SCOPE Framework: Physical & Environmental Security Control Domain

Table of Contents

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Purpose: The Physical & Environmental Security domain ensures the protection of organizational personnel, facilities, and physical assets through structured controls that prevent unauthorized access, monitor sensitive areas, manage environmental conditions, and securely decommission equipment. This domain encompasses facility access restrictions, visitor and equipment logging, environmental safeguards (e.g., HVAC, power, fire), secure disposal of data-bearing devices, and surveillance and intrusion detection systems. By embedding physical safeguards into operational processes, the organization mitigates threats stemming from physical compromise, enhances situational awareness, and ensures continuity of operations in alignment with risk tolerance, compliance mandates, and business requirements.

Section 1. Facility Access Controls (FAC)

Effective physical protection of organizational facilities is foundational to overall information security. Facility Access Controls establish safeguards to prevent unauthorized physical access, damage, and interference to business premises and information systems. These controls ensure access to sensitive areas is limited, monitored, and aligned with job responsibilities, operational requirements, and risk tolerance.

1.1 FAC-01: Facility Access Authorization

The organization shall establish, document, and maintain access authorization policies and procedures to ensure that only authorized personnel are granted physical access to facilities housing critical infrastructure, data systems, or sensitive information.

1.2 FAC-02: Physical Access Control Systems (PACS)

The organization shall implement and maintain PACS technologies (e.g., keycards, biometric scanners) to enforce access restrictions and monitor entries and exits for all protected areas.

1.3 FAC-03: Role-Based Physical Access

The organization shall restrict physical access to secure areas based on job function and role, with approvals required from designated personnel responsible for information or asset protection.

1.4 FAC-04: Entry & Exit Authentication Mechanisms

The organization shall ensure that individuals entering and exiting secure facilities authenticate using at least one form of identification, with multi-factor verification required for high-security zones.

1.5 FAC-05: Access Reviews and Recertifications

The organization shall perform periodic reviews of all physical access permissions to validate continued need and revoke access when no longer required.

1.6 FAC-06: Badge Management Program

The organization shall maintain a formal badge management process to issue, track, and revoke access badges, including procedures for lost or stolen badges.

1.7 FAC-07: Physical Access Logging

The organization shall log all physical access attempts to controlled areas, including date, time, and individual identity, and retain logs in accordance with organizational retention policies.

1.8 FAC-08: Segmentation of Secure Areas

The organization shall design facilities with layered physical security zones, separating general areas from secure zones such as server rooms, network closets, and security operation centers.

1.9 FAC-09: Tailgating & Piggybacking Prevention

The organization shall implement controls and awareness mechanisms to prevent tailgating and piggybacking, including the use of mantraps, turnstiles, or security personnel where appropriate.

1.10 FAC-10: Emergency Access Protocols

The organization shall establish procedures for emergency physical access, including who may authorize such access, how it is logged, and post-event reviews.

1.11 FAC-11: After-Hours Facility Access

The organization shall restrict after-hours access to facilities to pre-approved personnel and require additional logging and notification controls for such events.

1.12 FAC-12: Physical Access Revocation

The organization shall immediately revoke facility access for terminated or suspended personnel and document the deactivation within the PACS.

1.13 FAC-13: Maintenance Personnel Access Controls

The organization shall establish strict controls and supervision requirements for external maintenance personnel requiring temporary access to facilities.

1.14 FAC-14: Delivery & Loading Dock Security

The organization shall control and monitor access to delivery zones and loading docks to prevent unauthorized entry and exposure of assets or systems.

1.15 FAC-15: Construction & Renovation Area Controls

The organization shall implement physical security measures for construction or renovation areas to prevent unauthorized access to adjacent secure zones.

1.16 FAC-16: Security Escort Requirements

The organization shall require escort of non-authorized individuals (e.g., contractors, guests) within controlled areas, with escorts remaining present for the full duration of the visit.

1.17 FAC-17: Facility Access Control Training

The organization shall ensure that personnel with access to secure areas receive training on physical security responsibilities, including reporting suspicious activity and handling access credentials.

1.18 FAC-18: Badge and Access Device Deactivation Procedures

The organization shall define and enforce procedures for deactivating and recovering physical access devices when lost, stolen, damaged, or no longer required.

1.19 FAC-19: Physical Access Anomaly Detection

The organization shall monitor access control logs for anomalies (e.g., access attempts during off-hours or repeated failed entries) and alert security personnel for investigation.

1.20 FAC-20: Temporary Access Management

The organization shall issue and track time-bound, limited-access credentials for temporary personnel, ensuring automatic expiration and revocation at the end of the defined period.

1.21 FAC-21: Dual-Person Entry Requirements

The organization shall require dual-person entry for highly sensitive areas (e.g., data centers, classified material rooms) as part of enforcing separation of duties and reducing insider threats.

1.22 FAC-22: Access Control System Testing & Maintenance

The organization shall periodically test and maintain physical access control systems to ensure operational effectiveness, integrity, and integration with monitoring technologies.

Section 2. Visitor & Equipment Logging (VEL)

Effective control over visitor activity and equipment movement within organizational facilities is critical for preventing unauthorized access, tampering, data theft, and physical compromise of systems. The Visitor & Equipment Logging (VEL) control family ensures all ingress, egress, and transfer events involving external parties and sensitive equipment are formally recorded, monitored, and subject to security protocols aligned with risk posture.

2.1 VEL-01: Visitor Registration Requirements

The organization shall require all visitors to register upon arrival at any facility, providing verifiable identification and stating the purpose and duration of the visit.

2.2 VEL-02: Visitor Log Maintenance

The organization shall maintain secure visitor logs that include name, organization (if applicable), arrival/departure time, escort name, purpose of visit, and areas accessed, retaining logs per organizational policy.

2.3 VEL-03: Visitor Identity Verification

The organization shall verify visitor identity against government-issued photo identification or other trusted credentials before granting facility entry.

2.4 VEL-04: Pre-Authorized Visitor List Controls

The organization shall maintain and utilize a pre-authorization process to approve visitors in advance, reducing risk of unauthorized or unexpected access.

2.5 VEL-05: Visitor Badge Issuance & Control

The organization shall issue time-bound, uniquely identifiable visitor badges that differentiate visitors from personnel, and ensure badges are collected upon exit.

2.6 VEL-06: Escort Requirement for Visitors

The organization shall require all visitors to be accompanied by an authorized escort at all times when inside restricted or sensitive facility areas.

2.7 VEL-07: Visitor Access Restriction Zones

The organization shall limit visitor movement to designated non-sensitive areas unless explicitly authorized for access to higher-security zones.

2.8 VEL-08: Visitor Activity Monitoring

The organization shall implement procedures for monitoring visitor behavior and activity during facility presence, including visual observation or surveillance support.

2.9 VEL-09: Visitor Access Time Restrictions

The organization shall restrict visitor access to normal operating hours unless prior written approval for after-hours access is granted and documented.

2.10 VEL-10: Visitor Equipment Declaration Requirements

The organization shall require visitors to declare any electronic or physical equipment brought on premises, subjecting such items to inspection and entry in an equipment log.

2.11 VEL-11: Equipment Entry Logging

The organization shall log all external or personally owned equipment brought into facilities, including asset descriptions, serial numbers, ownership, and intended use.

2.12 VEL-12: Equipment Exit Authorization

The organization shall require documented authorization prior to the removal of any equipment—owned, leased, or visitor-controlled—from the facility.

2.13 VEL-13: Temporary Equipment Passes

The organization shall issue temporary passes for authorized equipment entry/exit, with specific duration, asset description, responsible party, and approver identified.

2.14 VEL-14: Prohibited Equipment Enforcement

The organization shall enforce policies restricting the entry of prohibited equipment (e.g., USB drives, external hard disks, personal Wi-Fi devices) by visitors, and apply enforcement mechanisms as appropriate.

2.15 VEL-15: Digital Visitor Management System (VMS)

The organization shall utilize a digital VMS platform to streamline check-in/check-out processes, integrate with PACS, and improve auditability of visitor records.

2.16 VEL-16: Audit of Visitor & Equipment Logs

The organization shall perform periodic audits of visitor and equipment logs to ensure completeness, accuracy, and compliance with facility security protocols.

2.17 VEL-17: Contractor and Vendor Access Logging

The organization shall maintain distinct logging procedures for contractors and vendors that capture extended access permissions, duration of work, and responsible internal point of contact.

2.18 VEL-18: Ad-Hoc Equipment Tracking Events

The organization shall implement ad-hoc tracking for any equipment temporarily relocated or repurposed within the facility to ensure operational transparency.

2.19 VEL-19: Integration of Logs with Physical Security Events

The organization shall correlate visitor and equipment log data with physical access events to detect anomalies or discrepancies requiring investigation.

2.20 VEL-20: Retention of Visitor & Equipment Records

The organization shall retain visitor and equipment logs for a minimum period defined by policy, regulatory requirements, or based on risk assessments, ensuring secure storage and controlled access.

2.21 VEL-21: Tamper Protection for Physical Logs

If using physical logbooks, the organization shall implement tamper-evident measures and restrict logbook access to authorized personnel only.

2.22 VEL-22: Immediate Reporting of Lost or Unreturned Equipment

The organization shall require visitors and responsible personnel to immediately report any equipment not returned as required, triggering investigation and appropriate escalation.

Section 3. Environmental & Power Controls (EPC)

Environmental and power management systems play a critical role in maintaining operational continuity and the physical safety of information systems. The Environmental & Power Controls (EPC) control family ensures safeguards are in place to detect, mitigate, and respond to conditions such as fire, flooding, extreme temperatures, humidity, and power disruptions, reducing risk to personnel, assets, and data availability.

3.1 EPC-01: Environmental Monitoring Systems

The organization shall deploy and maintain environmental monitoring systems to detect temperature, humidity, smoke, water presence, and other environmental factors in data centers and critical infrastructure zones.

3.2 EPC-02: HVAC System Security & Redundancy

The organization shall implement secure, redundant HVAC systems to maintain appropriate environmental conditions for facilities housing sensitive equipment, ensuring continuity in the event of system failure.

3.3 EPC-03: Fire Detection Systems

The organization shall install automatic fire detection systems in accordance with local fire codes and industry best practices, with integration into building management or alarm systems.

3.4 EPC-04: Fire Suppression Systems

The organization shall equip critical areas with non-destructive fire suppression systems (e.g., FM-200, inert gas, or pre-action sprinklers) that minimize risk to electrical systems and stored data.

3.5 EPC-05: Emergency Power Off (EPO) Controls

The organization shall provide Emergency Power Off (EPO) controls in critical areas to safely shut down equipment or power circuits during emergencies, ensuring the controls are clearly labeled and restricted.

3.6 EPC-06: Uninterruptible Power Supply (UPS)

The organization shall implement UPS systems to provide immediate backup power to critical systems in the event of primary power failure and support graceful system shutdown.

3.7 EPC-07: Backup Power Generation

The organization shall maintain standby generators or alternate power sources capable of sustaining operations for a defined duration, based on the organization’s Recovery Time Objectives (RTO).

3.8 EPC-08: Scheduled Testing of Power Systems

The organization shall conduct scheduled tests and maintenance of UPS units, generators, and related systems to validate readiness and detect degradation or failure.

3.9 EPC-09: Water Detection & Leakage Alarms

The organization shall deploy water detection systems (e.g., leak sensors) in areas at risk of flooding or water intrusion, including beneath raised floors and near plumbing infrastructure.

