Handling instructions for CJIs-related documents marked SENSITIVE

These instructions apply to all ELA CJI-related documents or information marked as SENSITIVE, when shared with external stakeholders involved in CJIs or in CJI-related activities.

Creation (applicable to ELA staff only)

- Documents containing sensitive non-classified information must be marked using the standard security marking "SENSITIVE". Do not use any other markings than the security marking SENSITIVE.
- Documents containing sensitive non-classified information must only be accessible to recipients with a need-to-know for official purposes, bearing in mind the principle of professional secrecy and the obligations under the Staff Regulations (Article 17).
- All persons handling sensitive non-classified information must be made aware of the handling instructions. Ensure that sensitive documents or information include a copy of or a link to these handling instructions.

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

- This document is SENSITIVE and should only be handled and stored on appropriately secured corporate (i.e. non-personal) devices (such as: corporate end user devices and secure printers).
- This document should not be read or edited in public places where there is a risk of being overlooked.
- This document should not be left unattended and should 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 this document outside the office should in principle be avoided, unless necessary due to the particularities of an activity, e.g. during an inspection.
- This document should be stored in a way that prevents automatic sharing with people that do not have a need-to-know (electronic documents secured in encrypted file shares or systems).
- Printing, copying and scanning of this document must be performed on appropriately secured devices. This document should be removed from printers, photocopiers, faxes, shared scanning folders or other shared devices immediately, while its scanned copies, including both electronic and hard copies, shall be removed from any insufficiently secured locations as soon as possible, including shared drives, unencrypted e-mails, scanner device memory and printers in unsecured office areas.

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

- This document is SENSITIVE and can be disseminated only on a need-to-know basis for official purposes, exclusively to other persons/authorities/stakeholders involved in the inspection (including preparatory stages) or in charge of inspection-related activities in their respective country;
- A copy of the present handling instructions must always be included in the document when shared with other parties.
- Any further transmission must comply with the national law of your respective country. ELA is not responsible for the further use of this document or information by the competent national authorities.

- This document or the information in it must not be used as evidence in judicial proceedings.
- Where this document is transmitted physically, e.g. via internal mail or courier services, it should be sealed inside an opaque envelope. Where it is transmitted electronically, it should be protected through appropriate security measures, including encryption in transit using appropriate cryptographic mechanisms.
- Any person receiving SENSITIVE information who is not the intended recipient must inform the sender without undue delay and destroy the information by appropriate secure procedures.

Downgrading (applicable to ELA staff 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

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