

# Physical Network and Server Room Security Documentation

## 3.1. Purpose and Scope

This document outlines the critical physical security measures, stringent access control protocols, and essential environmental protections implemented for all World Bank server rooms, data centers, and associated physical network infrastructure rooms (e.g., Main Distribution Frames (MDFs), Intermediate Distribution Frames (IDFs)). The purpose of these documented controls is to ensure the ongoing confidentiality, integrity, and availability (CIA) of World Bank's core IT systems and the data they process. This is achieved by preventing unauthorized physical access, mitigating environmental threats, and protecting against physical damage or interference. This policy applies to all World Bank facilities housing such critical infrastructure globally. The compromise of a server room can lead to a catastrophic failure of network services and data breaches, regardless of other cybersecurity measures in place.

Our server rooms and data centers are the operational heart of World Bank, housing the critical systems and data that underpin our services to customers and our internal operations. Protecting these facilities physically is as crucial as our digital defenses. This document details the multi-layered security approach adopted by World Bank, drawing from established industry best practices and standards to create a resilient and secure environment.

## 3.2. Server Room Access Control Protocols

Access to World Bank server rooms and data centers is strictly controlled through a combination of technological measures, documented procedures, and personnel oversight:

- **Multi-Factor Authentication (MFA) for Entry:** All personnel requiring entry to server rooms must authenticate using a minimum of two distinct factors. This typically involves a bank-issued proximity access card (something you have) combined with either a unique Personal Identification Number (PIN) entered at a keypad (something you know) or a biometric verification such as fingerprint or iris scan (something you are). Single-factor access is prohibited.
- **Principle of Least Privilege:** Physical access to server rooms is granted on a strict "need-to-access" basis, aligned with the individual's job role and responsibilities. Generic or departmental access is not permitted. Each access request requires documented authorization from the individual's department head and final approval from IT Security or Data Center Management.
- **Comprehensive Access Logging:** All entry and exit events are meticulously logged by the access control system, capturing data fields as specified in the "Premises Access Log Policy and Procedures" (Document 1.1). This includes timestamps, individual

identifiers, access point, and authorization method. These audit trails are reviewed daily for anomalies and retained securely as per policy.

- **Authorized Personnel Lists:** IT Security and Data Center Management jointly maintain and review, at least quarterly, the lists of personnel authorized for access to each server room. Any changes (additions, removals due to role change or termination) must be formally requested and approved.
- **Visitor and Contractor Access Control:**
  - Non-World Bank personnel (visitors, contractors, vendors) are prohibited from unescorted access to server rooms.
  - All such individuals must be pre-approved by Data Center Management and IT Security, registered in the visitor management system, and issued temporary, restricted-access badges programmed only for the specific time and duration of their required visit.
  - They must be escorted at all times by an authorized World Bank employee from Data Center Operations or IT Security while within the server room. The escort is responsible for the visitor's/contractor's actions.
  - A log of all visitor/contractor entries, escorts, and purpose of visit is maintained. Access controls such as ID-based locks are standard, often supplemented by biometric scans and PINs for high-security data centers.
- **Emergency Access Procedures:** A documented procedure exists for granting emergency access to authorized emergency services personnel (e.g., fire department). This procedure prioritizes life safety but includes provisions for security escort if the situation allows and requires post-incident logging and review of access.
- **Physical Key Management:** The use of physical keys for server room access is minimized and restricted to override or backup scenarios. Any such keys are stored in secure key safes, with access strictly controlled through a sign-out/sign-in log, subject to regular audit by security.
- **Anti-Tailgating and Anti-Passback Measures:** Physical deterrents such as mantraps or full-height turnstiles are implemented at primary server room entrances where feasible. Access control systems are configured with anti-passback logic. Security awareness training emphasizes the responsibility of all authorized personnel to prevent tailgating.
- **Regular Access Review:** Periodic reviews (at least semi-annually) of all access permissions to server rooms are conducted by IT Security to ensure continued necessity and appropriateness.

The security of a server room relies not just on the strength of its doors and locks, but on a comprehensive access control process. This process integrates technology (MFA, biometric

scanners ), clear procedures (authorization workflows, escort policies), and human oversight (log reviews, challenging unbadged individuals). Even sophisticated technological controls can be circumvented if procedural discipline is lacking, for example, through tailgating. Therefore, World Bank emphasizes a layered defense where technology is reinforced by rigorous operational procedures and vigilant personnel.

### **3.3. Overview of Physical Network Security Zones (Conceptual)**

World Bank facilities employ a conceptual model of physical network security zones to segregate areas based on their sensitivity and the nature of the assets they contain. This layered security approach ensures that access controls become progressively stricter as one moves from public areas towards highly sensitive zones housing critical infrastructure. While detailed blueprints are confidential and not part of this general policy document, the conceptual zones include:

- **Zone 1: Public Access Areas:** Lobbies, reception areas, and public meeting rooms where visitors may be present with minimal restriction, though general surveillance is in place.
- **Zone 2: General Office Areas:** Workspaces for general employees. Access is typically controlled by standard employee badges. Network jacks in these areas provide access to the general corporate network.
- **Zone 3: Secure Operations Zones:** Areas housing specialized operational teams or sensitive but not top-tier critical IT infrastructure (e.g., departmental servers, specialized labs). Access is more restricted, often requiring departmental authorization in addition to a standard badge.
- **Zone 4: Data Centers and Primary Network Rooms (MDFs/IDFs):** These are highly restricted zones housing core servers, storage, network equipment, and critical telecommunications links. Access is governed by the stringent protocols detailed in this document (Section 3.2 and 3.4). These areas are physically hardened.
- **Zone 5: High-Security Vaults/Specialized Compartments:** Within data centers or other secure locations, these zones may house cryptographic key management hardware, highly classified data processing, or critical backup media. Access is extremely limited to a few named individuals and requires multiple layers of authentication and often dual control.

This zoning strategy helps in applying appropriate levels of security controls commensurate with the risk and value of the assets within each zone, forming a defense-in-depth physical security architecture.

### **3.4. Critical Server Room Security Features Documentation**

World Bank server rooms and data centers are equipped with a range of critical security features designed to protect against unauthorized access, environmental hazards, and service disruptions. These features are documented, regularly inspected, and tested:

- **Surveillance (CCTV):**

- Comprehensive CCTV coverage is installed at all server room entry and exit points, within the server room covering equipment aisles and individual racks (where appropriate and respecting privacy for personnel), and along the external perimeter of the data center facility.
- Cameras are equipped with low-light IR capability, motion detection, and are strategically positioned to eliminate blind spots.
- Recordings are digitized, timestamped, and retained for a minimum of 90 days, with longer retention for specific incident-related footage. Access to recordings is restricted to authorized security personnel.

- **Environmental Monitoring and Control:**

- A network of sensors continuously monitors critical environmental parameters including temperature, humidity, water presence (leak detection under raised floors and near cooling units), and airflow.
- Acceptable operating ranges are defined (e.g., Temperature: 20-22°C (68-72°F); Relative Humidity: 40-55%).
- Automated alerts are triggered and sent to Data Center Operations staff and the Security Operations Center (SOC) if parameters deviate from predefined thresholds.
- HVAC (Heating, Ventilation, and Air Conditioning) systems are redundant and designed to maintain optimal operating conditions for IT equipment.

- **Fire Detection and Suppression:**

- Multi-stage fire detection systems are employed, including Very Early Smoke Detection Apparatus (VESDA) or aspirating smoke detectors for incipient fire detection, supplemented by traditional photoelectric and ionization smoke detectors.
- Gaseous fire suppression systems (e.g., Novec 1230, FM-200, or similar clean agents) are installed to extinguish fires without damaging sensitive electronic equipment. Water-based sprinkler systems (dry-pipe or pre-action) may exist as a secondary system or as required by local code but are not the primary suppression method within the server whitespace.

- Systems are regularly inspected, tested, and certified according to manufacturer recommendations and local fire codes. Test schedules and results are documented.

- **Power Redundancy and Conditioning:**

- Dual power feeds (A and B feeds) from independent Power Distribution Units (PDUs) are provided to server racks and critical equipment to support redundant power supplies in devices.
- Enterprise-grade Uninterruptible Power Supplies (UPS) provide conditioned power and sufficient battery runtime to allow for graceful shutdown of systems or to bridge the gap until backup generators are operational.
- Backup diesel generators with Automatic Transfer Switches (ATS) are in place to provide long-term power during utility outages. Fuel levels and generator readiness are regularly checked and documented.
- Regular, documented testing of UPS systems (load tests, battery health) and generator systems (auto-start, load assumption) is mandatory.

- **Physical Construction and Hardening:**

- Server rooms are constructed with reinforced walls, ceilings, and heavy-duty, self-closing, and locking doors.
- There are no exterior windows directly into server room whitespace. Any necessary internal windows (e.g., to a control room) are made of shatter-resistant materials.
- Physical barriers and secure pathways are established for network and power cabling.

