Security requirements for access to ECHA's Interact Portal by Individual experts participating in Committees (hereinafter referred to as "Individual Experts")

1. General security requirements

a. Access to the Interact Portal is allowed only by authorised users when they comply with these security requirements.

b. The Interact Portal can be accessed only through a secure remote access solution using two-factor user authentication.

c. All factors for authentication, physical or logical (e.g. hardware tokens, PIN codes and passwords) used for authentication to the Interact Portal must be carefully protected against being lost, stolen or disclosed when used or stored. Passwords or any other authentication mechanisms related to ECHA's information systems are unique to each user and may not be shared with other people. Individual Experts will return their hardware tokens to ECHA (or to another party delivered the token to them) when they are not participating in the Committee work anymore.

d. Files which contain sensitive information and which are not downloadable for Individual Experts can be only online accessed and viewed from the Interact Portal. Any content of such files are not allowed to be copied, including also copying or printing out such data on a screen (screenshots).

e. Confidential information can only be discussed in a place where it cannot be overheard by any unauthorised parties.

f. Confidential information can only be accessed in a place where it cannot be seen by unauthorised parties. Access to the Interact Portal from public places is not permitted under any circumstances.

g. Individual Experts must sign a specific non-disclosure agreement and a commitment before being granted access to the Interact Portal giving a commitment that the non-public information from the Interact Portal is not disclosed to any unauthorised party and the security requirements are followed.

h. All suspected or occurred security incidents must be reported to ECHA without delay. Security incidents include among others: misuse of credentials by another person, loss or theft of an authentication token or another related equipment, unauthorised access or infection on workstation used for access to the Interact Portal.

i. Individual Experts shall participate in mandatory security trainings and awareness briefings organised by ECHA.

j. In case of non-compliance with the security requirements, the individual expert's access to the Interact Portal may be limited or completely blocked, pending the implementation of additional security measures or resolution of the non-compliance.

2. Security requirements for the Individual Experts' IT-systems

Scope: workstations (or any other client devices, such as a tablet) used to access the Interact Portal by Individual Experts

a. The risk of malware infection must be mitigated at least with the following controls:

   i. Malware prevention software (antivirus, antimalware) must be running on all such systems that are generally vulnerable to malware infections. Antivirus signatures must be regularly and frequently updated, and antivirus has to be monitored.

   ii. In the case of having access to emails from the workstations in scope, malicious emails must be filtered out (antivirus and anti-spamming).

   iii. Users must be careful when joining mass memories (external hard drives, USB stick etc.) to their workstations; only trusted mass memories with reasonable business reasons should be joint.

b. Security vulnerabilities must be remediated by installing security updates regularly on client systems. It is highly recommended to use auto-updated features if the client device is not covered by organisation's centralised patch management system (e.g. a private computer is used for access to the Interact Portal).

c. Normal use of Individual Expert's workstation shall happen with standard user privileges. Local administrator or other administrator level privileges should be used only when necessary.

d. Accountability of who is using and accessing the Individual Experts systems must be ensured by using personal user accounts. Individual Expert's account to his/her workstation (or any other client devices) is never allowed to be shared with other users.

e. Client devices must be adequately protected against unauthorised access during the users' absence, even when this is for a short time only. Therefore at least the following security measures shall be implemented:

   i. Secure user authentication based on passwords or a stronger authentication mechanism. If the authentication mechanism is based on passwords, the password policy must be implemented and such that it covers a mandatory frequency of password changes, a minimum length and satisfies standard password complexity requirements.

   ii. Devices automatically lock the screen after a short period of inactivity. Devices are also manually locked whenever the user leaves the computer, particularly when doing telework.

f. Any build-in data storage (e.g. HDD, SSD) of client devices for teleworking, as well as other portable devices, must be adequately encrypted, regardless of the fact that offline copies of confidential information are not allowed.

g. A client firewall (personal firewall) must be enabled with reasonably restrictive (especially inbound) rules.
Note: the client firewall can be configured to be disabled only when the device is

directly connected to an internal office network that is adequately protected, i.e. when access from Internet to that internal network is adequately controlled.

3. Identity and access management

Scope: access rights related to the Interact Portal.

ECHA, or other organisation in case the access management has been delegated, shall coordinate the following identity and access right management tasks:

a. granting access rights to ECHA's information systems only to authorised individuals based on business need-to-know.

b. making the authorised individuals sign a non-disclosure agreement before granting them access and keeping file of the agreements.

c. checking the validity of non-disclosure agreements and verifying the individual's identity before granting the access.

d. recording the list of all users and their access rights, including users' contact details and role.

e. immediately revoking all access to ECHA's information systems who do not have any more business reason for access.

f. once a year, at a minimum, reviewing the list of all active users and their access rights and documenting these access right reviews.