Annex II

Examples of IT Contractors' access belong to the different access categories

Below are listed some examples of IT Contractor's access belong to the different access categories defined in the policy.

<u>Basic Level</u>

- Standard user access to ECHA's development or testing systems where no confidential business information is stored or processed. The systems do not have interfaces or other direct access to confidential business information.
- Read-only browser based access to a monitoring systems or machine data analytics systems.

Note: Full, layer 3 VPN connectivity to ECHA environment cannot belong to this level. Whenever ECHA's network is extended to IT Contractor's network, IT Contractor's access is at least *Increased Level*.

<u>Increased Level</u>

- Access with *system administration privileges to ECHA's development or testing systems*, where restricted or highly restricted information is not stored or processed. The systems do not have interfaces or other direct access to confidential business information.
- Normal user level access up-to internal information. For example access to ECHA's Intranet, limited access to the tickets in Remedy assigned to IT Contractor, or access to the documents stored in ECHA's systems relevant for the services provided by IT Contractor
- Full VPN connectivity to such ECHA development or testing environment, where restricted or highly restricted information is not stored or processed.

<u>High Level</u>

- Access with system administration privileges to ECHA's production systems where (a significant amount of) restricted or highly restricted information is not intended to be stored:
  - System administrator access to network devices
  - Privileged access to email system
  - System administrator access to ECHA website or eChemPortal
- IT Contractor has a normal user access to restricted or highly restricted information. For example IT Contractor has controlled access with end user privileges to the REACH, Biocides or other similar restricted data through the applications, i.e. similar access as Member States Competent Authorities have to ECHA's IT systems belong to scope of the Security Declaration and Standard Security Requirements.
  IPSec VPN access to ECHA's production environment for monitoring systems or applications (without direct access to data)