**Data Governance:**

**Data governance** is the set of policies, procedures, and controls that an organization develops to safeguard its information while making it useful for transactional and analytic purposes.

**Data Governance Roles**

1. Data Steward - responsible for leading an organization's data governance activities
2. Data Owner - senior business leader with overall responsibility for a specific data domain
3. Data Custodian - role given to someone who implements technical controls that execute data governance policies.

**Data access requirements** determine which people need access to what data.

|  |  |
| --- | --- |
| **Classification term** | **Classification description** |
| **Public** | Data intended for public consumption. For example, anything on a public-facing website meets this classification. No disclosure implications. |
| **Internal** | Data intended for use within an organization. For example, a comprehensive organization chart including names. Disclosure compromises an organization's reputation or operations, but not its privacy or confidentiality obligations. |
| **Sensitive** | Data intended for limited use within an organization. For example, a list of employees and their compensation. Disclosure implies a violation of privacy or confidentiality. |
| **Highly Sensitive** | Data intended for restricted use, typically due to compliance obligations. Examples include Social Security numbers and bank account numbers. Disclosure implies a legal obligation in the event of a data breach. |