**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

**Terms and definitions from Course 1, Module 4**

**Antivirus software:** A software program used to prevent, detect, and eliminate malware and viruses

**Database:** An organized collection of information or data

**Data point:** A specific piece of information

**Intrusion detection system (IDS):** An application that monitors system activity and alerts on possible intrusions

**Linux:** An open-source operating system

**Log:** A record of events that occur within an organization’s systems

**Network protocol analyzer (packet sniffer):** A tool designed to capture and analyze data traffic within a network

**Order of volatility:** A sequence outlining the order of data that must be preserved from first to last

**Programming:** A process that can be used to create a specific set of instructions for a computer to execute tasks

**Protecting and preserving evidence:** The process of properly working with fragile and volatile digital evidence

**Security information and event management (SIEM)**: An application that collects and analyzes log data to monitor critical activities in an organization

**SQL (Structured Query Language):** A query language used to create, interact with, and request information from a database