Glossary terms from module 3

Terms and definitions from Course 1, Module 3

Asset: An item perceived as having value to an organization

Availability: The idea that data is accessible to those who are authorized to access it

Compliance: The process of adhering to internal standards and external regulations

Confidentiality: The idea that only authorized users can access specific assets or data

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

Hacktivist: A person who uses hacking to achieve a political goal

Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal law established to protect patients' health information

Integrity: The idea that the data is correct, authentic, and reliable

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

Privacy protection: The act of safeguarding personal information from unauthorized use

Protected health information (PHI): Information that relates to the past, present, or future physical or mental health or condition of an individual

Security architecture: A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats

Security controls: Safeguards designed to reduce specific security risks

Security ethics: Guidelines for making appropriate decisions as a security professional

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Security governance: Practices that help support, define, and direct security efforts of an organization

Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Mark as completed