Title

Physical Security and Technical Systems Standards (Including Human Rights Requirements)

Category

PROTECTION – PHYSICAL AND TECHNICAL SECURITY STANDARDS

Description

This document outlines international best-practice requirements for physical and technical security controls in high-risk operational environments. It provides practical, risk-based guidelines for physical barriers, perimeter fencing, vault design, CCTV and surveillance systems, power management (including UPS), and alarm systems. It also includes comprehensive guidance on implementing the Voluntary Principles on Security and Human Rights (VPSHR), ensuring all security arrangements uphold human rights and legal standards.

Tags

- Physical Security

- Technical Systems
- Vault Design
- CCTV
- Access Control
- UPS
- Surveillance
- Human Rights
- VPSHR
- Crime Prevention Through Environmental Design (CPTED)
- Risk Assessment
- Asset Protection
- Security Standards
- Compliance

Upload Notes / Admin Guidance

- 📌 Intended for **reference in risk assessments, design reviews, training**.
- 📌 Supports **MPS16–21 (Protection), MPS22 (Documentation), MPS25 (Intelligence)**.
- 📌 Fully text-based for optimal AI use, with **image descriptions included**.
- 📌 **Human Rights compliance requirements (VPSHR)** embedded for alignment with international norms.

- 📌 Recommended format: *PDF or DOCX*, with clear section headings.

Document Content

---

1. Purpose

To set minimum standards for physical and technical security controls based on international best practices and risk assessment. These requirements are intended to reduce security risk while respecting human rights obligations.

---

2. General Principles

- Security controls must be risk-assessed and proportionate.
- Security is a “weakest link” problem: effectiveness depends on the integrity of all parts.
- Security design must balance access, usability, cost, and protection.
- Defence in depth through multiple, mutually reinforcing layers of control is required.

---

3. Physical Security Controls

3.1 Bollards

- Used where high-risk areas border public spaces or highways.
- Distance between bollards ≤ 1.7 m to prevent vehicle ramming.
- Consider standoff space between bollards and building façade.

3.2 Perimeter Fencing

- Used to define and partition high-risk areas.
- Clear signage warning against unauthorised access.
- Design with double fence lines for critical areas (e.g., stockyards):
    - Outer fence: ≥ 2.5 m high with barbed/razor wire; buried 0.5 m.
    - Inner fence: tight mesh with ≥ 2.5 m height.
    - ~4 m clear no-man’s land between fences, maintained for visibility.
    - CCTV coverage and lighting in this space.

3.3 Bullet-Resistant Materials

- Applied to transparent barriers facing public areas where armed robbery risk exists.

3.4 Perimeter Wall Reinforcing

- Required where the perimeter wall is the primary defence.

3.5 Lighting

- Designed for effective CCTV operation.
- Match light source (white/LED, yellow/sodium) to CCTV specs.
- Apply CPTED principles: clear sightlines, well-lit work areas.

3.6 Vaults

- Must meet insurance requirements, typically a two-hour delay standard.
- Equipped with:
  - Dual custody tumbler/key locks.
  - Duress alarm.
  - Seismic alarm.
  - Motion detection (secured/unsecured states).
  - CCTV coverage.
  - Entry/exit logging.
  - Bolt status monitoring.
- Combination changes required:
  - At least annually.
  - Whenever a knowledgeable person leaves their role.

3.7 Doors and Frames

- Must meet local regulatory standards or company standards where these are higher.
- The entire structure (doors, frames, walls) must resist forced entry for the designed delay time.

3.8 Sally Ports

- Used where vehicle access to secure areas is required.
- Kept clear and under surveillance.
- Doors designed so both cannot open simultaneously without positive control.

---

4. Technical Systems Standards

4.1 Power Supply

- Secure systems require robust power management with UPS.
- UPS requirements:
  - Professional maintenance support.
  - Bypass switch for safe servicing.
  - Remote management and alarm interface.
  - Alarms for power loss and battery depletion.
  - 60 % load limit for battery health.

    - Managed environment (temperature/humidity).
    - Used only for critical systems.
    - Supports automated server shutdown sequences.

4.2 Equipment Enclosures

- Waterproof, dustproof, earthed.
- Neat, labelled cabling.
- Anti-tamper alarms.
- Lockable, with unique locks.
- Equipment lists and maintenance sheets inside doors.
- Spike and surge protection.
- IP address labels.

4.3 Server Rooms

- Restricted access.
- Clean, dust-free, environmentally controlled.
- Cabling neat and labelled.

4.4 Cabling

- Tamper-resistant ducts in high-risk areas.

5. Input Sensors

- Seismic detectors and video-enabled motion detection for vaults.
- Personal duress sensors in high-risk, public-interfacing areas.
- Perimeter activity detectors with immediate alarm integration.
- Motion/acoustic monitoring for windows, entrances, roof spaces.
- RFID asset tracking for high-value packages and equipment.

---

6. CCTV Systems

- Camera placement based on risk assessments and cross-functional input.
- Camera types to match operational needs:
  - Thermal imaging.
  - High-definition fixed or automatic PTZ with motion tracking.
  - Avoid manual PTZ where possible.
- Design for day/night use, high-resolution imaging.
- Minimum frame rate requirements by risk:
  - High-risk areas: 25 ips; 5 ips background; 13–15 ips motion.
  - Moderate: 13–15 ips; 2 ips background; 5–10 ips motion.
  - Low risk: 13–15 ips optional.

- Consider video analytics integration with the Security Management System.
- Equipment placement designed for maintenance access.

---

7. Access Control Systems

- Biometric readers at entry/exit of secure areas.
- Consider biometrics for internal partition doors within high-risk zones.

---

8. Human Rights Requirements: Voluntary Principles on Security and Human Rights (VPSHR)

- **Core Principle:** Security must respect human rights and fundamental freedoms.
- **Implementation Includes:**
  - Risk assessments considering human rights records of security providers.
  - Regular consultation with communities, governments, civil society.
  - Clear communication of human rights policies to security forces.
  - Training on the use of force, proportionality, and accountability.
  - Incident reporting and investigation protocols.
  - Contract clauses requiring compliance with VPSHR standards.
- **Interactions with Public Security:**
  - Transparent arrangements.

    - Proportional deployment.
    - Appropriate use of force.
    - Medical aid for injuries.
    - Reporting and investigation of abuses.
- **Interactions with Private Security:**
    - Background checks.
    - Professional training.
    - Contractual obligations for ethical conduct.
    - Monitoring and accountability.
    - Defensive, not offensive, roles.
    - Confidentiality and respect for rights.

---

9. Annex: Model VPSHR Clauses for Contracts

Includes recommended contractual language covering:

- Definitions of Security and Human Rights Standards.
- Commitments to use of force only when necessary.
- Training obligations for security forces.
- Screening for personnel with human rights abuse records.
- Chain of command and company liaison protocols.

- Investigation and transparency requirements.
- Medical care provisions.

End of Document