

Privileged Access Management (PAM) Documentation

Section 1: Purpose, Policy Statement, and Scope

- **1.1 Purpose:** This document outlines World Bank's policy, procedures, and controls for managing, monitoring, and securing all forms of privileged access to its information systems, applications, and data. Privileged access, if not properly controlled, represents a significant risk to the Bank's security and operational integrity. This documentation aims to establish a robust Privileged Access Management (PAM) program to mitigate these risks.
- **1.2 Policy Statement:** World Bank is committed to implementing and maintaining a comprehensive Privileged Access Management (PAM) program based on the principle of least privilege. All privileged access will be strictly controlled, monitored, audited, and granted only when necessary and for the minimum duration required. This policy ensures that privileged accounts are protected from misuse, compromise, and unauthorized access, thereby safeguarding critical assets and sensitive data in compliance with regulatory requirements and industry best practices.
- **1.3 Scope:**
 - This policy applies to all privileged accounts within World Bank's IT environment, including but not limited to:
 - Administrative accounts on servers, operating systems (Windows, Linux/Unix), network devices (firewalls, routers, switches), databases, and security appliances.
 - Service accounts used by applications, services, and automated processes that possess elevated permissions.
 - Application superuser accounts (e.g., admin accounts for Core Banking System, Online Banking Platform).
 - Domain administrator accounts (e.g., Active Directory Enterprise Admins, Domain Admins).
 - Cloud infrastructure administrative accounts (e.g., AWS root/IAM privileged users, Azure Global Administrators).
 - Emergency access accounts (firecall/break-glass accounts).
 - Privileged access granted to third-party vendors and contractors.
 - This policy applies to all World Bank employees, contractors, consultants, and third-party vendors who are granted, manage, or utilize privileged access.

- The PAM program covers the entire lifecycle of privileged accounts, from provisioning to de-provisioning.
- Effective PAM is not merely about technology; it's a holistic strategy integrating people, processes, and technology. The absence of a strong PAM program often leads to unmanaged "privilege creep," where users accumulate excessive permissions over time, significantly expanding the attack surface. This documentation aims to address this by ensuring that access is consistently reviewed and right-sized, rather than being a one-time setup.

Section 2: Roles and Responsibilities

- **2.1 Security Manager:**

- Oversees the PAM program, including policy development, implementation, and enforcement.
- Approves PAM tool selection, configuration standards, and significant policy exceptions.
- Reviews PAM audit reports and ensures remediation of identified issues.

- **2.2 PAM Solution Administrators:**

- Responsible for the day-to-day administration, configuration, and maintenance of the PAM solution (e.g., credential vaulting, session management, access request workflows).
- Onboard privileged accounts into the PAM system.
- Monitor the health and security of the PAM infrastructure itself.

- **2.3 System/Application/Network/Database Owners/Administrators:**

- Identify privileged accounts within their respective systems and ensure they are managed through the PAM solution.
- Request privileged access for themselves or their teams through approved PAM workflows.
- Utilize privileged access responsibly and in accordance with this policy.
- Report any suspected misuse or compromise of privileged credentials immediately.

- **2.4 Human Resources (HR):**

- Notify IT/Security promptly of employee terminations or role changes that require revocation or modification of privileged access.

- **2.5 Internal Audit / Compliance Team:**

- Conduct periodic audits of the PAM program, controls, and adherence to this policy.
- Verify compliance with regulatory requirements related to privileged access (e.g., FFIEC, SOX, PCI DSS).
- **2.6 Privileged Users (All Employees/Contractors with Privileged Access):**
 - Adhere strictly to this PAM policy and associated procedures.
 - Use unique, strong passphrases/passwords for their individual accounts that request privileged access.
 - Never share privileged account credentials.
 - Use privileged access only for authorized tasks and for the minimum time necessary.
 - Report any security concerns or suspicious activity related to privileged accounts.
- The successful implementation of a PAM program necessitates a cultural shift where privileged access is viewed as a significant responsibility, not an entitlement. This requires clear communication from management about the importance of PAM, comprehensive training for all privileged users, and consistent enforcement of the policy. Without this, even the most sophisticated PAM technology can be undermined by human error or intentional misuse.