3.10 EPC-10: Cable and Wiring Management

The organization shall ensure that cabling and electrical wiring is organized, elevated when necessary, and protected from environmental threats such as water exposure, heat, or physical stress.

3.11 EPC-11: Raised Floor Environmental Design

The organization shall use raised flooring in data centers and network rooms to support air circulation, prevent water damage, and facilitate cable management where feasible.

3.12 EPC-12: Airflow Optimization & Containment

The organization shall implement airflow management strategies such as hot/cold aisle containment or directional airflow to maximize cooling efficiency and prevent equipment overheating.

3.13 EPC-13: Environmental Alarm Notifications

The organization shall configure environmental monitoring systems to trigger automated alerts for threshold violations (e.g., temperature or humidity spikes), sending notifications to designated personnel.

3.14 EPC-14: Fire Extinguisher Placement & Inspection

The organization shall ensure fire extinguishers are appropriately placed throughout the facility, inspected regularly, and suited for the fire classes most likely to occur (e.g., Class C for electrical).

3.15 EPC-15: Physical Separation of Environmental Systems

The organization shall house HVAC, electrical, and power distribution systems in physically protected areas to reduce the risk of tampering, accidents, or collateral damage during facility incidents.

3.16 EPC-16: Humidity Control and Alerting

The organization shall actively monitor humidity levels in equipment zones and trigger alerts when deviations occur that could lead to electrostatic discharge or condensation risks.

3.17 EPC-17: Environmental Incident Response Procedures

The organization shall develop and maintain procedures for responding to environmental emergencies (e.g., overheating, flooding, power loss), including notification, evacuation, system shutdown, and recovery processes.

3.18 EPC-18: Ventilation for Hazardous Emission Prevention

The organization shall ensure proper ventilation is in place to prevent accumulation of hazardous gases or vapors resulting from equipment operations, power systems, or battery backups.

3.19 EPC-19: Surge Protection Measures

The organization shall implement surge protection devices at critical power junctions and for high-value equipment to defend against voltage spikes and power surges.

3.20 EPC-20: Monitoring Equipment Calibration

The organization shall regularly calibrate environmental sensors and monitoring equipment to ensure accuracy in detecting threshold violations and environmental hazards.

3.21 EPC-21: Tamper Detection for Power & HVAC Panels

The organization shall implement tamper-evident controls and periodic inspections for HVAC control units, electrical panels, and circuit boxes within secured facility areas.

3.22 EPC-22: Remote Monitoring of Environmental Systems

The organization shall enable remote monitoring capabilities for environmental and power systems to allow offsite observation, alerting, and response actions where appropriate.

Section 4. Device Disposal & Destruction Procedures (DDD)

Improper disposal of information system components can result in unintended disclosure of sensitive data, regulatory noncompliance, and increased organizational risk. The Device Disposal & Destruction Procedures (DDD) control family ensures that all decommissioned devices—whether data-bearing or not—are properly sanitized, tracked, and disposed of through secure, documented, and policy-driven processes.

4.1 DDD-01: Disposal Policy Definition

The organization shall develop, document, and maintain a formal policy for the disposal and destruction of all IT assets, including media, storage devices, and equipment with potential data retention.

4.2 DDD-02: Data Sanitization Procedures

The organization shall implement data sanitization procedures prior to disposal or repurposing of devices, using methods consistent with NIST SP 800-88 or equivalent standards.

4.3 DDD-03: Media Type-Specific Sanitization Techniques

The organization shall define and apply sanitization techniques appropriate to the media type (e.g., degaussing for magnetic tapes, cryptographic erasure for SSDs, physical destruction for optical media).

4.4 DDD-04: Cryptographic Erasure Protocols

The organization shall utilize cryptographic erasure for systems employing full-disk encryption, ensuring keys are destroyed in a secure and irreversible manner prior to device disposal.

4.5 DDD-05: Asset Disposal Tracking

The organization shall track each asset through the disposal lifecycle, including unique asset identifiers, sanitization status, transfer logs, and final disposal or destruction confirmation.