- **Secure Cable Management:**

- Network and power cables are neatly routed in secure overhead cable trays or under raised flooring systems to prevent accidental damage, tripping hazards, or unauthorized tampering.
- Fiber optic and copper data cables are physically separated from power cables to minimize electromagnetic interference where practical.
- All cables (power, network, console) are clearly labeled at both ends with source and destination information according to World Bank standards.

- **Server Rack Security:**

- All server racks are individually lockable cabinets. Rack doors must be kept locked unless authorized personnel are actively working on the equipment within.

- Policies are in place for securing unused rack U-space with blanking panels to maintain proper airflow and deter unauthorized access.
- **Emergency Lighting:** Battery-backed emergency lighting is installed throughout server rooms and access/egress paths to ensure visibility during power outages or emergencies.
- **Policy on Combustibles and Liquids:** A strict policy prohibits the storage of combustible materials (e.g., cardboard boxes, paper) and unnecessary liquids within server rooms. Any chemicals or liquids required for specialized equipment maintenance are stored and handled according to safety data sheets (SDS) and bank policy.

The simple existence of these features is insufficient; their operational readiness is paramount. Therefore, World Bank mandates not only the installation of these security measures but also their rigorous documentation, regular testing schedules, and continuous monitoring. For example, a state-of-the-art fire suppression system offers no protection if its maintenance is overdue or its activation status is unknown. Documenting the specific type of system, its prescribed test frequency, the date of the last successful test, and continuous system health monitoring transforms a list of features into a verifiable and manageable component of the overall physical security program. This level of detail is crucial for internal audits, regulatory compliance, and ensuring the resilience of World Bank's critical IT infrastructure.

### **3.5. Maintenance and Emergency Procedures for Physical Infrastructure**

Robust procedures for both scheduled maintenance and emergency situations are essential to ensure the continued security and availability of server room infrastructure:

- **Scheduled Maintenance Windows:**
  - All planned maintenance activities within server rooms (e.g., HVAC system servicing, electrical system upgrades, server hardware installations/decommissioning, network equipment changes) must be scheduled in advance through the World Bank change management system.
  - Work orders detailing the scope, timing, personnel involved, and potential impact must be approved by Data Center Management and, if significant, by IT Security.
  - Access for maintenance personnel (internal or external) will be granted according to the protocols in section 3.2.
- **Emergency Maintenance:**
  - Procedures are defined for unscheduled, emergency maintenance required to address critical failures (e.g., cooling unit malfunction, UPS failure).

- Emergency maintenance requires verbal or system-logged approval from senior Data Center Management or IT leadership.
- Security escort and oversight are mandatory for external vendors performing emergency work. All actions taken are to be documented post-event.
- **Emergency Power Off (EPO) System:**
  - Clearly marked EPO buttons or systems are installed at strategic locations within and outside server rooms.
  - The use of EPO is restricted to extreme emergency situations posing an immediate threat to life safety or catastrophic equipment damage (e.g., uncontrolled fire, major flooding directly impacting live electrical gear).
  - Activation of EPO requires, where feasible, verbal confirmation from at least two authorized senior personnel due to its significant operational impact. Procedures for system recovery post-EPO activation are documented.
- **Incident Response for Physical Events:**
  - Specific incident response plans are documented for various physical events, including:
    - Water leaks or flooding (e.g., activation of water sensors, notification to Facilities and Data Center Ops, equipment shutdown if necessary).
    - Fire (e.g., smoke detector activation, automated fire suppression deployment, personnel evacuation, notification to fire department and SOC).
    - Power failure (e.g., UPS activation, generator start-up, monitoring of critical systems, controlled shutdown if power cannot be restored within UPS runtime).
    - Unauthorized access attempts or physical intrusion (e.g., alarm activation, SOC notification, security patrol dispatch, law enforcement contact if needed).
  - These plans define roles and responsibilities for Data Center Operations staff, Physical Security teams, Facilities Management, and the SOC.
- **Evacuation Plans:**
  - Clear, well-lit emergency evacuation routes are prominently posted within all server rooms and data centers, indicating primary and secondary exits and assembly points.
  - Regular evacuation drills are conducted, including personnel working in data center environments.