Section 3: Privileged Account Lifecycle Management

- **3.1 Privileged Account Discovery and Inventory:**
 - Regular, automated discovery scans will be performed to identify all existing privileged accounts across the IT environment, including on-premise and cloud assets.
 - A comprehensive inventory of all privileged accounts will be maintained within the PAM solution or a designated secure repository. This inventory will include account name, associated system/application, owner, purpose, privilege level, and last password change/review date.
 - Service accounts will be specifically inventoried, documenting their purpose, dependencies, and responsible owner.
- **3.2 Privileged Account Provisioning:**
 - All requests for new privileged accounts or privileged access rights must be formally submitted through a documented approval workflow, managed via the PAM solution or a designated service management tool.

- Requests must include justification, scope of access required, and duration (if temporary).
- Approvals must be obtained from the system/application owner and the user's manager, with final approval from the Security Manager for highly sensitive privileges.
- The principle of least privilege will be strictly enforced: users will be granted only the minimum necessary privileges required to perform their job functions.
- Dedicated administrative accounts must be used for performing privileged tasks; daily user accounts must not have administrative privileges.

- **3.3 Privileged Credential Management:**

- All privileged account credentials (passwords, SSH keys, API keys) must be vaulted and managed by the central PAM solution. Direct knowledge of privileged passwords by human users should be minimized.
- The PAM solution will automatically rotate privileged account passwords at regular intervals (e.g., every 30-90 days, or more frequently for highly sensitive accounts) and after each use for "checkout" scenarios.
- Passwords generated by the PAM solution must meet World Bank's strong password complexity and length requirements.
- Hardcoded credentials in scripts, applications, or configuration files are strictly prohibited. Such credentials must be replaced with calls to the PAM vault API.
- Sharing of privileged account credentials is strictly prohibited. Access will be granted to individuals through the PAM system.

- **3.4 Privileged Access Reviews (Recertification):**

- Regular reviews of all privileged accounts and associated access rights will be conducted to ensure continued necessity and appropriateness.
- System/application owners and managers will review access for their respective areas at least quarterly.
- Dormant privileged accounts (e.g., inactive for more than 45-90 days) will be disabled or removed after investigation.
- Results of access reviews will be documented and retained for audit purposes.

- **3.5 Privileged Account De-provisioning:**

- Privileged access rights must be revoked or accounts disabled immediately upon employee termination, role change, or when access is no longer required.

- HR will have a formal process to notify IT/Security promptly of employee departures.
- The PAM system will be used to automate de-provisioning where possible.

Section 4: Privileged Session Management

- **4.1 Privileged Session Monitoring and Recording:**
 - All privileged sessions initiated through the PAM solution (e.g., RDP, SSH, database connections) must be monitored and recorded.
 - Session recordings will capture screen activity, keystrokes (where permissible and technically feasible), and commands executed.
 - Real-time session monitoring capabilities may be used by the SOC for high-risk activities or ongoing investigations.
 - Session recordings will be securely stored and retained according to the Log Retention Policy for audit and forensic purposes.
- **4.2 Privileged Threat Analytics / User Behavior Analytics (UEBA):**
 - The PAM solution, in conjunction with the SIEM, will be used to analyze privileged user behavior and detect anomalies that may indicate account compromise, insider threat, or policy violations.
 - Alerts will be generated for suspicious activities, such as logins from unusual locations, access at odd hours, or execution of unauthorized commands.
- **4.3 Just-in-Time (JIT) and Just-Enough-Access (JEA):**
 - Where feasible and appropriate, JIT access mechanisms will be implemented. Privileges will be granted dynamically for a limited time, only when needed for a specific task, and automatically revoked upon completion.
 - JEA principles will be applied to further restrict what actions a privileged user can perform during a session, even with elevated rights.

