Glossary terms

Terms and definitions

Business continuity plan (BCP): A document that outlines the procedures to sustain business operations during and after a significant disruption

Confidential data: Data that often has limits on the number of people who have access to it

Disaster recovery plan: A plan that allows an organization's security team to outline the steps needed to minimize the impact of a security incident

Private data: Information that should be kept from the public

Public data: Data that is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others

Security mindset: The ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data

Sensitive data: A type of data that includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI)