Handling instructions for Commission documents marked SENSITIVE

These instructions apply to all documents or information that are marked as SENSITIVE[1]. The following are the minimum required protection measures.

Creation (Commission only[2])

- Ensure that the document or information is marked using the security marking "SENSITIVE" and, where relevant, one or more distribution marking(s) as appropriate.
- The choice of distribution marking(s) should be based on the subject matter and level of damage that may be caused by unauthorised disclosure.
- Ensure that the document or information includes a copy of or a link to these handling instructions.
- Do not use any other markings than those laid down in *Security notice C(2019)1904*.

Handling (i.e. printing, copying, scanning, storing, reading and editing documents)

- Where possible, store SENSITIVE electronic documents in encrypted file shares or systems. Ensure that the markings and related access restrictions are applied.
- Documents should only be handled on appropriately secured corporate (i.e. non-personal) devices (end user devices, printers etc.).
- Documents should not be read or edited in public places where there is a risk of being overlooked.
- Documents should be secured when not in use (screens locked or physical documents locked away).
- Documents should be removed from shared output devices immediately, including printers and shared scanning folders.

Distribution (i.e. defining authorised recipients and determining methods of transmitting information)

- Information may only be distributed on a need-to-know basis in line with any distribution markings and bearing in mind the principle of professional secrecy under any relevant legislation (Staff Regulations or national legislation). SENSITIVE information must not be distributed outside of the audience indicated.
- Do not release SENSITIVE documents outside the relevant services of your organisation without authorisation from the originator.
- Any person receiving SENSITIVE information who is not the intended recipient must inform the sender and destroy the information by appropriate secure procedures.
- Where the information is transmitted physically, e.g. via internal mail or courier services, it must be sealed inside an opaque envelope.

[1] I.e information categorized as sensitive non-classified (SNC), as defined by Commission Decision (EU, Euratom) 2015/443, Article 9(5), and further elaborated in *Security notice C(2019)1904 on markings and handling instructions for sensitive non-classified information*

[2] Only Commission information can be considered as SNC, and so the instructions relating to creation and downgrading only apply within the Commission.

- Where information is transmitted electronically, it must be encrypted.

Downgrading (Commission only)

- Only the originator may downgrade a document.
- When a document no longer needs to be marked, the marking should be removed from the document and the handling instructions should also be removed.

Destruction

- Paper documents must be shredded using a cross-cut shredder, and shredded documents may be disposed of in the normal office waste.
- Documents stored on electronic media must be securely deleted so that the document cannot be easily recovered (e.g. by overwriting file contents). If the media cannot be overwritten or will not be reused, they must be securely destroyed.