9.1.2 Information Classification Facts

Information classification is the process of determining how and what information will be disclosed to ensure an organization's privacy requirements. There are many different information classification schemes used by different private and governmental organizations. For example, many organizations use the Information Security Classification Framework shown in the following table:

Sensitivity Classification	Description
High	Could cause extremely serious personal or organizational injury, including: ▪ Extreme financial loss ▪ Extreme operational harm, such as loss of control or loss of public trust ▪ Extreme personal harm, such as loss of life or social hardship For example, personally identifiable information (PII) and protected health information (PHI) is considered highly sensitivity and disposed of according to the appropriate laws and regulations.
Medium	Could cause serious personal or organizational injury, including: ▪ Significant financial loss ▪ Significant operational harm, such as loss of confidence or damage to reputation ▪ Significant personal harm, such as personal hardship or embarrassment
Low	Could cause limited or no injury to individuals or the organization, including: ▪ Limited financial loss ▪ Limited operational harm, such as reduced organizational effectiveness or loss of morale ▪ Limited personal harm, such as embarrassment or inconvenience

Other organizations may use a different information classification scheme, such as the following:

Policy	Description
Public with Full Distribution	*Public with full distribution* allows everyone to have free access to a copy of the information with no restrictions. A public website would be classified as public with full distribution.
Public with limited distribution	*Public with limited distribution* allows private information to be distributed to only selected individuals for a specific purpose. They may have to sign non-disclosure agreements (NDAs) to protect the information from becoming public knowledge.
Private Internal	*Private internal* information is restricted to individuals within the organization. Private internal information might include: ▪ Personnel records ▪ Financial records ▪ Customer lists
Private Restricted	*Private restricted* information is restricted to limited authorized personnel within the organization. Private restricted information might include: ▪ Trade secrets ▪ Strategic information ▪ Highly sensitive information
Proprietary	*Proprietary* information is information that a company wishes to keep confidential. Proprietary information can include secret formulas, processes, and methods used in production.
PII	*Personally identifiable information* (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. This includes: ▪ Full name (if not common) ▪ Home address ▪ Email address (if private from an association/club membership, et cetera) ▪ National identification number ▪ Passport number ▪ IP address (when linked, but it is not PII by itself in US) ▪ Vehicle registration plate number ▪ Driver's license number

	▪ Face, fingerprints, or handwriting ▪ Credit card numbers ▪ Digital identity ▪ Date of birth ▪ Birthplace ▪ Genetic information ▪ Telephone number ▪ Login name, screen name, nickname, or handle
PHI	*Protected health information* (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This includes any part of a patient's medical record or payment history.

There are different roles that identify the responsibilities regarding data quality.

Role	Description
Data Owner	A senior person in an organization with the authority to make decisions regarding the quality of data created, stored, consumed and retired.
Data Custodian	A person that is responsible for the quality of the data on a day-to-day basis.
Data Producers	A person responsible for creating or capturing data. Most people in an organization are data producers.
Data Consumers	A person who is using the data. The data must be good enough for them to perform their work. They define what is good data.
Privacy Officer	A person who oversees data activities to ensure they are in compliance with government laws.

The following table describes government and military classifications.

Policy	Description
Unclassified	*Unclassified* information can be accessed by the public and poses no security threat.
Sensitive but Unclassified	*Sensitive but unclassified* information, if disclosed, could cause some harm, but not a national disaster.
Confidential	*Confidential* information is the lowest level of classified information used by the military. It allows restriction of release of information under the Freedom of Information Act. Release of this information could cause damage to military efforts.
Secret	*Secret* information is information that, if disclosed, could cause severe and permanent damage to military actions. This could include information about: ▪ Troop movement ▪ Deployments ▪ Military capabilities
Top Secret	*Top secret* information is the highest level of classified information used by the military. If top secret information is released, it poses grave consequences to national security. This could include information about: ▪ Development of new weapons ▪ Intelligence-gathering activities