- Security mindset: the ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data.
- **Common data types:**
  - Public: already accessible to the public and poses a minimal risk to the organization if viewed or shared by others.
  - Private: information that should be kept from the public.
  - Sensitive: information must be protected from everyone who does not have authorized access.
  - Confidential: important for an organization's ongoing business operations.
- Business Continuity plan: a document that outlines the procedures to sustain business operations during and after a significant disruption.
- **Essential steps for business continuity plans:**
  - Conduct a business impact analysis
  - Identify, document, and implement steps to recover critical business functions and processes.
  - Organize a business continuity team.
  - Conduct training for the business continuity team.
- Disaster Recovery plan: allows an organization's security team to outline the steps needed to minimize the impact of a security incident.
- **Steps to create a disaster recovery plan:**
  - Implementing recovery strategies to restore software.
  - Implementing recovery strategies to restore hardware functionality.
  - Identifying applications and data that might be impacted after a security incident has taken place.