4.6 DDD-06: Chain of Custody for Disposal

The organization shall maintain documented chain-of-custody procedures for assets from the point of decommissioning through final destruction or off-site handoff.

4.7 DDD-07: Secure Storage Pre-Destruction

The organization shall store decommissioned devices in a physically secure location until final sanitization and disposal can be completed, with access restricted to authorized personnel only.

4.8 DDD-08: Disposal Authorization Controls

The organization shall require written or system-based authorization prior to initiating disposal or destruction of organizational IT assets.

4.9 DDD-09: Third-Party Disposal Oversight

The organization shall assess, approve, and monitor third-party vendors involved in device disposal or destruction activities, ensuring contractual and regulatory compliance.

4.10 DDD-10: Certificate of Destruction (CoD) Collection

The organization shall require a Certificate of Destruction (CoD) from internal or third-party disposal services for all destroyed assets, capturing key destruction details and retaining for audit.

4.11 DDD-11: Onsite Destruction Procedures

The organization shall maintain the capability for onsite physical destruction of storage devices and other components when required by data sensitivity or operational risk.

4.12 DDD-12: Disposal Log Retention

The organization shall retain disposal and destruction logs, including sanitization evidence and CoDs, in accordance with records management and compliance requirements.

4.13 DDD-13: Witnessed Destruction Requirement for High-Risk Media

The organization shall require witnessed destruction—by designated personnel or security officials—for media classified as high-risk or containing sensitive regulated data.

4.14 DDD-14: Decommissioning Review Process

The organization shall conduct a review of each device’s classification, data sensitivity, and ownership prior to decommissioning to determine appropriate sanitization and destruction actions.

4.15 DDD-15: Labeling of Decommissioned Equipment

The organization shall affix standardized labels or tags to decommissioned assets indicating status (e.g., “Sanitized,” “Pending Destruction”), including date and responsible party.

4.16 DDD-16: Non-Functioning Device Handling Protocols

The organization shall define special handling procedures for non-functioning or damaged devices to ensure data remnants are addressed despite hardware limitations.

4.17 DDD-17: Environmental Compliance for Disposal

The organization shall dispose of hardware and electronic waste in a manner compliant with environmental regulations and industry best practices, including e-waste and hazardous material protocols.

4.18 DDD-18: Asset Recovery & Reuse Security Checks

The organization shall require security validation checks on sanitized assets prior to reuse, transfer, or donation to confirm no residual data remains.

4.19 DDD-19: Training on Sanitization & Disposal Procedures

The organization shall provide training to personnel involved in device disposal on applicable policies, methods, and legal/regulatory requirements for secure disposal.

4.20 DDD-20: Audit of Disposal Activities

The organization shall conduct periodic audits of disposal records, vendor performance, and destruction methods to ensure continued alignment with organizational policy and risk thresholds.

4.21 DDD-21: Incident Handling for Improper Disposal

The organization shall establish and maintain incident response procedures for cases of improper disposal, data leakage from disposed devices, or failure to sanitize.

4.22 DDD-22: Disposal Exception Handling

The organization shall document and approve any exceptions to standard sanitization or disposal procedures, including justifications, risk assessments, and compensating controls.

Section 5. Video Surveillance & Intrusion Detection (VID)

Video surveillance and physical intrusion detection systems are essential safeguards for proactively detecting, deterring, and documenting unauthorized physical activity. The Video Surveillance & Intrusion Detection (VID) control family ensures organizations deploy, manage, and maintain surveillance and detection capabilities to monitor access to facilities, protect assets, and support forensic investigations—while aligning with privacy, retention, and operational integrity requirements.

5.1 VID-01: Surveillance Coverage Requirements

The organization shall ensure video surveillance coverage is implemented at all building ingress/egress points, critical internal zones, and areas housing sensitive infrastructure or assets.

