Access to ECHA Information

1. Purpose

This procedure describes how the security principles for ECHA information are balanced with the Agency's transparency and collaboration duties in the light of ECHA's dual task to keep third party data received by it secure on the one hand and to work with such data to protect human health and the environment in collaboration with its institutional partners (and their contractors) on the other hand.

It is to be noted that the question on access to ECHA information is separate from the question on ownership of that information. More in particular, ECHA may make certain information public (e.g. via the dissemination portal), while some restrictions to the re-use of that information continue to apply due to intellectual property rights of the data owner.

2. Scope

This procedure applies to all information held by the Agency, regardless whether it is the legal owner of such information or not.

Out of scope:

Requests for information: External questions and requests for (access to) information shall be replied to by the ECHA Helpdesk, the ECHA Information Desk or the recipient directly in accordance with the ECHA Code of Good Administrative Behaviour (*MB/11/2008 amended by MB/21/2013*). Replies shall normally not include non-public information (but if they exceptionally do, such information shall be exchanged securely via S-CIRCABC and only after the necessary authorisation is obtained in line with Annex 1 of this Procedure).

Access to document (ATD): Any request which falls within the scope of Regulation (EC) No 1049/2001 on public access to documents shall be dealt with in line with the instructions foreseen in *WIN-0011 Processing of initial applications for access to documents*.

Access to own file: Any request for access to one's own file (i.e. requests for access to any document held by ECHA in a process leading to the adoption of a decision or a formal opinion that concerns the requester directly) shall be handled in accordance with *ED/44/2015 Access to one's own file*.

Access for EU bodies with investigative powers: in accordance with Article 98 of REACH and *MB/30/2009 final*, OLAF shall be given full access to ECHA information at request in case of an investigation. Additionally also the Internal Audit Service of the Commission (IAS), the European Court of Auditors (ECA) and the European Data Protection Supervisor (EDPS) shall have full access to all ECHA information at request in accordance with the Framework Financial Regulation, the ECHA Financial Regulation and Regulation (EC) No 45/2001 on the protection of personal data. In case they use contractors for carrying out their tasks, they shall be bound by the confidentiality clauses foreseen in the contract and at ECHA's request they may be asked to sign a non-disclosure agreement.

3. Description

3.1. Security classification

ECHA does not process EU classified information, as defined in Commission decision (EU) 2015/444. However, all information in ECHA belongs to one of the following categories, which constitute information security confidentiality classification levels:

- Public
- Internal (for external audience ‹empty›)
- Restricted (for external audience marked "Confidential")
- Highly Restricted (for external audience marked "Confidential")

The Process Owner or delegate can classify information as Restricted or Highly Restricted only if the extra effort (administrative overhead and management of access rights) is justified. For example data referred to under Article 118(2) or 119(2) of the REACH Regulation or Article 66(2), 67(3) or 7(4) of Biocidal Products Regulation, although generally considered to constitute confidential business information, may not be necessarily classified as Restricted or Highly Restricted if most of ECHA staff have a business need to know reason for access and restricting it from the rest of ECHA staff would lead to disproportionate costs in resources needed to set up the access rights and manage them.

The rules applicable to different security levels are defined in Annex 1. All documents which have no security marking have to be considered Internal. Process Owners can set up additional security rules for their information.

Any exception to the security principles described in this document is to be duly motivated and explicitly authorised by the Executive Director, unless delegated.

3.2. Internal access to ECHA information

Information held by ECHA is accessible to ECHA staff and other authorised persons unless the Process Owner decides that the information needs protection and should be accessible by a restricted number of persons on a need-to know basis.

The access rights are provided based on the four-eye principle, meaning that there is always a person establishing the access rights of a person, different from the one physically entering the information in the system. Access rights are withdrawn when an individual leaves the service.

A centralised identity and access management system is used for managing the access rights.

