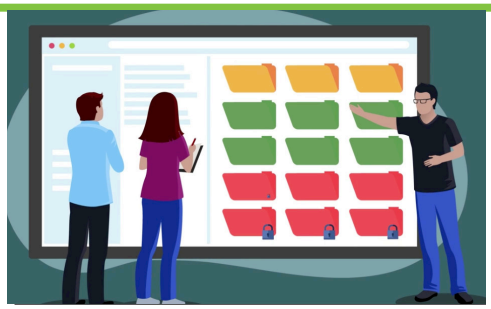
Click Thinking Spotlight

Data Classification

Not all information we deal with in the workplace is the same. Knowing how to treat it can be difficult without guidelines. A data classification policy eliminates ambiguity and clarifies what fits where.

- Many organizations find it essential to have a data classification policy—and may even be required to for regulatory purposes, or due to increased scrutiny from board members. Regardless of the reason, classifying data makes sense.
- A data classification policy eliminates ambiguity and clarifies what fits where. It dictates how information should be treated and protected, setting ground rules that everyone can follow.
- A policy also acknowledges that there are risks involved with data disclosure that can impact an organization's reputation and undermine its integrity—and that access should be meted out in a way that reduces risk.
- Whether your organization serves the private sector, the public sector or both, the overriding concept is the same: Data should be classified in a manner that sufficiently protects the organization, its employees and the people and clients it serves.
- In the private sector, a typical policy might include the following categories: Public or Unrestricted, Internal or Private, Confidential, Sensitive.
- In the public sector, where data disclosure can impact public safety or even national security, these designations may look like this: Unclassified, Sensitive, Confidential, Secret, Top Secret.
- With categories set, the next step is to designate what fits where using the scheme as a guide.
- For example, let's say you run a shipping company that serves both the private and public sectors. Your data includes a press release about new delivery areas, government contracts, employee tax id numbers and plans to acquire a competitor.
- The press release would be considered public, or unclassified if relating to a government entity. The employee tax id numbers would be considered internal. The government contracts would be considered confidential. And the acquisition plans would be considered sensitive.
- In any scheme, each piece of data has its place. However, data can also be reclassified. The takeaway here is that the plan is a changing entity that accounts for new developments.
- With a data classification policy in place, guidelines for handling and disclosing data are clear to all, which can lead to a more secure and efficient workplace.



For the Data Classification module, see your manager or information security contact.