5.2 VID-02: Camera Placement Risk Analysis

The organization shall perform a documented risk analysis to determine optimal camera placement and coverage zones, minimizing blind spots and ensuring alignment with threat vectors.

5.3 VID-03: Intrusion Detection System Deployment

The organization shall deploy physical intrusion detection systems (e.g., motion sensors, door contact alarms, vibration sensors) in secure and restricted areas to detect unauthorized entry attempts.

5.4 VID-04: Real-Time Monitoring Capabilities

The organization shall maintain capabilities for real-time monitoring of surveillance and intrusion detection systems by designated security personnel or integrated security platforms.

5.5 VID-05: Video Retention Policies

The organization shall establish and enforce retention policies for video footage based on business need, regulatory requirements, and privacy considerations, ensuring secure deletion after the retention period expires.

5.6 VID-06: Surveillance System Access Controls

The organization shall implement role-based access controls to restrict access to live feeds, video archives, and system configuration settings to authorized personnel only.

5.7 VID-07: Tamper Detection for Surveillance Devices

The organization shall implement technical or physical measures to detect and alert for tampering or obstruction of surveillance cameras and intrusion detection equipment.

5.8 VID-08: Secure Storage of Surveillance Footage

The organization shall store all surveillance recordings in a secure environment, with encryption at rest and in transit where feasible, and access restricted by policy.

5.9 VID-09: Privacy Zoning and Masking

The organization shall configure surveillance systems to avoid or mask areas where surveillance may infringe on individual privacy or violate legal/contractual boundaries.

5.10 VID-10: Intrusion Event Logging and Alerts

The organization shall ensure that all intrusion detection events generate timestamped alerts and are logged for analysis, investigation, and audit.

5.11 VID-11: Surveillance System Time Synchronization

The organization shall synchronize surveillance system clocks with organizational time sources to maintain consistent and accurate timestamps across all security records.

5.12 VID-12: Surveillance Footage Auditability

The organization shall implement logging and auditing mechanisms to track access to surveillance footage and ensure accountability for viewing or exporting activities.

5.13 VID-13: Integration with Physical Access Control Systems (PACS)

The organization shall integrate video surveillance and intrusion detection systems with PACS to enable correlation between access events and corresponding video evidence.

5.14 VID-14: Surveillance System Maintenance Schedule

The organization shall maintain a preventative maintenance schedule for all video and intrusion detection systems, ensuring optimal performance and immediate repair of degraded components.

5.15 VID-15: Surveillance System Testing & Validation

The organization shall periodically test surveillance cameras, sensors, and alerting mechanisms to validate functionality, image clarity, recording accuracy, and intrusion detection reliability.

5.16 VID-16: Covert Surveillance Authorization

The organization shall require documented executive authorization and legal counsel review before implementing covert surveillance measures in any facility.

5.17 VID-17: Monitoring of Perimeter Zones

The organization shall deploy surveillance and intrusion detection systems at facility perimeter boundaries, including fences, gates, and building exteriors, to detect unauthorized approach or access attempts.

5.18 VID-18: Emergency Response Integration

The organization shall ensure surveillance and intrusion detection systems are integrated with emergency response protocols, enabling rapid verification of alerts and coordination with law enforcement or internal response teams.

5.19 VID-19: Camera Failover and Redundancy

The organization shall implement redundancy and failover capabilities for critical surveillance cameras and recording systems to maintain coverage during equipment failure or power loss.

5.20 VID-20: Third-Party Surveillance Restrictions

The organization shall prohibit or strictly regulate third-party control or monitoring of organizational surveillance systems, ensuring vendor access is logged, justified, and limited to the scope of service.

5.21 VID-21: Remote Surveillance Access Control

The organization shall implement safeguards to manage and secure remote access to surveillance systems, including multi-factor authentication and session logging for offsite monitoring.

5.22 VID-22: Post-Incident Video Review Protocols

The organization shall define and enforce procedures for reviewing surveillance footage and intrusion logs following security incidents, with findings documented for root cause analysis and corrective action.