

DOC-SEC-0005 - Data Classification and Handling Standard

Document ID: DOC-SEC-0005

Owner: CISO

Approver: CIO

Version: 3.0

Status: Published

Effective date: 2026-01-01

Review date: 2027-01

Applicability: All employees, contractors, and temporary workers handling Compass One information

Source system: Policy repository; enforcement in the document repository and approved enclaves

Fictional document created for the GS Reference Enterprise. Not real policy.

PURPOSE

This standard states how Compass One decides what an information asset is, how it must be marked, where it may live, who may see it, and how it is disposed of. It implements the Compass One information classification model and supports the acceptable use rules in DOC-SEC-0003.

SCOPE

The standard covers information in every form, including documents, database records, message content, and physical media. Contract-specific markings, clauses, and program instructions control handling wherever they are stricter than this standard.

- This standard applies to all employees, contractors, and temporary workers.
- A contract instruction overrides this standard whenever the contract is stricter.

INFORMATION CLASSES

Compass One recognises seven information classes. Class is a property of the information itself, not of the system that happens to store it.

- Every information asset must carry one of seven Compass One information classes.
- Unmarked information is treated as internal proprietary information by default.
- The owning department owns the classification of internal proprietary information.
- The Compliance function owns the classification of controlled unclassified information.
- Contract-delivered federal material is treated as federal contract information by default.
- Export-controlled technical data requires an export determination before storage.

MARKING

- Every document containing controlled unclassified information must carry a visible marking.
- The marking must cite the contract clause that imposes the control.
- Marking is applied by the document author at creation.
- An unmarked deliverable may not leave a Compass One system boundary.

STORAGE AND TRANSMISSION

Storage location is determined by the highest class present in the asset. Mixing classes in one container raises the container to the highest class it holds.

- Controlled unclassified information must reside in an approved enclave.
- Covered defense information must reside in a program approved enclave.
- Internal proprietary information may reside in the standard document repository.
- Compass One prohibits storage of controlled unclassified information in chat platforms.
- Compass One prohibits storage of export-controlled technical data in shared drives.
- Transmission of controlled unclassified information requires an approved encrypted channel.
- Personal email accounts are prohibited for every Compass One information asset.

ACCESS AND SHARING

- Access to program-scoped information is granted by program boundary rather than job title.
- A named access list is required for every controlled unclassified information repository.
- External sharing of commercial information requires data owner approval.
- A non-disclosure agreement must exist before any external sharing of proprietary information.

RETENTION AND DISPOSAL

- Compass One retains federal contract information for the full contract retention period.
- Physical media holding controlled unclassified information must be shredded by approved means.
- Disposal of controlled unclassified information requires a recorded certificate of destruction.

INCIDENT HANDLING

- A suspected disclosure of controlled unclassified information must be reported within one hour.
- Every report must follow the incident reporting procedure in DOC-SEC-0002.
- A covered defense information incident requires Government reporting within seventy two hours.

OWNERSHIP AND REVIEW

- The CISO owns this standard.
- This standard is reviewed each January by the CISO.