EUROPEAN COMMISSION
DIRECTORATE-GENERAL
CLIMATE ACTION
Directorate C - Innovation for a Low Carbon, Resilient Economy
CLIMA.C.1 – Low Carbon Solutions (I): Montreal Protocol, Clean Cooling & Heating, Digital Transition

Security good practices for the users of the F-gas Portal and HFC Licensing System (V2.0 - 05/08/2022)

The F-gas Portal and HFC Licensing System (hereafter ‘the registry’) is a web-based application aiming at implementing certain measures of Regulation (EC) 517/2014 of the European Parliament and the Council on fluorinated greenhouse gases (‘the F-gas Regulation’). These measures include this registry for quotas enabling the allocation nd transfer of quotas, as well as the authorisation of quota use to enable the implementation of the phase-down of hydrofluorocarbons (HFCs) placed on the Union market. The registry also represents the entrance point for companies to fulfil their reporting obligations under Article 19 of the F-gas Regulation.

The European Commission sets requirements for measures to ensure the security of the registry. These security measures and best practices must be applied by users of the system to avoid:

- (ab)use of the system and/or modification of data by a non-registered user due to an unsecured workstation or due to Internet use or weak password policy,
- misuse of the system and/or modification of data due to lack of knowledge within the organisation on the application or on the procedures to operate the system.

Use the non-exhaustive list of additional considerations presented below. The list is to be complementary to your internal IT security measures.

Workstations (pc laptops, pc desktops, tablets)

- Logout or lock your computer when leaving your workstation to prevent unauthorised access.
- Ensure that the screen lock for users of the registry has a short timeout period so that workstations are locked automatically.
- Ensure that workstations of users of the registry are used for authorised business purposes only and do not have unauthorised software installed.

Passwords:

- **Do not share your passwords with anyone.** Passwords and usernames for logging into the registry are strictly personal. Any authorised user of the system shall ensure that the password is not disclosed to anyone else. A user's password and/or username circulating between several people is considered as a serious security breach. The Commission may in such cases restrict logging into the system for this user or block the user’s access to the system.
- Comply with the applicable password policies and procedures.
- Use strong passwords:
    - At least 10 characters, using 3 out of 4 of the following requirements uppercase, lowercase, numeric, and special characters, and when possible, use passphrases.
    - Different than the last five ones used and not contain user’s information.
- Use one password per system/database.
- Change the passwords on a regular basis (change every 3 months is advised),
- Never provide your registry credentials in an e-mail or phone call. If you are asked for your registry do not answer. Such requests are an attempt to steal access information with the purpose of hacking the system.
- Never write down your username or password. If you forget your password or username, you can reset them safely through the system EU-LOGIN.
- Suspicions that the username and/or password has been compromised, or that others wrongfully gained access to the system, must be reported to the European Commission by email to CLIMA-HFC-Registry@ec.europa.eu

- Never use simple codes such as last name, first name or business name as your username or password

Viruses:

- **Comply with the anti-virus policy** as new viruses are discovered every day.
- Use the corporate antivirus and ensure it is updated. Do not deactivate the antivirus.
- Do not open or download any files attached to an e-mail from an unknown, suspicious, or untrustworthy source.
- Any use of the system must be made using a secure Internet connection (protected by a firewall) on a computer that at any given time has updated software that prevents the computer from being exposed to harmful malwares and viruses.
- Be wary of e-mails you receive, even from the system. Only open attachments and links in e-mails of which you are sure that they are safe.

Training:

- Provide periodic training to all users on the security requirements and procedures for the use of the registry.
- Provide a dedicated training to new employees on the security requirements for the registry.

Use of application:

- Before connecting to the registry, prepare a list of actions you want to do in the application to avoid errors in operations or exceeding the session time of no action.
- When logging into the system, users should only use computers that are not used by others (i.e., no shared computers).
- **Logout from the system and close the browser window** when you leave the application.

Contact your IT department or the European Commission F-gas support at CLIMA-HFC-Registry@ec.europa.eu:

- If you encounter any suspicious behaviour of the registry,
- For more information on security requirements.
- Keep up to date on news and notices about the system on the message board of the application

Violation of security measures

Any violation of the mandatory security measures may result in rejection of account opening or exclusion from the system. Note that if such violation is discovered after the account is opened, and it turns out that the account was opened erroneously, the system Administrator may close an account immediately without any kind of warning to the account holder. Suspected document forgery, and other crimes in connection with the system, will be prosecuted.