ECHA staff, including for this purpose all statutory staff, seconded national experts and trainees, shall have access to restricted and highly restricted ECHA information, on a strictly business need-to-know basis, as confirmed by the Process Owner. The same shall apply to

interim staff, on site consultants and other external parties visiting or working at the ECHA premises ad hoc (e.g. visiting researcher, Commission staff or contractor).

All staff members sign a declaration of commitment and confidentiality when entering the service of the Agency (*ED/184/2012*), while interims, on site consultants and other visiting external parties shall sign a confidentiality and security declaration (see annex 1 to *ED/53/2014*).

When access is required to IT systems that are non-standard for the user group to which the user belongs, such access shall be authorised by the respective line manager.

3.3. External access to ECHA information

ECHA collaborates on a daily basis with a number of external partners in its core operational processes, which also involves the need to share information. When this involves the sharing of restricted or highly restricted information, there are specific procedures in place for granting such access, depending on the entity concerned, the type of request and the circumstances of the case.

3.3.1. Regular access for Member States and the Commission

In order for the Member States Competent Authorities (MSCAs) and Enforcement Authorities and the Commission to be able to carry out their duties under the REACH, CLP, PIC and Biocides Regulations, authorised staff members of such authorities can request access to certain ECHA databases via a secure connection. Access rights are managed by MSCA User Administrators from the Competent Authorities (or Mandated National Institutions), the official list of which is managed in COMA.

In line with *Management Board Decision 15/2019* each MSCA (and the relevant Commission services) shall apply Standard Security Requirements and sign a Declaration of Commitment before receiving access to the following ECHA IT systems:

- The ECHA REACH-IT system
- The ECHA IUCLID Member State database (REACH/CLP)
- The Portal Dashboard which facilitates point of access to ECHA's IT systems
- The Register for Biocidal Products (R4BP)
- The ECHA IUCLID Member State database (Biocides)
- The Interact Portal, Platform for Authorities
- The Poison Centre Notification Portal (PCNP)

The National Enforcement Authorities (NEAs) receive access to a version of Portal Dashboard specifically designed for them, following Security Recommendations and a related Declaration of Commitment:

- The Portal Dashboard – National Enforcement Authorities

The Designated National Authorities (DNAs) under the PIC Regulation follow the specific Terms and Conditions prepared for:

- The PIC Information System

3.3.2. Regular access for members of ECHA bodies, networks and expert groups

In order for the members (including also advisers, invited experts, alternate members and observers) of the ECHA bodies, networks and expert groups[1] to be able to carry out their work, access can be given to restricted and highly restricted information based on a decision of the responsible Process Owner, via Secure CIRCABC and in accordance with *ED/46/2015 on the Use of S-CIRCABC for Handling ECHA Information* (including the necessity to sign a declaration of commitment by each user before access to data is granted).

Additionally it is foreseen in the respective rules of procedure that all members (including also advisers, invited experts, alternate members and observers) of the ECHA Committees and Forum sign a declaration of confidentiality before access to data is granted.

3.3.3. Regular access for IT contractors

When remote access to ECHA's IT systems containing restricted or highly restricted information is required in the context of providing off-site outsourced IT services to ECHA, such remote access shall be handled in accordance with *POL-0016 IT Contractor's Remote Access*.

3.3.4. Ad hoc access for contractors and other external parties

Ad hoc requests for **public** and **internal** data are authorised by the responsible Process Owner, taking into account workload and IPR related concerns.

Ad hoc and project-based requests for external access to **restricted** and **highly restricted** information (e.g. for researchers, Commission or Member State staff and their contractors or ECHA contractors) require the authorisation of the Executive Director and shall be dealt with on a case-by-case basis, and a decision shall be taken based on the merits of each case. The decision of the Executive Director shall be preceded by a review by the Process Owner, responsible for the ECHA information in question and the Information Security Manager (E.1). The authorisation of the ED shall be obtained before any contract involving the sharing of non-public information is signed by ECHA. For scientific data requests, the priorities and responsibilities defined in *PRO-0066 Scientific data requests* shall apply.