Section 5: Specific Privileged Access Scenarios

- **5.1 Emergency Access (Firecall/Break-Glass Procedure):**
 - A documented emergency access procedure (often called "firecall" or "break-glass") exists for situations where normal privileged access mechanisms fail or are unavailable, and immediate privileged access is required to resolve a critical system outage or security incident.
 - **Procedure Outline:**

1. **Request Initiation:** Authorized personnel (e.g., senior IT operator, on-call manager) identify the need for emergency access.
 2. **Approval:** Request must be approved by at least two authorized managers (if available, otherwise one with documented justification). Approval is logged.
 3. **Credential Release:** Pre-defined emergency account credentials (stored securely, e.g., in a physical safe with dual control or a break-glass component of the PAM tool) are released to the designated individual.
 4. **Session Monitoring:** If technically feasible, the emergency session must be monitored or recorded. If not, detailed manual logging of actions taken is mandatory.
 5. **Activity Logging:** All actions performed using the emergency account must be meticulously logged by the user.
 6. **Notification:** The Security Manager and relevant stakeholders must be notified of the firecall activation as soon as possible.
 7. **Credential Reset and Review:** Immediately after the emergency is resolved, the password for the emergency account must be changed. A full review of the firecall incident, actions taken, and justification must be conducted within 24 hours.
- Emergency accounts must be highly restricted, audited regularly, and their passwords changed after each use and on a scheduled basis.
- **5.2 Third-Party Vendor Privileged Access:**
 - All privileged access granted to third-party vendors must be provisioned through the PAM solution.
 - Vendor access will be time-bound, restricted to specific systems and tasks as per contractual agreements, and adhere to the principle of least privilege.
 - MFA will be enforced for all vendor privileged access.
 - All vendor privileged sessions will be monitored and recorded.
 - Vendor accounts will be reviewed regularly and disabled immediately upon contract termination or completion of work.
 - **5.3 Service Account Management:**
 - Service accounts must have their passwords vaulted and automatically rotated by the PAM solution.

- Service accounts must be configured with the minimum necessary privileges.
- Dependencies of service accounts on applications and systems must be documented and managed to prevent outages during password rotation.
- Regular audits will be conducted to identify and remediate unmanaged or overly privileged service accounts.

Section 6: Auditing, Compliance, and Policy Review

- **6.1 Auditing:**

- The PAM solution will generate comprehensive audit logs of all privileged account activity, access requests, approvals, credential usage, and session recordings. These logs will be forwarded to the SIEM for correlation and analysis.
- Regular audits of PAM configurations, policies, and procedures will be conducted by Internal Audit and/or external auditors.

- **6.2 Compliance:**

- This PAM policy and its implementation support compliance with various regulatory frameworks including FFIEC guidance, SOX (access controls, segregation of duties), and PCI DSS (Requirement 7: Restrict access to cardholder data by business need to know; Requirement 8: Identify and authenticate access to system components).

- **6.3 Policy Review and Exceptions:**

- This PAM Documentation will be reviewed and updated at least annually, or upon significant changes to World Bank's IT environment, threat landscape, or regulatory requirements.
- Exceptions to this policy must be formally documented, risk-assessed, and approved by the Security Manager and, if necessary, Senior Management. Approved exceptions will be regularly reviewed.

Appendix A: Privileged Access Management Simulation Items/Scenarios for World Bank

1. **Privileged Account Discovery:** Run an automated scan to identify any new, unmanaged administrator accounts on a segment of Windows servers.
 - **Action:** Compare findings against the authorized PAM inventory. Investigate any discrepancies.

