

Document Marking

A 90-minute discussion for any size organization on when a document needs a mark

Habits

- Start from your document marking policy. Three labels are enough: Public, Internal / Confidential, and Restricted.
- Treat an unmarked file as Internal / Confidential. If it holds personal data or credentials, treat it as Restricted.
- Mark information when it leaves the organization: email, print, download, or a handoff.
- Encrypt email that carries personal data, and set the sensitivity so the next person can see it.
- Keep the file in a folder whose permissions match the label. Label the folder at the highest level inside it.
- Add a labelling product later if you want one. The mark does not wait for the product.

Red flags

- A file leaves with no mark
- Personal data in an email that is not encrypted
- A printed pack with no header or footer
- A folder anyone can open that holds Restricted files
- Two labels on the same file, and no person named to decide
- A labelling product on order, and no mark in the meantime

First hour

1. **Stop.** Do not forward the pack again until it carries a mark.
2. **Mark.** Put the label on the file, the email, and any printed copy.
3. **Move.** Put the file in a folder whose permissions match the label.
4. **Tell.** Tell the person who owns the information, and the people who already received it.

Marks follow ISO/IEC 27001:2022 Annex A: A.5.12 Classification of information and A.5.13 Labelling of information.