

Labeling Data and Information

The actual labeling method will vary depending on the media type in which the data and information are stored.

The sample labeling methods are only intended to outline possible solutions; as such, **they are not prescriptive** and do not elaborate on the particulars (i.e., the complete context in which the data and information exists) or the manner in which security classification is applied (i.e., to a system and application, record, or specific field).

Sample Labeling Methods

Type	Method
Hard copy documents	Rubber ink stamps for each level may be needed to mark hardcopy documents received from outside the organization.
Email	Identify security classification in subject line of email, if classified as Protected A, B, or C.
Electronic documents	Identify security classification in document metadata. If the electronic document is to be printed or viewed in .pdf format, the security classification should appear on every page, including the cover page—this can be done by including the security classification in the header/footer, or by use of a watermark. Date of creation and information about the department that created the document should be included.
Data, databases and business applications	Identify security classification in system/application metadata. Labels may be required for online screen displays and reports generated by a system.
Other media	The security classification may be identified on labels applied to media (e.g., CDs, DVDs, USB drives, etc.). A message with the security classification label should be displayed when the information stored on the media is accessed.

For more information, please refer to [Safeguarding Government Information](#) or contact your [Sector Information Security Officer \(SISO\)](#).