2. **Least Privilege Verification:** Review the permissions of three randomly selected privileged user accounts (e.g., a database admin, a network admin, an application admin).
 - **Action:** Determine if their assigned privileges exceed what is necessary for their documented job roles.
3. **Password Vault Checkout:** A system administrator needs to perform urgent maintenance on a critical database server.
 - **Action:** Simulate the administrator requesting and checking out the database root/SA password from the PAM vault. Verify MFA is prompted.
4. **Automated Password Rotation Test:** Trigger an on-demand password rotation for a specific service account managed by PAM.
 - **Action:** Verify the password is changed in the vault and successfully updated on the target system/application without disrupting the service.
5. **Privileged Session Monitoring:** An administrator initiates an SSH session to a critical Linux server through the PAM solution.
 - **Action:** SOC analyst to verify the session is being actively monitored and recorded by the PAM tool. Review a snippet of the recording.
6. **JIT Access Request:** A developer requests temporary root access to a UAT server for 2 hours to troubleshoot an application deployment issue.
 - **Action:** Simulate the JIT request and approval workflow. Verify access is granted for the specified duration and automatically revoked.
7. **Firecall Procedure Activation:** Simulate a scenario where the primary PAM solution is unavailable, and emergency root access to the Core Banking System's primary database server is needed.
 - **Action:** Execute the documented firecall/break-glass procedure, including obtaining approvals and releasing credentials.
8. **Post-Firecall Review:** Following the simulated firecall.
 - **Action:** Conduct a mock post-incident review, verify documentation of actions taken, and ensure the firecall account password was reset.
9. **Third-Party Vendor Access:** A third-party vendor requires temporary privileged access to a specific application server for support.
 - **Action:** Provision access via PAM with time limits and session recording enabled. Verify their access is restricted only to the necessary server.

10. **Dormant Privileged Account Detection:** Identify privileged accounts that have not been used for more than 60 days.
 - **Action:** Initiate the review and disabling process for these accounts.
11. **Privileged Access Recertification:** System owner for the CRM application is prompted to review and recertify all users with administrative access to the CRM.
 - **Action:** Simulate the owner reviewing and approving/rejecting access.
12. **Alert for Suspicious Privileged Activity:** SIEM generates an alert for a domain administrator account logging in from an unusual geolocation.
 - **Action:** SOC analyst to investigate the alert, verify user's legitimate location, and escalate if suspicious.
13. **Hardcoded Credential Scan:** Use a tool to scan a sample application's codebase or configuration files for hardcoded privileged credentials.
 - **Action:** Report findings for remediation (replacement with PAM vault calls).
14. **SSH Key Management Audit:** Review SSH keys granting privileged access to critical Linux servers.
 - **Action:** Verify keys are managed within PAM, associated with specific users/purposes, and unauthorized keys are not present.
15. **Service Account Dependency Mapping:** A service account password used by three applications is scheduled for rotation.
 - **Action:** Verify the PAM system or documentation correctly identifies all dependent applications to ensure coordinated updates.
16. **Attempt to Bypass PAM:** A user with local admin rights (non-privileged user account) attempts to install unapproved software that could be used to escalate privileges.
 - **Action:** Verify endpoint security controls block the installation and/or alert the SOC.
17. **Privileged Account Provisioning Workflow Test:** A new system administrator is hired.
 - **Action:** Simulate the process of requesting, approving, and provisioning their necessary privileged accounts through the PAM system, ensuring least privilege.
18. **Audit Trail Review for Privileged Access:** Select a critical system and review the PAM audit logs for all privileged access events (requests, approvals, sessions) over the past 7 days.
 - **Action:** Check for completeness and identify any anomalies.

19. **MFA Enforcement for PAM Access:** Attempt to log in to the PAM administrative console using only a username and password.

- **Action:** Verify that MFA is enforced and the login fails without the second factor.

20. **Training Verification:** Randomly select five privileged users.

- **Action:** Verify they have completed the mandatory PAM awareness and usage training within the last 12 months.