

Four Labels. One Goal. Protect What Matters.

North Carolina uses a system based on four data classifications to help guide employees on how to handle, store, share, and apply sensitivity labels to data:



Public

Content anyone may access, as it does not contain sensitive or high-risk information or data.

Examples:

Information on publicly accessible websites, routine correspondence, published press releases, marketing materials, job postings.



Internal

Content intended for staff or approved partners within your agency or state government. If made public, it would not cause harm.

Examples:

Work schedules and assignments, administrative records, internal newsletters, internal policies, meeting materials, drafts of documents not yet published.



Confidential

Private information that is often limited to a small audience on a need-to-know basis. If exposed, it could cause operational issues or harm to a person, employee, the agency, or the state and could result in regulatory or legal fines.

Examples:

Business unit plans, security information, drafts of annual/quarterly reports, forecasting assumptions, personnel records, legal proceedings and investigations, source code and detailed architecture, policies/guidelines related to physical or technical security.



Restricted

The most protected category and intended for a limited audience, content includes regulated or legally protected data. Exposure would cause a significant impact or harm to a person, employee, the agency, or the state.

Examples:

Personally identifiable information (PII), payment card industry (PCI) data security standards, protected health information (PHI), criminal justice information (CJI), Social Security numbers, state and federal tax information (FTI), attorney-client communications, state employee HR records.

What Label Should I Choose?

Answer a few simple questions to find the right sensitivity label.

1. Is this information approved for public release?

YES → PUBLIC

NO → Go to Question 2



2. Is this routine business information intended for internal use or anyone working in state government?

YES → INTERNAL

NO → Go to Question 3



3. Could unauthorized access or disclosure cause harm to a person, employee, agency, or the state? (Examples include customer, personal, financial, contract, security, or other information intended only for authorized users.)

YES → CONFIDENTIAL

NO → Go to Question 4



4. Is this among our most sensitive information, where unauthorized access or disclosure could cause serious harm or where access must be tightly limited? (Examples include highly sensitive personal data, credentials, security information, or other specially protected data.)

YES → RESTRICTED

NO → CONFIDENTIAL



Still Not Sure? Do Not Guess.

Check the Statewide Data Classification and Handling Policy (<https://it.nc.gov/data-classification>) or consult with your manager, supervisor, or security or privacy office.