MICAD LIMITED
Advanced Industrial Security Supervisor Training

# Glossary of Terms

This glossary defines key terms and concepts used throughout the course.

## A

**Access Control:** The process of restricting access to physical areas, systems, or data based on predefined security policies. This can involve physical measures (e.g., locks, security guards) and logical measures (e.g., passwords, access control lists).

**Active Shooter:** An individual actively engaged in killing or attempting to kill people in a confined and populated area.

**Administrative Controls:** Security measures implemented through policies, procedures, and guidelines, rather than through technology.

Alarm System: A system designed to detect unauthorized entry or other security threats and trigger an alarm.

**Asset:** Any item of value to an organization, including physical assets (equipment, buildings), information assets (data, intellectual property), and personnel.

## B

**Biometrics:** The use of biological characteristics (e.g., fingerprints, iris scans) for authentication and access control.

**Business Continuity Plan (BCP):** A plan outlining how an organization will continue its operations during and after a disruptive event.

## C

**CCTV (Closed-Circuit Television):** A video surveillance system consisting of cameras, monitors, and recording devices.

**Chain of Custody:** The documented process of handling evidence to ensure its integrity and admissibility in legal proceedings.

**Cipher:** An algorithm for encryption or decryption.

**Crisis Management:** The process of responding to and managing a crisis situation to minimize its impact.

**Cybersecurity:** The protection of computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

**Cybersecurity Incident:** Any event that adversely impacts the confidentiality, integrity, or availability of an organization’s information systems or data.

## D

**Data Loss Prevention (DLP):** Measures taken to prevent sensitive data from leaving an organization's control.

**Digital Forensics:** The application of computer science and investigative techniques to gather and analyze evidence from digital devices.

## E

**Encryption:** The process of converting readable data into an unreadable format to protect its confidentiality.

**Emergency Response Plan:** A plan detailing procedures for responding to various types of emergencies.

**I**

**Incident Response:** The process of responding to and recovering from a security incident.
**Intrusion Detection System (IDS):** A system that monitors network traffic for malicious activity.

**P**

**Perimeter Security:** Measures taken to secure the boundary of a physical area.
**Physical Security:** Measures taken to protect physical assets and personnel from unauthorized access, theft, or damage.
**PLC (Programmable Logic Controller):** A digital computer used for automation of electromechanical processes.
**Policy:** A high-level statement of organizational intent.
**Procedure:** A step-by-step guide to accomplishing a task.

**R**

**Risk Assessment:** The process of identifying, analyzing, and evaluating risks.
**Risk Mitigation:** The process of reducing the likelihood or impact of a risk.

**Risk Management:** The systematic application of management policies, procedures and practices to the activities of analyzing, evaluating, controlling and monitoring risk.

**Role-Based Access Control (RBAC):** An access control model that grants users access based on their roles within an organization.

### S

**SCADA (Supervisory Control and Data Acquisition):** A system used to monitor and control industrial processes.

**Security Awareness Training:** Training designed to educate employees about security threats and best practices.

**Surveillance:** The systematic observation of an area or activity, often using CCTV.

### T

**Technical Controls:** Security measures implemented through technology, such as firewalls, intrusion detection systems, and encryption.

**Threat:** Any potential danger or event that could compromise security.

**Vulnerability:** A weakness in a system or process that could be exploited by a threat.

This glossary is not exhaustive, but it covers many of the key terms used in this course. The specific meaning of a term may vary slightly depending on the context.