The ED decision shall include the standard security requirements based on the text of Annex II of this procedure. The access shall only be given after written agreement to the security requirements of the ED decision.

The external distribution of such restricted or highly restricted information shall only take place via secure channels, such as encrypted email, encrypted USB stick, courier service or registered mail or a secure collaboration platform such as S-CIRCABC.

[1] The ECHA bodies include the Management Board, Board of Appeal, Enforcement Forum and Committees and their working groups. An overview of the ECHA networks and expert groups can be found in the annex to ED/39/2014.

4. Flowchart

N/A

5. Definitions

Term or abbreviation	Definition
ATD	Access to documents
COMA	ECHA Contact Management tool
DNA	Designated National Authority
ECA	European Court of Auditors
EDPS	European Data Protection Supervisor
IAS	Internal Audit Service of the Commission
MSCA	Member State Competent Authority
NEA	National Enforcement Authority
OLAF	European Anti-Fraud Office
S-CIRCABC	External Collaboration Platform

6. Records

N/A

7. References

Associated document code	Document name
(EC) No 1725/2018	General Data Protection Regulation
(EC) No 1049/2001	Access to Documents Regulation
MB/30/2009 final	Decision concerning terms and conditions of internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Communities' interests
MB/11/2008 amended by MB/21/2013	ECHA Code of Good Administrative Behaviour
Management Board Decision 15/2019	Revised Decision of the Management Board on the adoption and scope of application of unified declarations of commitment by a Member State Competent Authority/Mandated National Institution/Designated National Authority of a Member State and the European Commission with respect to security aspects for ECHA's information systems
2015/444	Commission Decision (EU, Euratom) on the security rules for protecting EU classified information
ED/184/2012	Declarations of commitment and confidentiality
ED/39/2014	Guidance for the prevention of potential conflicts of interest in ECHA networks and expert groups
ED/53/2014	Rules for access to the ECHA premises
ED/46/2015	Use of S-CIRCABC for Handling ECHA Information
ED/44/2015	Access to one's own file

8. Annexes

ANNEX I – Security rules for ECHA information

ANNEX II - Standard Security Requirements for Access to Information by Selected Contractors

Annex I: Security rules for ECHA information

	Security levels			
Internal marking	**Public**	**Internal**	**Restricted**	**Highly Restricted**
External marking		**‹empty›**	**Confidential**	
Type of information	Information (that can be) published or disseminated on ECHA website or information otherwise legally publicly available.	Information that is not public, but meant for the use of ECHA and its bodies, working groups and networks.	Only information where the unauthorised disclosure could be disadvantageous to the essential interests of ECHA, its staff or those who have provided the information to ECHA.	Only information where the unauthorised disclosure would seriously harm the essential interests of ECHA, its staff or those who have provided the information to ECHA.
Legal base	By default, all ECHA information shall be public, unless an exception from the ATD Reg. applies. If the information is made public proactively, it shall be marked "public".	Information which belongs to one exceptions of the ATD Regulation, e.g.: • Information of commercial interest; • Personal information; • Information related to court proceedings, legal advice, inspections, investigations or audits; • Information contained in documents for internal use if disclosure would seriously undermine the decision-making process. The classification will depend on the degree of sensitivity of the information concerned.		
Examples	• Minutes of Management Board meeting • Declaration of interest of Committee member • Candidate List • Final BoA decision	• Draft and final evaluation decision • CLH accordance check decision • DCM document • Staff contact details • Training applications	• Registration dossier and decisions • BoA procedural documents • IAC audit reports • Declaration of interest of ECHA staff • Salary related document • Tender file and evaluation report	• Datasharing dispute decision • Notification of intention to submit an AfA • Notifications received from downstream users • Personal and medical file, • Appraisal document • Job application and CV
Access inside ECHA	No restrictions.	Any staff, including seconded national experts, interims, trainees and consultants working on ECHA premises.	The Process Owner or delegate decides the initial list of staff/roles that can access the information, but they may internally distribute the information further based on business need-to-know.	The Process Owner or delegate always decides the list of staff/roles that can access the information based on business need-to-know.
External access	No restrictions.	Any ECHA Head of Unit or Director can authorise access to non-ECHA staff based on business need-to-know.	Only the Executive Director may authorise access to non-ECHA staff. The Executive Director can delegate the authorisation.	
Distribution inside ECHA	No restrictions.		Put in a sealed envelope, deliver by hand or send by e-mail with indication "Restricted" in the title and if possible also use "confidential" flag.	Put in a sealed envelope, deliver by hand or send by e-mail with indication "Highly Restricted" in the title and if possible also use "confidential" flag.

External distribution	No restrictions.	Put in a sealed envelope or send as normal e-mail.	If on paper send by courier service or registered mail in a sealed envelope. If in electronic form put on an encrypted USB memory stick and send it by post. Only after the recipient has acknowledgement the receipt of the encrypted USB memory stick give the password e.g. over the phone. Alternatively upload on a collaboration platform with strong authentication or send as an encrypted e-mail attachment.
Paper storage	No restrictions.		Store in a locked cupboard or room. Do not leave unattended if not stored in a locked cupboard or room. If printed on a shared printer use secure printing.
Electronic storage	No restrictions.		Store only to repositories with access control restrictions. Also encrypt *at rest* if stored in non-ECHA systems.
Paper disposal	No restrictions.	Put in a locked confidential waste disposal container or alternatively shred it.	
Electronic disposal	No restrictions.	Delete the file.	
Disposal of electronic media	No restrictions.	Reformat or physically destroy (CDs/DVDs or optical media).	Securely wipe, degauss (broken hard disks or other magnetic media) or physically destroy (CDs/DVDs or optical media).

ANNEX II - Standard Security Requirements for Access to Information by Selected Contractors

The security requirements set out in the following refer to the handling of information provided by ECHA under Specific Contract No. ECHA/XXXX/XX (XXXX) under the Framework Contract No. ECHA/XXXX/XX.

"Information" refers to all non-public information provided to the Contractor by ECHA.

1) The Contractor solemnly declares that it:

a) acknowledges that the right to access to the Information is solely granted for facilitating the tasks that the Contractor has received from ECHA and it will make no use and destroy all Information after the task has been concluded or the contract with ECHA has been expired or terminated;
b) expresses its willingness to cooperate with ECHA in sharing of information on security measures and in the occasion of a potential on the spot verification by ECHA of their implementation; and
c) shall treat all material encountered during the duration of the contract(s) in question in line with the confidentiality rules applying to all contracts between ECHA and Contractors;
d) will take all practical steps to keep the material confidential and shall restrict access to the material to the members of the Contractor's team directly involved in the project only.

2) The Contractor has taken physical security measures for the building or the rooms in which the Information is processed or stored in order to guarantee that physical access to computer, network and end user facilities with access to the Information provided is restricted to authorised persons. These measures include restricted access to the Contractor's premises using physical locks or other forms of access control (e.g. reception) to ensure that unauthorised persons cannot enter without supervision into areas where the Information is processed or stored.

3) The Contractor has implemented at least the following restrictions for the handling of the Information provided:

a) The Information and any respective communication is destroyed using a secure disposal solution e.g. Microsoft SDelete, after ECHA approved the final report or when no longer needed or when the contract expires or is terminated. Confirmation of the destruction is provided to ECHA within 5 working days after ECHA's approval of the final report and contains:
    i. The names of the files provided by ECHA and the dates on which they were delivered to the Contractor;
    ii. The IP or MAC addresses or any identified codes of the machines and database names on which the data has been stored or processed;
    iii. Names of the persons who had access to the files;
    iv. A certificate that the Information and any respective communication has been destroyed securely and the date and method of the secure deletion;
b) There is no Information stored de-centrally in workstations or local servers and no local databases created;
c) The Information can be accessed only by the authorised persons in the Contractor's physically secured and access restricted networks and rooms;
d) Access is granted only on a strict business need-to-know basis and clearly documented;

e) Printouts are removed immediately if printed on a shared printer, copy machine or fax machine;
f) There is a 'clean desk' policy, that is clear instructions in order to guarantee that information is stored in locked cabinets, and that no print-outs are left unprotected or unattended
g) The Information cannot be exported in electronic or paper format outside of the physically secured and access restricted networks and rooms except when exchanging information with ECHA, where the transmission of data is encrypted over public networks (i.e. Internet) using SSL encryption;
h) Data storage devices and media are wiped or destroyed if they are not needed anymore, and hard disks are wiped, 'degaussed' or physically destroyed in case of hard disk failure. Paper documents and printouts will be shredded or otherwise securely disposed when no longer needed; and
i) There are clear instructions in order to ensure that the Information is not discussed in public places or in (mobile) telephone calls.

4) The Contractor has taken at least the following ICT security measures for the system which allows the processing of the Information provided:

a) There is no possibility of remote access to the Information i.e. access is only allowed within the Contractor's premises;
b) There is network protection with firewalls, anti-virus and e-mail and web proxies for workstations connected to the Local Area Network;
c) No unprotected wireless networks are used;
d) Workstation logon use individual user accounts and no shared accounts are allowed;
e) The password security is restrictive, with a clear definition of the frequency of mandatory password changes, minimum length of passwords and password complexity requirements (password change frequency is a maximum of 90 days and passwords are at least 8 characters long and must contain numbers, lower case and capital letters (and special characters, or three out of the four categories);
f) A 'clear screen' policy is established, with locking workstation whenever leaving the desk, and automatic screen saver with password protection after a period of inactivity (maximum 15 minutes); and
g) A logging and monitoring policy is established, including logging and analysis of security events, availability and capacity monitoring, an intrusion detection/prevention system, and detection of unusual activity.

5) The Contractor certifies that the users handling the Information provided are required to sign a specific non-disclosure undertaking indicating that:

a) They guarantee that the Information is not disclosed to unauthorised persons, unless already publicly available;
b) The information systems placed at their disposal are not accessible during their absence, even when this is for a short time only;
c) They promise not to reveal their password or any other authentication mechanism, or share them with other persons;
d) They will try to access only the Information for which they have been granted explicit authorisation;
e) They will use the information systems placed at their disposal or under their control only in the way in which they are intended to be used;
f) They will not try to test any weaknesses in the systems and not try to circumvent the security measures put in place; and

6) The Contractor accepts that:

a) In case of a change in security measures, a security breach or an issue that could affect ECHA, the Contractor undertakes to report this to ECHA within 1 working day of noticing it.
b) ECHA can undertake an audit of the Contractor's security measures for the access to the Information. The audit will be carried out by ECHA or by an external contractor under an ECHA contract. These audits will be properly announced by ECHA to the Contractor in advance. ECHA will bear the costs of such audits;
c) Any deviation from these Standard Security Requirements is authorised only if it provides an equivalent level of security and is recognised by ECHA;
d) These Standard Security Requirements will be regularly reviewed by ECHA to reflect the changes in the threats, ICT environment and usage of the ICT systems; these reviews may lead to a new rule or condition or amendments thereof if agreed in writing by the parties; and
e) As a consequence of the assessment of an emergency situation, a new rule or condition or amendments thereof for the access to the Information may also become applicable if agreed in writing by the parties.

7) The Contractor may release the Information to its sub-contractor(s) provided that the sub-contractor(s) have agreed in writing to all the principles set out in these 'Standard Security Requirements for Access to Information by Selected Contractors of ECHA'.

Place	
Date	
Signature	