ECHA Indicative teleworking rules and requirements for IT hosting contractor

The requirements are applicable when IT Contractors staff member does teleworking outside of delivery centre (their standard office), and have access to ECHA's IT-systems, ECHA's network environment or Contractor's IT management system or environment used to provide IT service for ECHA.

Approval for teleworking is conditional based on existing justifications and benefits. Compliance with the requirements does not automatically mean that ECHA accept the request for teleworking but based on comparing the risk to the benefits.

Additional teleworking requirements shall be applied on top of all other security requirements with the following exceptions due to nature of the teleworking: user is not working in the standard physically access controlled office environment and the client device is not connected to protected office network. To compensate missing security measures due to the above-mentioned exceptions, there are the following additional teleworking requirements:

a. Teleworking and remote access related risk shall be assessed, and teleworking policy and rules must be in place:

   i. A documented risk analysis has taken place to identify and assess risks related to the teleworking. Teleworking can be allowed only when the risk level is acceptable in comparison to the business benefits.

   ii. A teleworking policy, that defines the purpose, procedures, conditions and responsibilities for teleworking, shall be in place. The implemented teleworking policy should be in line with indicative teleworking requirements as well as other relevant ECHA security requirements and take into account the results of the risk assessment.

   iii. Teleworking is allowed only if the person is working in a place where information in the screen cannot be seen by unauthorised parties. Teleworking from public places is not permitted under any circumstances.

b. Teleworking-related security procedures

   i. The security awareness process in place shall ensure that the security considerations relevant for teleworking are understood.

   ii. The incident reporting and response process in place must also cover teleworking e.g. to limit the potential impact of loss or theft of equipment.

c. IT security requirements for teleworking access solution and the devices used for teleworking:

   i. The traffic between the client device and the contractor's network shall be adequately protected by encryption, i.e. a secure VPN connection must be established.

ii. Only authorised telework users using authorised devices can establish a secure connection. Therefore, both users and the devices used for teleworking must be reliably authenticated[1] (as with two-factor user authentication and secure device authentication).

iii. Any build-in data storage (e.g. HDD, SSD) of client devices for teleworking shall be adequately encrypted.

iv. A client firewall must be enabled with reasonably restrictive (especially inbound) rules. When a VPN connection is established, the applications (if any) that are allowed to initiate outbound connections must be controlled.

[1] For example, using pre-installed certificates