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

5. System lock-down

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

6. Removable media control

The users must not connect any non-trusted USB device to their PC.

It is recommended that computers be configured to deactivate the use of USB port. At least they should log the event of USB device connection.

7. Application White Listing

It is strongly recommended that an exhaustive list of authorised software installed on users' computers be defined.

It is strongly recommended that administrators make sure that no others software are installed on the user's computer, by carrying out monitoring or scanning.

It is strongly recommended that any unauthorised software be removed.

8. Audit and Logging

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

9. Secure Internet Connection

Any use of the Registry must be done through a secure Internet connection.

The secure connection must 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 must restrict access to Internet using blacklisting functionalities.

10. User education

Users must be trained to use the Union Registry and have been sensibilised to information security issues.

The users must avoid sharing the computer used to connect to the Union Registry with other people.

Links in emails to access the Union Registry must 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 must only open attachments to emails that do not come from the Union Registry 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 must contact the National Administration Helpdesk.

The Registry helpdesk sends all emails from kvoteregister@miljodir.no.

If the users have any cause for suspicion, they must immediately contact the National Administration Helpdesk.

National Administration Helpdesk contact:

E-mail: kvoteregister@miljodir.no;
Phone (working hours 9-15): +47 952 04 667.

11. Users computer configuration

Computer must 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.

Browser must be configured so that credentials cannot be stored by the browser and all temporary stored navigation information (such as historic, passwords, cookies) are automatically deleted when closing the browser.

Booting from CD/DVD and/or USB devices (by BIOS configuration) must 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 must 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 must 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 username and password is deemed under the liability of the user of this username and password.

All authorised users of the Union Registry must ensure that the username, password and SMS one-time login codes 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 username by phone, but neither the Commission nor National Administrators will ever ask end-users to communicate their username and 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 Registry, this is https://ets-registry.webgate.ec.europa.eu/euregistry/XX/index.xhtml. If the users do not type the address, each time they connect, they must 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 – G3" to "ets-registry.webgate.ec.europa.eu",
- Is valid until 5 April 2019 and
- has the following fingerprint: " 1e 27 22 9b 1d a1 ef 1b fb 0d fb a0 c6 35 40 55 7b fd 01 64 "

When leaving their computer, the users must log out of the Union Registry so that unauthorised persons cannot gain access to their account in the Union Registry.

The users must 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 must not be used for transactions on the Internet at the same time.