

Secure Configuration Policy

Section 1: Policy Statement, Objectives, and Scope

- **1.1 Policy Statement** World Bank mandates the implementation and maintenance of secure configurations for all its information technology (IT) assets, including systems, network devices, applications, databases, and endpoints. This policy establishes the framework for defining, implementing, monitoring, and managing secure baselines derived from industry best practices such as Center for Internet Security (CIS) Benchmarks, National Institute of Standards and Technology (NIST) guidelines, and vendor-specific hardening recommendations. Adherence to this policy is critical to minimizing vulnerabilities, reducing the attack surface, and protecting World Bank's information assets against unauthorized access, modification, or disruption.
- **1.2 Objectives** The primary objectives of this Secure Configuration Policy are to:
 - Establish and enforce standardized, secure baseline configurations for all IT assets across World Bank.
 - Reduce the risk of security incidents arising from misconfigurations, default settings, or unnecessary services and functionalities.
 - Ensure compliance with relevant regulatory requirements (e.g., FFIEC, PCI DSS, SOX) and internal security standards regarding system hardening.
 - Provide a consistent and repeatable process for configuring new assets and maintaining the security posture of existing assets.
 - Facilitate efficient vulnerability management and patch management by starting from a hardened state.
 - Support the principle of least functionality by disabling or removing all services, protocols, and software not explicitly required for business purposes.
- **1.3 Scope**
 - This policy applies to all IT assets owned, operated, or managed by World Bank or on its behalf, including but not limited to:
 - Servers (physical and virtual)
 - Operating Systems (server and endpoint)
 - Network Devices (firewalls, routers, switches, wireless access points, VPNs)
 - Databases and Database Management Systems

- Applications (COTS, custom-developed, web applications, mobile applications)
- Endpoints (desktops, laptops, mobile devices, IoT devices where applicable)
- Cloud services and infrastructure (IaaS, PaaS, SaaS configurations managed by World Bank)
- Security appliances (IDS/IPS, WAF, SIEM, PAM)
- This policy applies to all World Bank employees, contractors, consultants, and third-party vendors involved in the design, deployment, administration, and maintenance of IT assets.
- The establishment of secure configurations is not a one-time activity but an ongoing lifecycle process. This involves initial hardening, continuous monitoring for configuration drift, regular audits, and updates to baselines as new threats emerge or system requirements change. This dynamic approach is essential because static configurations can quickly become vulnerable in the face of evolving attack techniques and software updates.

Section 2: Roles and Responsibilities

- **2.1 Security Manager:**

- Oversees the development, implementation, and enforcement of this Secure Configuration Policy.
- Approves baseline configuration standards and any deviations.
- Ensures regular review and updates of configuration standards.

- **2.2 IT Operations / System Administrators:**

- Responsible for implementing and maintaining secure configurations on servers, operating systems, and other assigned infrastructure components according to approved baselines.
- Perform regular configuration audits and remediate deviations.
- Manage patch deployment in line with secure configurations.

- **2.3 Network Administrators:**

- Responsible for implementing and maintaining secure configurations on all network devices according to approved baselines.
- Manage firewall rules, router ACLs, and switch configurations securely.

- **2.4 Database Administrators (DBAs):**

- Responsible for implementing and maintaining secure configurations for all database systems according to approved baselines, including access controls, encryption, and auditing features.
- **2.5 Application Owners / Development Teams:**
 - Ensure that applications are developed and deployed with secure configurations, adhering to the Secure Software Development Lifecycle (SSDLC) policy.
 - Responsible for hardening application-specific settings and removing unnecessary features.
 - Collaborate with IT Operations to ensure underlying infrastructure meets application security requirements.
- **2.6 Endpoint Management Team:**
 - Responsible for implementing and maintaining secure configurations on all corporate endpoints (desktops, laptops, mobile devices) according to approved baselines.
- **2.7 Cloud Security Team / Administrators:**
 - Responsible for defining and implementing secure configurations for cloud resources (IaaS, PaaS) and ensuring SaaS applications are configured securely according to vendor best practices and World Bank standards.
- **2.8 Internal Audit / Compliance Team:**
 - Conduct periodic audits to verify compliance with this Secure Configuration Policy and associated standards.
 - Report findings and recommendations to management.
- A consistent approach to secure configurations across diverse platforms and technologies requires strong central governance combined with distributed responsibility for implementation. While the Security Manager defines the "what" (the policy and standards), the various IT and development teams are responsible for the "how" (the actual implementation and maintenance). This necessitates clear documentation of baselines, robust training, and effective communication channels to ensure all parties understand their obligations and have the resources to meet them. Without this, configuration drift is inevitable, undermining the security posture of the Bank.

