Title

Security Terms and Definitions – Reliable People, Protection, Technical Systems, Operations & Assurance

---

✅ Category

Security Framework – Foundational Knowledge

✅ Description

This document defines critical security terms and concepts used across the Security Management System. It supports AI training by clarifying terminology for consistent interpretation in policy, SOPs, and training materials. It includes definitions for Reliable People, Protection, Technical Systems, and Operations & Assurance to ensure understanding aligned with international standards and best practices.

✅ Tags

security, human reliability, access control, CCTV, incident management, chain of custody, data protection, human rights, ISO27001, security operations, technical systems

---

✅ Upload Notes (Admin Only)

Provides authoritative definitions for security terminology used across all MPS standards. Intended to improve AI understanding and ensure consistent use of key terms in all security-related AI outputs.

📌 Reliable People Terms

Reliable People
The concept of Reliable People in security is rooted in human reliability engineering and human factors management. It refers to the deliberate selection, screening, training, leadership, and management of personnel to ensure they act consistently, ethically, and in line with security requirements. Reliability is achieved through integrity testing, ongoing vetting, competence-based training, and fostering a positive security culture.

Golden Rules
A concise set of non-negotiable security principles that all personnel must follow. These rules are widely communicated, easy to remember, and supported by clear disciplinary consequence models to reinforce compliance.

Consequence Models
Structured, documented systems defining proportional consequences for violations of company policies, procedures, or Golden Rules. Consequence Models promote fairness, consistency, and transparency, helping employees understand what behaviour is acceptable and what is not.

Integrity Testing
A form of psychometric testing designed to evaluate an individual's honesty, reliability, and ethical decision-making. It can be applied pre-employment or during employment to assess personal integrity and support the development of a trustworthy workforce.

Single Point Briefing (SPB)
A clear, one-page visual guide showing step-by-step instructions for a specific task. Typically includes diagrams or photos with concise text. Used for training, standardisation, and quick reference to ensure safe, consistent execution of tasks.

Induction Training
Structured onboarding sessions that introduce new employees to security policies, operational procedures, ethics expectations, and the company's security culture. Ensures all personnel understand their role in protecting company assets and maintaining safety.

📌 Protection Terms

Voluntary Principles on Security and Human Rights (VPSHR)
A globally recognised framework guiding companies to maintain the safety and security of operations while respecting human rights. VPSHR emphasises risk assessments, stakeholder engagement (including communities), transparency, and accountability when working with public and private security forces.
Learn More

Government Security / Public Security
Terms used interchangeably to describe official security forces provided by government agencies. Within VPSHR, Public Security refers to law enforcement and military forces tasked with safeguarding company operations while respecting human rights.

Private Security
Security services contracted by a company from private providers. Providers must comply with local laws and often with international standards such as the International Code of Conduct for Private Security Providers (ICoCA).

International Code of Conduct Association (ICoCA)
An international multi-stakeholder initiative that certifies and monitors private security providers for compliance with human rights standards, ethical conduct, and duty-of-care obligations. Membership demonstrates a commitment to responsible security operations.
[Learn More](#)

Community Engagement
Structured processes of dialogue and collaboration with local communities to identify, mitigate, and resolve security-related concerns. Essential to preventing conflict, ensuring safety, and respecting human rights, as emphasised by VPSHR.

Security Risk Assessment
A structured process to identify, evaluate, and prioritise security threats and vulnerabilities in order to design proportionate, effective controls. Typically aligns with international risk management standards such as ISO 31000.

📌 Technical Systems Terms

Uninterruptible Power Supply (UPS)
A device that provides emergency power to security systems in the event of a mains failure, ensuring continued operation of critical infrastructure like CCTV, alarms, and access control.

Radio-Frequency Identification (RFID)
Technology using electromagnetic fields to automatically identify and track tags attached to objects. In security, RFID can track personnel movements, valuable assets, sealed containers, and equipment to improve chain-of-custody integrity.

Security Management System (SMS)
An integrated system that monitors, controls, and coordinates security operations. Typically includes alarm monitoring, access control management, video surveillance integration, and incident reporting capabilities.

Access Control System (ACS)
Electronic or manual systems that manage and monitor who can enter or exit facilities, areas, or secure zones. Includes badge readers, biometric systems, and entry logs.

CCTV (Closed-Circuit Television)
A video surveillance technology that captures and records imagery for security monitoring, deterrence, and forensic investigation. Modern systems include advanced analytics and remote monitoring capabilities.

Security Information and Event Management (SIEM)
A system that collects, analyses, and correlates security events and logs from various

sources to detect and respond to threats in real time. Supports incident response, compliance, and audit requirements.

Alarm Management System
A centralised platform that receives, prioritises, and tracks security alarms and events. Supports effective, timely response to security incidents.

Data Protection
Policies and processes that ensure security-related data (including video footage and access logs) is stored, handled, shared, and disposed of in compliance with privacy laws and ethical standards, such as GDPR or local data protection legislation.

📌 Operations & Assurance Terms

Chain of Custody
A documented process ensuring continuous control over valuable or sensitive items as they move through different stages, locations, or handlers. Essential for maintaining integrity and supporting legal or audit requirements.

Search Protocol
Standardised, documented procedures for conducting searches of people, vehicles, or items entering or leaving controlled areas, ensuring fairness, legality, and effectiveness.

Security Assurance
An independent process of evaluating whether security controls are effective, fit-for-purpose, and compliant with policies and standards. Includes audits, reviews, and testing.

Incident Management System (IMS)
A structured system for recording, investigating, resolving, and analysing security incidents to prevent recurrence, improve controls, and support continuous improvement.

Surveillance Plan
A documented approach for deploying and using monitoring technologies and personnel based on risk assessments, objectives, and legal requirements.

Audit Trail
A chronological record of system activities, security events, or chain-of-custody handovers that enables traceability, accountability, and forensic investigation.

Key Control
A system for managing, tracking, and auditing the use of physical keys or access devices to maintain security over facilities and assets.