- **Emergency Contact Lists:**

- Up-to-date emergency contact lists are maintained and readily accessible (both physically in secure locations and digitally) for all relevant internal teams (Data Center Ops, Security, Facilities, IT Management) and critical external service providers (e.g., local fire and police departments, HVAC maintenance vendor, primary power utility company, generator service company). These lists are reviewed and updated quarterly.

Unexpected events are inevitable in complex environments like data centers. World Bank's documented maintenance and emergency procedures are designed to ensure a swift, coordinated, and effective response to minimize downtime, protect assets, and ensure personnel safety, whether the event is a critical cooling system failure or a security breach attempt.

### **3.6. Actionable Items and Examples for Simulation**

The following items can be used to create realistic scenarios and test understanding of physical network and server room security policies in a simulation:

1. **Server Room Entry Rule:** "No food or drink of any kind is permitted inside the controlled perimeter of any World Bank server room or data center at any time."
2. **Procedure:** "All tools, equipment, and portable electronic devices (including personal mobile phones unless explicitly authorized for work purposes within the server room) belonging to vendors or contractors must be logged in with security personnel upon entry and logged out upon exit from the server room. Spot checks may be conducted."
3. **CCTV Policy:** "CCTV recordings covering server room access points, critical aisles, and equipment areas are retained for a minimum of 120 days. Access to live feeds and recordings is restricted to authorized Security and Data Center Management personnel and logged."
4. **Environmental Alert Scenario (Simulation):** The SOC receives an automated alert: "Server Room 2 - Main Aisle - Temperature High: 28°C. Upper Threshold: 24°C. CRAC Unit 3B showing fault." *Simulation Task: What are the immediate actions for the SOC and Data Center Operations team based on documented procedures?*
5. **Fire Suppression System Test:** "The Novec 1230 fire suppression system in Data Center 1, Bay C, is scheduled for its quarterly integrity test and agent level check on. Notification to be sent to all personnel with access."
6. **UPS System Test:** "Monthly automated load test of UPS system SRV1-UPS-A is scheduled. Data Center Operations to monitor battery health indicators and runtime calculations."



7. **Backup Generator Test:** "Weekly auto-start test for backup generator DG-01 is logged. Monthly full-load transfer test is scheduled for the first Saturday of each month, outside of critical processing windows."
8. **Access Request Form Field:** "Justification for Server Room Access: Provide a detailed description of the work to be performed, specific racks/servers to be accessed, and estimated duration of access. (Change Request # or Incident Ticket # must be included)."
9. **Escort Policy Enforcement:** "All non-Data Center Operations staff (e.g., application developers, project managers) requiring temporary access to a server room must be continuously escorted by an authorized Data Center team member. The escort is responsible for ensuring the visitor adheres to all server room policies."
10. **Emergency Power Off (EPO) Procedure Detail:** "EPO system activation requires verbal confirmation from two authorized senior personnel (e.g., Data Center Manager and IT Operations Director), documented via recorded line if possible, except in cases of immediate and obvious life safety risk (e.g., visible arcing, fire involving electrical equipment)."
11. **Network Cable Labeling Standard:** "All network cables (copper and fiber) must be clearly labeled at both ends with a unique identifier that corresponds to documentation detailing source and destination port, device, and patch panel information, adhering to TIA-606-C standards."
12. **Server Rack Security Policy:** "All server rack doors (front and rear) must be kept locked when unattended by authorized personnel actively working on the equipment within that rack. Keys to racks are managed by Data Center Operations."
13. **Maintenance Log Entry Example:** "HVAC Unit SR1-AC3: Routine quarterly maintenance performed. Filters replaced, coolant levels checked, belts inspected. System operating within normal parameters. Next scheduled service: . Work Order: WO12345."
14. **Incident Scenario (Simulation):** A water leak sensor is triggered under Raised Floor Tile F-27 in Server Room 3, adjacent to critical SAN storage arrays. *Simulation Task: Detail the first three steps of the documented emergency procedure for Data Center Operations.*
15. **Security Drill Scenario (Simulation):** "World Bank Security will conduct an unannounced drill simulating an unauthorized individual attempting to tailgate into the main data center during a shift change." *Simulation Task: How should authorized personnel and security guards respond according to policy?*
16. **Policy Statement:** "Photography, video recording, and audio recording within World Bank server rooms are strictly prohibited without explicit, prior written permission from

IT Security Management and Data Center Management. Any approved recording must be supervised."

17. **Procedure (Clean Environment):** "A 'clean desk/clear screen' policy is strictly enforced for all workstations, crash carts, and temporary staging areas located within the server room environment. No unnecessary paper, manuals, or personal items are to be left out."

18. **Physical Intrusion Detection:** "Motion sensors and door contact alarms are active on all server room entry/exit points and are monitored 24/7 by the SOC. Any unauthorized activation triggers an immediate security response."

19. **Equipment Installation/Removal:** "All IT equipment (servers, network devices, storage) being installed or removed from a server room must be documented in the asset management system, and the process must be coordinated with Data Center Operations to ensure power, cooling, and space allocations are appropriate. Serial numbers are recorded."

20. **Policy Review:** "This Physical Network and Server Room Security Documentation shall be reviewed annually by IT Security and Data Center Management, and updated as necessary to reflect changes in technology, threats, or business requirements."

3.7. Table: Server Room Security Measures and Monitoring

This table provides a structured overview of key physical and environmental security measures implemented in World Bank server rooms, detailing how each is monitored to ensure ongoing effectiveness. This is crucial for understanding the continuous effort required to maintain a secure and resilient data center environment.

Security Measure/Control	Detailed Description	Monitoring Frequency/Method	Responsible Team(s)	Last Test/Audit Date (Example)
Access Control System (ACS)	Multi-factor (Badge + PIN/Biometric) at all entries; Anti-passback; Door position sensors.	Continuous electronic logging; Daily log review for anomalies; Quarterly access list audit.	Physical Security, Data Center Ops	2024-09-15 (Audit)
CCTV Surveillance	High-resolution IP cameras with IR, motion detection covering entries, exits, aisles, critical equipment.	Continuous 24/7 recording; Real-time monitoring by SOC for key areas; Weekly spot checks of recordings; Monthly camera function test.	Physical Security, SOC	2024-10-01 (Function Test)
Temperature Monitoring	Redundant sensors per zone/aisle; Target 20-22°C.	Real-time monitoring via Building Management System (BMS)/DCIM; Automated alerts for deviations >2°C.	Data Center Ops, Facilities	N/A (Continuous)

<b>Humidity Monitoring</b>	Redundant sensors per zone; Target 40-55% RH.	Real-time monitoring via BMS/DCIM; Automated alerts for deviations >5% RH.	Data Center Ops, Facilities	N/A (Continuous)
<b>Water Leak Detection</b>	Rope/spot sensors under raised floors, near CRAC units, and liquid-cooled racks.	Real-time monitoring via BMS/DCIM; Automated alerts upon detection. Weekly visual inspection.	Data Center Ops, Facilities	2024-10-20 (Visual Insp.)
<b>Fire Detection System</b>	VESDA/Aspirating smoke detectors; Photoelectric/Ionization detectors. Integrated with BMS and suppression system.	Continuous system health monitoring; Semi-annual professional testing and certification.	Data Center Ops, Facilities, Fire Vendor	2024-07-10 (Cert.)
<b>Fire Suppression System</b>	Novec 1230 / FM-200 gaseous clean agent system.	Continuous pressure/agent level monitoring; Semi-annual professional inspection and certification.	Data Center Ops, Facilities, Fire Vendor	2024-07-10 (Cert.)
<b>Uninterruptible Power (UPS)</b>	2N or N+1 redundant UPS systems; Min. 15-min runtime at full load.	Real-time status monitoring (load, battery health, runtime); Monthly automated self-test; Annual full battery discharge test.	Data Center Ops, Electrical Vendor	2024-09-05 (Annual Test)
<b>Backup Generator(s)</b>	Diesel generators with ATS; Sufficient fuel for 72hrs+ operation.	Weekly auto-start test (no load); Monthly load test; Annual full building load test. Fuel levels checked weekly.	Data Center Ops, Facilities, Gen Vendor	2024-10-15 (Monthly Load)
<b>Physical Intrusion Detection</b>	Motion sensors within server room (armed during off-hours); Door contact alarms on all doors.	24/7 monitoring by SOC; Alarms trigger immediate response. Quarterly sensor test.	Physical Security, SOC	2024-08-20 (Sensor Test)
<b>Rack Security (Locks)</b>	Lockable front and rear doors on all server cabinets.	Daily visual inspection by Data Center Ops during walkthroughs to ensure doors are secured.	Data Center Ops	N/A (Daily Visual)
<b>Emergency Lighting</b>	Battery-backed emergency lights for egress paths and key areas.	Monthly functional test (30-second); Annual full duration test (90-minute).	Facilities	2024-10-01 (Monthly Test)