Section 3: Secure Configuration Standards and Baselines

- **3.1 Baseline Development and Sources:**

- World Bank will develop and maintain documented secure configuration baselines for all in-scope IT assets.
- Baselines will be derived from a combination of:
 - **Center for Internet Security (CIS) Benchmarks:** Level 1 and Level 2 profiles will be adopted or adapted as appropriate for the asset's criticality and the Bank's risk appetite.
 - **National Institute of Standards and Technology (NIST) Guidelines:** Relevant NIST Special Publications (e.g., SP 800-53, SP 800-70, SP 800-123, SP 800-128) will be used as references for establishing secure configurations.
 - **Vendor-Specific Hardening Guides:** Recommendations from hardware and software vendors (e.g., Microsoft, Cisco, Oracle, VMware) for securing their products will be incorporated.
 - **Regulatory Requirements:** Specific configuration mandates from FFIEC, PCI DSS, SOX, and other applicable regulations will be embedded in the baselines.
- Baselines will be tailored to World Bank's specific environment and risk profile. A risk assessment will determine the applicability and stringency of specific configuration settings.
- **3.2 Key Configuration Areas (General Principles):** Regardless of the specific asset type, secure configurations will address the following areas:
 - **Account Security:**
 - Disabling or removing default accounts and passwords immediately upon deployment.
 - Enforcing strong password/passphrase policies (complexity, length, history, expiration) for all accounts, especially administrative accounts.
 - Implementing account lockout mechanisms after a defined number of failed login attempts.
 - Restricting and closely monitoring the use of privileged accounts (see PAM Documentation).
 - **Service and Port Management (Least Functionality):**
 - Disabling all unnecessary services, protocols, daemons, and ports on systems and network devices.
 - Removing or disabling unnecessary software and features.

- **Access Control:**
 - Implementing the principle of least privilege for all user and service accounts.
 - Configuring file system and network share permissions to restrict access based on job roles.
 - Securely configuring remote access mechanisms (e.g., VPNs, SSH) with strong authentication (MFA).
- **Logging and Auditing:**
 - Enabling sufficient logging to capture security-relevant events as defined in the Logging and Monitoring Policy.
 - Protecting log files from unauthorized modification or deletion.
- **Patch and Vulnerability Management:**
 - Ensuring systems are configured to facilitate timely patch deployment.
 - Regularly scanning for vulnerabilities introduced by misconfigurations.
- **Data Protection:**
 - Configuring encryption for sensitive data at rest and in transit where applicable.
 - Securely configuring backup and recovery mechanisms.
- **Network Security:**
 - Secure configuration of firewalls with restrictive rule sets (default deny).
 - Secure configuration of routers and switches (e.g., disabling unused management interfaces, securing SNMP).
 - Implementing network segmentation and isolation for critical systems.
- **Secure Software Development Lifecycle (SSDLC):**
 - Applications developed in-house or for the Bank must follow secure coding practices and be configured securely at deployment. This includes input validation, output encoding, secure API configurations, and proper error handling.
- **3.3 Specific Asset Type Hardening Examples:**
 - **Operating Systems (Windows, Linux Servers):**
 - Application of CIS Level 2 benchmarks, tailored after risk assessment.

- Removal of unnecessary roles and features.
- Configuration of host-based firewalls.
- Implementation of security-enhanced kernels or modules (e.g., SELinux).
- User Account Control (UAC) settings (Windows).
- Regular security template application and verification.
- **Network Devices (Firewalls, Routers, Switches):**
 - Changing default administrative credentials and SNMP community strings.
 - Disabling unnecessary management protocols (e.g., Telnet, HTTP, SNMPv1/v2c).
 - Implementing secure management protocols (e.g., SSHv2, HTTPS, SNMPv3).
 - Configuring Access Control Lists (ACLs) and firewall rules based on least privilege.
 - Enabling logging of all administrative access and significant network events.
 - Securing routing protocols.
- **Databases (e.g., Oracle, SQL Server, PostgreSQL):**
 - Removing default database accounts and schemas.
 - Enforcing strong authentication for database users.
 - Restricting database user privileges to the minimum required.
 - Enabling database auditing for sensitive operations.
 - Encrypting sensitive data within the database (TDE) and database backups.
 - Regularly patching the DBMS software.
- **Web Servers (e.g., Apache, Nginx, IIS):**
 - Removing default web pages and sample applications.
 - Disabling unnecessary modules and CGI scripts.
 - Configuring for HTTPS only, disabling weak SSL/TLS protocols and ciphers.

- Implementing security headers (e.g., HSTS, CSP, X-Frame-Options).
- Restricting directory browsing.
- **Cloud Infrastructure (IaaS/PaaS - e.g., AWS, Azure):**
 - Secure configuration of Identity and Access Management (IAM) roles and policies.
 - Network security group and virtual firewall configurations based on least privilege.
 - Encryption of storage (e.g., S3 buckets, Azure Blobs, managed disks).
 - Enabling and centralizing cloud provider audit logs (e.g., CloudTrail, Azure Monitor).
 - Secure configuration of serverless functions and container services.
- **3.4 Vendor Security Baselines:**
 - For COTS software and hardware, World Bank will, where available and appropriate, adopt or adapt security baselines and hardening guides provided by the respective vendors (e.g., Microsoft Security Baselines , Cisco hardening guides).
 - These vendor baselines will be evaluated against World Bank's internal standards and CIS/NIST benchmarks to ensure they meet or exceed our security requirements.
 - During procurement and vendor selection, preference will be given to products that offer robust security configuration options and well-documented hardening guidance.
 - