

Annex 2: Standard handling instructions for **SENSITIVE NON-CLASSIFIED (SNC)** information at Cedefop

CREATION

- Documents containing sensitive non classified (SNC) information must be **marked** using the security marking “**SENSITIVE (SNC)**”.
- SNC information filenames must not contain any SNC specific data.
- The use of watermarks or headers such as ‘**CONFIDENTIAL**’ or ‘**RESTRICTED**’ or any other indication of confidentiality **is prohibited**.
- Documents containing SNC information must **only be accessible to recipients with a need-to-know** for official purposes (principle of professional secrecy, art.17 Staff Regulations).
- All persons handling SNC information must be made aware of the **handling instructions** by **including a copy or a link to them** within the SNC information they refer to.
- The owners of SNC information may use **distribution markings** to further restrict the **access to a specific audience**, excluding those users (regular users and administrators) with permissions granted at the location/s where the extra SNC document is/ will be stored.

HANDLING

(i.e. access, reading, editing, copying, scanning, printing, storing)

- The **holder** of any SNC information is **responsible for protecting** it, inside and/or outside Cedefop.
- The **access** to SNC information handled or stored on Cedefop equipment is **forbidden to unauthorised** persons.
- Documents containing SNC information must only be **handled and stored** on equipment or applications that are appropriately **secured** corporate devices.
- SNC information must be **protected from eavesdropping and observation** during teleworking and missions outside the office and must not be handled or stored in public.
- SNC documents must **not be left unattended** and must be **secured when not in use** (screens locked and physical documents stored in a locked office or a locked cupboard).
- **Handling of physical copies** of SNC documents outside the office is in principle **avoided**, unless necessary due to the particularities of an activity.
- **When technically feasible**, SNC electronic documents must be stored **in encrypted formats or systems**.
- **Printing, copying and scanning** of SNC documents must be **performed securely** using appropriately secured devices and the resulting **copies restricted to the minimum**. SNC documents must be removed from printers, etc. immediately and scanned copies removed from any insufficiently secured locations as soon as possible.

DISTRIBUTION

- SNC information may **only be distributed on a need-to-know basis** with these handling instructions included.
Recipients must be **aware of the handling instructions** attached.

- As a rule, SNC information must **not be distributed outside of the authorised audience**.
- **Any sharing** of SNC information **outside of the authorised audience** requires the **authorisation from the line manager and the appropriate measures in place from DMO/ICT**.
- Any person receiving SNC information who is **not the intended recipient must inform the sender and destroy the information** by appropriate secure procedures.
- Where SNC information is **transmitted physically**, e.g. via courier services, they must be **sealed inside an opaque envelope**.
- Where SNC information is **transmitted electronically**, they must be protected through **appropriate security measures**.
- When **sharing SNC information internally within an authorised Cedefop staff**, it is recommended to share a **link to the SNC document rather than attaching** the SNC document in the body of the e-mail or chat.
- When **sharing SNC information internally outside of the authorised Cedefop staff**, the sender must **request the recipient's inclusion** in the authorised Cedefop staff either through permission settings or distribution marking, as appropriate. Under no circumstances must the sender remove the SNC classification to facilitate sharing. **Any unauthorised disclosure** resulting from the sender's removal of the SNC marking is the **sole responsibility of the sender**
- When **sharing SNC information externally out of Cedefop authorised staff**, the sender must either request the inclusion of the external recipient within a distribution marking via DMO or ICT; or create a separate copy of the original document and **remove the label "SENSITIVE (SNC)"** from the copy prior to sharing. However, the general **"SENSITIVE" marking must be retained**, along with the link to the relevant handling instructions.
- When sharing information with a distribution marking on it as an attachment, the SNC information must be encrypted, **kept secure** and available only **to the members of the designated distribution marking**.

DOWNGRADING

- **Only the originator may downgrade** a document.
- When a SNC information no longer needs to be marked, **the security marking and the handling instructions must be removed**.

DESTRUCTION

- The destruction of SNC documents must be done in such a way that they **cannot be easily reconstructed**.
- **Paper copies must be shredded, and electronic copies must be securely overwritten, physically destroyed or otherwise rendered irrecoverable**.