

# Premises Access Log Policy and Procedures

## 1.1. Purpose and Scope

This policy establishes clear guidelines for the recording, reviewing, and managing of access to all World Bank premises. The primary objectives are to prevent unauthorized entry, protect World Bank assets (including information assets), and ensure the safety of all personnel. It is a foundational principle that cybersecurity efforts can be undermined if physical access is not rigorously controlled; an intruder gaining physical access could bypass numerous digital defenses. This policy applies to all individuals requiring access to any World Bank facility, including employees, contractors, vendors, visitors, and emergency responders. It covers all World Bank owned or leased properties, such as corporate headquarters, branch offices, operational centers, and data centers. The procedures outlined herein are aligned with best practices, including those suggested by ISO 27001 Annex A.11 concerning Physical and Environmental Security.

A comprehensive access logging system is a first line of defense and a critical source of information during any physical security investigation. A breach of physical security can render even the most sophisticated cyber defenses useless, making meticulous access control and logging paramount.

## 1.2. Standard Data Fields for Access Logs

To ensure that access logs are comprehensive and useful for security monitoring, investigation, and compliance, all physical access control systems and manual logs at World Bank must capture the following standard data fields for each access event:

- **Log ID:** A unique sequential or system-generated identifier for each individual log entry, ensuring traceability.
- **Date of Access:** The full date of the access attempt or event (Format: YYYY-MM-DD).
- **Time In:** The precise time of entry into the premises or secured area (Format: HH:MM:SS, 24-hour).
- **Time Out:** The precise time of exit from the premises or secured area (Format: HH:MM:SS, 24-hour). This is critical for tracking visitor presence and ensuring areas are clear.
- **Full Name of Individual:** The complete legal name of the person accessing the facility, as verified against official identification for visitors and contractors, and as per employee records.
- **Employee ID / Visitor ID / Contractor ID:** The unique identification number assigned by World Bank (for employees and long-term contractors) or a temporary ID issued to visitors.

- **Organization/Department:** The individual's affiliated organization (e.g., vendor company name) or their internal department if an employee.
- **Escort Name & ID (if applicable):** The full name and employee ID of the World Bank employee escorting a visitor or contractor in areas where escorts are mandatory.
- **Access Point/Location:** A specific, unambiguous identifier for the physical point of access (e.g., "Main Lobby Entrance," "Data Center SRV1-North Door," "Branch 105 - Vault Anteroom," "Parking Garage Level 2 Elevator").
- **Purpose of Visit/Access:** A concise but clear statement of the reason for entry (e.g., "Scheduled Client Meeting," "Server Hardware Replacement," "Routine Branch Operations," "Fire Alarm System Test," "Emergency Medical Assistance").
- **Authorization Method:** The method used to gain access (e.g., "Badge Swipe," "Biometric Scan (Fingerprint)," "Keypad PIN Entry," "Manual Sign-in by Security," "Remote Unlock by SOC").
- **Authorization Grantor (if manual/remote):** The name and ID of the security personnel or authorized manager who approved a manual entry or remote unlocking of an access point.
- **Badge Number Issued (for visitors/temporary):** The unique number of the temporary access badge issued.
- **Asset Carried In/Out (if applicable):** A description of any significant assets being brought into or removed from the facility (e.g., "Laptop SN: WB12345," "Server Chassis SN: SRV987," "Sealed Document Package," "No significant assets"). This is particularly important for data centers and sensitive areas.
- **Log Entry Timestamp:** An automated, system-generated timestamp indicating when the log record itself was created or captured in the system.
- **Security Officer on Duty:** The name or ID of the security officer responsible for the specific access point or zone at the time of the event, if applicable.

The granularity and accuracy of these data fields are fundamental. They directly influence the effectiveness of logs for forensic analysis, compliance reporting, and the potential for automated anomaly detection. For instance, fields like "Purpose of Visit," "Authorization Method," and "Asset Carried In/Out" provide critical context. This context can help distinguish normal activity from suspicious deviations, such as an employee accessing a data center outside of typical business hours with an unusual "Purpose of Visit" while carrying out undocumented assets. Such detailed logs are essential for both manual reviews by security personnel and for feeding into advanced analytical tools, including machine learning systems designed to detect anomalous behavior. Financial institutions are mandated to maintain detailed access logs to facilitate audit trails and ensure compliance with security policies.

### 1.3. Access Log Procedures (Employee, Visitor, Contractor, Maintenance, Emergency)

Specific procedures govern access for different categories of personnel to ensure appropriate levels of security and accountability:

- **Employees:**

- Employees are granted access to World Bank premises and relevant internal zones based on their role and responsibilities, primarily via their issued employee identification badge.
- All badge swipes at readers are automatically logged with the fields specified in document Mobile and Portable Device Security Policy.
- Lost or stolen badges must be reported immediately to the Security Department, as per the Mobile and Portable Device Security Policy. The lost badge will be deactivated, and a new one issued.
- Access to high-security zones or access outside of standard business hours may require pre-approval from a manager or adherence to specific departmental protocols, with such approvals noted or linked in the access log system where feasible.

- **Visitors:**

- All visitors must pre-register or register upon arrival at a designated reception/security desk.
- Visitors must present a valid government-issued photo identification for verification.
- Upon successful verification, visitors will be issued a temporary, uniquely numbered visitor badge, which must be visibly worn at all times while on World Bank premises.
- All visitor details, including name, organization, purpose of visit, World Bank host, and badge number, will be logged.
- Visitors requiring access beyond public reception areas must be escorted by an authorized World Bank employee in most areas, and mandatorily in sensitive zones like data centers or trading floors. The escort's details are logged.
- Upon departure, visitors must sign out and return their temporary badge to security/reception.

- **Contractors/Vendors:**

- Contractors and vendors requiring regular access will undergo a vetting process and may be issued time-limited access badges specific to their work areas and approved hours.

- Access for specific projects or short-term work requires pre-registration by the sponsoring World Bank department, including verification of work orders or contractual agreements.
- All contractor access is logged, detailing the company, purpose, and specific areas accessed.
- Tools and equipment brought onto or removed from premises by contractors may be subject to inspection and logging, particularly in sensitive areas.
- **Maintenance Personnel (Internal/External):**
  - Access for maintenance personnel (both World Bank staff and external vendors) follows similar protocols to contractors, with stringent controls for access to critical infrastructure areas like server rooms, electrical rooms, or telecommunication closets.
  - Purpose of maintenance, systems affected, and expected duration must be logged. Access to sensitive areas like server rooms is strictly controlled and requires explicit authorization, often with supervision.
- **Emergency Responders (Police, Fire, Medical):**
  - Procedures are in place to facilitate expedited access for legitimate emergency responders. Security personnel will prioritize life safety and emergency mitigation.
  - Where possible, responders will be logged in by security. If immediate entry is paramount, security will log details retrospectively as soon as feasible.
  - Security personnel will attempt to escort emergency responders if the situation permits and it does not impede their emergency duties.
  - A post-incident review will reconcile access records and actions taken.

These differentiated procedures ensure that while access is facilitated according to need, it is always controlled and logged, aligning with best practices for securing premises and managing entry to sensitive areas.

#### **1.4. Review, Audit, and Retention of Access Logs**

The collection of access log data is only effective if coupled with robust review, audit, and retention processes. World Bank implements the following:

- **Daily Review:** On-duty security personnel at key facilities (e.g., data centers, corporate headquarters) perform daily reviews of access logs. This includes checking for immediate anomalies such as multiple consecutive failed access attempts at a single point, door-forced-open alarms, tailgating alerts from integrated CCTV analytics, or discrepancies in visitor sign-out times.

- **Weekly Supervisory Review:** Security shift supervisors or site security managers conduct a weekly review of summarized access activity. This review focuses on access to sensitive areas (e.g., data centers, vaults, executive floors), after-hours access patterns, and any unresolved anomalies from daily reviews.
- **Monthly Audit:** The World Bank Security Management team conducts a formal monthly audit of access logs. This audit involves:
  - Cross-referencing log data with visitor pre-registration lists, contractor work schedules, and employee after-hours access approvals.
  - Verifying the correct functioning of logging systems and the accuracy of data capture.
  - Assessing compliance with access control procedures (e.g., escort policies, badge issuance).
  - Identifying any systemic issues or patterns requiring policy adjustment or further investigation. This aligns with the necessity for regular security audits mentioned in physical security policy frameworks.
- **Log Retention Period:** All physical access logs, whether electronic or manual, shall be retained for a minimum period of three (3) years. This period may be extended based on specific regulatory requirements (e.g., PCI DSS , banking regulations) or ongoing investigations. This meets or exceeds general recommendations for data center access log retention.
- **Secure Storage and Access Control:** Access logs are stored in a secure, centralized electronic system with strong access controls. Only authorized security personnel and auditors have access to view or query log data. Any access to the log data itself is audited to ensure integrity and prevent tampering.
- **System Integrity Checks:** Automated checks and regular manual verifications are performed to ensure that all access control points are correctly transmitting log data and that the logging systems are functioning as intended.

Maintaining detailed access logs is a critical compliance requirement for financial institutions, facilitating audit trails and adherence to security policies. The process of gathering access logs is also a key preparatory step for any comprehensive physical security audit. The multi-tiered review process (daily, weekly, monthly) is designed not just for reactive investigation but also for proactive identification of patterns that might precede a security incident, such as an employee testing access limits or a contractor attempting unauthorized entry to restricted zones. This proactive stance allows for timely intervention and refinement of access policies.

## 1.5. Incident Reporting and Investigation for Access Anomalies

Prompt and effective response to access anomalies is crucial for maintaining physical security. World Bank defines access anomalies and the procedures for addressing them as follows:

- **Definition of Access Anomalies:** An access anomaly is any access event or pattern that deviates from established policies, expected behavior, or authorized permissions. Examples include, but are not limited to:
  - Repeated unauthorized access attempts at any access point.
  - Successful access to an area for which the individual is not authorized.
  - Access outside of permitted hours or days without prior approval.
  - Alarms triggered by access control systems (e.g., door forced open, door held open too long, anti-passback violation).
  - Tailgating incidents, whether observed directly or via CCTV/sensor alerts.
  - Use of a lost, stolen, or cloned access badge.
  - Discrepancies in visitor or contractor log-in/log-out records.
  - Attempts to tamper with access control hardware (readers, locks, sensors).
- **Immediate Reporting Protocol:**
  - Security personnel witnessing an anomaly or receiving an automated alert must immediately report the event to the on-site Security Supervisor and the central Security Operations Center (SOC) or designated Head of Security.
  - Employees observing suspicious access behavior are required to report it to the Security Department promptly.
- **Initial Investigation Steps:**
  - **Verification:** Verify the identity of the individual(s) involved, if present.
  - **Authorization Check:** Confirm the individual's authorization status for the specific access point and time via the access control system and any pre-approval records.
  - **CCTV Review:** Immediately review relevant CCTV footage corresponding to the time and location of the anomalous log entry or alarm.
  - **Interview:** If the individual is apprehended or available, conduct a brief interview to understand the circumstances (while adhering to HR guidelines).
  - **System Check:** Verify the operational status of the involved access control hardware and software.
- **Escalation Matrix:**

- Minor anomalies (e.g., accidental single wrong badge swipe by an authorized employee) may be resolved and documented at the local security level.
- Repeated anomalies, unauthorized access to sensitive areas, suspected malicious intent, or any anomaly involving potential data compromise will be immediately escalated to Security Management.
- Further escalation to Human Resources, Legal Department, or law enforcement will be determined by Security Management based on the severity and nature of the incident.
- **Documentation:** All reported access anomalies, investigation steps, findings, and resolutions must be meticulously documented in the World Bank incident reporting system. The report must reference the specific access log entry IDs, CCTV footage timestamps, and any other relevant evidence. This documentation is crucial for trend analysis, policy improvement, and potential disciplinary or legal actions, aligning with best practices for incident management.
- **Use Cases for Simulation:**
  - **Use Case 1 (Suspicious - Potential Insider Threat):** Log entry shows Employee ID E54321 (John Carter, Marketing Department) attempting to badge into Data Center Zone B (highly restricted) at 11:30 PM on a Friday. Access is denied. John Carter has no authorized access to any Data Center zone. *Investigation:* Review John Carter's access history, his current role responsibilities, CCTV of the attempt, and interview him regarding the reason for the attempt.
  - **Use Case 2 (Incident - Forced Entry):** Access log shows "Door Forced Open Alarm" for "Emergency Exit 3 - West Wing" at 02:05 AM. No corresponding authorized badge swipe is logged immediately before or after. *Investigation:* Dispatch security patrol, review CCTV covering Exit 3, check perimeter integrity, and notify local law enforcement if intrusion is confirmed.
  - **Use Case 3 (Visitor Anomaly - Potential Data Theft):** Visitor Sarah Miller (Temp Badge V0789, escorted by E001122) was logged out at 16:45. At 17:15, Temp Badge V0789 is recorded attempting access to the R&D Lab (a zone she was not authorized for during her visit). *Investigation:* Confirm badge V0789 was physically returned. Review CCTV of R&D Lab entrance and visitor exit points. Interview escort E001122. Check if any assets are missing from the R&D Lab.

Rapid and thorough investigation of access anomalies is key to preventing minor issues from escalating into significant security breaches. World Bank's access logs serve as a primary investigative tool, providing the initial data points to understand and reconstruct any physical security event.

## 1.6. Actionable Items and Examples for Simulation

The following items provide concrete examples and procedural points that can be used in a cybersecurity simulation scenario focused on physical access control at World Bank:

1. **Log Entry Example (Authorized Employee - Normal Hours):** LOGID: 202410260001, DATE: 2024-10-26, TIME\_IN: 08:55:03, TIME\_OUT: 17:02:11, NAME: Alice Wonderland, EMPL\_ID: E00789, ORG\_DEPT: IT Department, ESCORT: N/A, ACCESS\_PT: Main Office Entrance 1, PURPOSE: Routine Work, AUTH\_METHOD: Badge Swipe, AUTH\_GRANTOR: N/A, VISITOR\_BADGE: N/A, ASSET\_IO: N/A, LOG\_TS: 2024-10-26 08:55:03, OFFICER\_ID: SO\_001
2. **Log Entry Example (Authorized Visitor - Escorted):** LOGID: 202410260002, DATE: 2024-10-26, TIME\_IN: 09:30:15, TIME\_OUT: 11:05:00, NAME: Bob The Builder, VISITOR\_ID: V01234, ORG\_DEPT: External Consultant Inc., ESCORT: Alice Wonderland (E00789), ACCESS\_PT: Main Office Entrance 1, PURPOSE: Meeting with IT Dept, AUTH\_METHOD: Manual Sign-in, AUTH\_GRANTOR: SO\_001, VISITOR\_BADGE: B0678, ASSET\_IO: Laptop SN: ABC123, LOG\_TS: 2024-10-26 09:30:15, OFFICER\_ID: SO\_001
3. **Log Entry Example (Denied Access - After Hours, Suspicious):** LOGID: 202410270003, DATE: 2024-10-27, TIME\_IN: 02:10:45, TIME\_OUT: N/A, NAME: Charles Xavier, EMPL\_ID: E00123, ORG\_DEPT: Research, ESCORT: N/A, ACCESS\_PT: Data Center Zone A, PURPOSE: Access Denied - After Hours/Unauthorized, AUTH\_METHOD: Badge Swipe, AUTH\_GRANTOR: N/A, VISITOR\_BADGE: N/A, ASSET\_IO: N/A, LOG\_TS: 2024-10-27 02:10:45, OFFICER\_ID: SO\_002
4. **Log Entry Example (Maintenance Contractor - Scheduled):** LOGID: 202410260004, DATE: 2024-10-26, TIME\_IN: 10:00:00, TIME\_OUT: 16:30:00, NAME: David Copperfield, CONTRACTOR\_ID: C00567, ORG\_DEPT: HVAC Services Ltd., ESCORT: N/A (Supervised Access), ACCESS\_PT: Server Room 1, PURPOSE: Scheduled HVAC Maint., AUTH\_METHOD: Badge Swipe (Temp), AUTH\_GRANTOR: SO\_001, VISITOR\_BADGE: B0679, ASSET\_IO: Toolbox, Ladder, LOG\_TS: 2024-10-26 10:00:00, OFFICER\_ID: SO\_001
5. **Log Entry Example (Forced Door Alarm - Incident):** LOGID: 202410270005, DATE: 2024-10-27, TIME\_IN: 03:15:22, TIME\_OUT: N/A, NAME: SYSTEM\_ALERT, EMPL\_ID: N/A, ORG\_DEPT: N/A, ESCORT: N/A, ACCESS\_PT: Loading Dock Door 3, PURPOSE: Forced Entry Alarm, AUTH\_METHOD: Sensor\_Trip, AUTH\_GRANTOR: N/A, VISITOR\_BADGE: N/A, ASSET\_IO: N/A, LOG\_TS: 2024-10-27 03:15:22, OFFICER\_ID: SOC\_AUTOMATED
6. **Procedure:** All visitors must present a valid, government-issued photo ID for identity verification by security personnel before a temporary access badge is issued. Copies are not accepted.
7. **Procedure:** Employees must report a lost or stolen employee badge to the World Bank Security Department via the emergency hotline (Ext. 7777) or the online security portal within one (1) hour of discovering its absence.



8. **Procedure:** Access to data centers between 10:00 PM and 6:00 AM local time, or on weekends/holidays, requires dual authorization (e.g., approved access request in the system plus valid badge swipe and PIN/biometric verification).
9. **Log Review Checklist Item (Daily):** "Verify all 'Time Out' entries for temporary visitor badges issued the previous day. Investigate any badges not returned or missing 'Time Out' entries by cross-referencing with host sign-off."
10. **Log Review Checklist Item (Weekly):** "Cross-reference after-hours access logs for sensitive areas (Data Centers, Treasury) with pre-approved access lists or emergency work orders. Flag and investigate all discrepancies."
11. **Use Case (Suspicious Activity for Simulation):** An access log shows an employee badge, which was reported lost two days prior by its owner, being successfully used to enter a low-security area like the employee cafeteria. *Simulation Task: What actions should the SOC analyst take?*
12. **Use Case (Tailgating Incident for Simulation):** CCTV footage linked to an access log shows an authorized employee (Employee A) badging in, and another individual (Employee B, whose badge was declined seconds earlier at the same reader) closely following Employee A through the door without badging. *Simulation Task: Document the incident and recommend corrective actions for Employee A and B.*
13. **Policy Statement:** Physical access logs, both electronic and any supporting manual logs, shall be retained securely for a minimum of three (3) years to meet regulatory audit requirements and support forensic investigations.
14. **Procedure:** Security guards must physically verify the identity of any individual requesting manual entry due to a "forgotten badge" against the employee database. The event must be logged with the authorizing supervisor's approval noted. Repeated requests from the same individual will be flagged to HR and Security Management.
15. **Example of an "Asset Carried Out" Log Detail:** "Server Hard Drive SN: XYZ789, Model: Seagate Exos 16TB. Authorized for secure disposal by J. Smith (IT Manager, Ticket #INC0012345)."
16. **Procedure:** During declared emergency evacuations, security personnel will prioritize life safety. While precise logging of every individual's exit may not be feasible, attempts will be made to account for personnel at designated muster points. A post-event reconciliation of who was on-site versus who evacuated will be conducted.
17. **Log Review Checklist Item (Monthly):** "Analyze access patterns for employees who have recently changed roles or departments to ensure their access rights have been updated appropriately and old permissions revoked."

18. **Policy Statement:** Access privileges are granted based on the principle of least privilege; personnel will only be granted the minimum level of access necessary to perform their job responsibilities.
19. **Procedure:** All requests for new or modified physical access permissions must be submitted through the IT Service Portal, require manager approval, and are then actioned by the Physical Security team. An audit trail of these requests and approvals is maintained.
20. **Use Case (Contractor Anomaly for Simulation):** A cleaning contractor, typically authorized only for general office areas after 6 PM, attempts to access a secure server room corridor at 2 PM. Their badge is denied. *Simulation Task: How should security respond and investigate?*

### 1.7. Table: Standard Physical Access Log Data Fields

The following table provides a structured reference for the key data fields that constitute a comprehensive physical access log entry at World Bank. Understanding these fields is essential for creating, interpreting, and auditing access logs within the simulation environment, and for recognizing data points that might indicate normal versus potentially suspicious activity.

Field Name	Description/Purpose	Example (Normal Entry)	Example (Suspicious/Anomaly Indicator)
Log ID	Unique identifier for each log entry.	202410260001	(Missing or duplicate ID)
Date of Access	Full date of the access event.	2024-10-26	2023-02-30 (Invalid Date)
Time In	Exact time of entry (HH:MM:SS).	08:55:03	02:10:45 (For routine office worker)
Time Out	Exact time of exit (HH:MM:SS).	17:02:11	N/A (For visitor badge not returned)
Full Name of Individual	Verified full name of the person.	Alice Wonderland	John Doe (Name mismatch with ID E00789)
Employee ID/Visitor ID etc.	Unique identifier for the person.	E00789	E99999 (Unknown ID)
Organization/Department	Person's affiliation.	IT Department	Marketing (For Data Center access)
Escort Name & ID	Name/ID of World Bank escort, if required.	N/A (For employee) / Bob Green (E00123) (For visitor)	N/A (For visitor in restricted area)
Access Point/Location	Specific door, gate, or area accessed.	Main Office Entrance 1	Vault Door (By non-vault personnel)

<b>Purpose of Visit/Access</b>	Stated reason for entry.	Scheduled Server Maintenance	"Retrieving personal item" (For Data Center at 3 AM) / Access Denied - Unauthorized
<b>Authorization Method</b>	How access was gained/attempted.	Badge Swipe	Forced_Open_Alarm / Badge_Clone_Alert
<b>Authorization Grantor</b>	Person authorizing manual/override entry.	N/A (For badge swipe) / SO_001 (For manual sign-in)	(Blank for manual override)
<b>Badge Number Issued</b>	Temporary badge ID for visitors/contractors.	B0678	(Same badge ID issued to multiple concurrent visitors)
<b>Asset Carried In/Out</b>	Description of significant assets.	Laptop SN: WB12345	Unidentified server components (No authorization)
<b>Log Entry Timestamp</b>	System-generated time of log record creation.	2024-10-26 08:55:03	(Timestamp significantly different from Time In)
<b>Security Officer on Duty</b>	ID of the officer overseeing the access point.	SO_001	(Officer on duty not matching roster)
<b>Access Result</b>	Outcome of the access attempt.	Granted	Denied - Expired Credentials / Denied - Unknown User
<b>Alarm/Event Type (If any)</b>	Specific alarm associated with the access event.	N/A	Door_Held_Open_Too_Long / Tamper_Switch_Activated
<b>Credential Type Used</b>	Type of credential presented.	Employee_Badge_Prox	Visitor_Badge_Expired / Unknown_Card_Format
<b>Entry/Exit Lane (If applicable)</b>	Specific turnstile or lane used at multi-lane access points.	Lane 3	(Simultaneous entry attempts on multiple lanes by same ID)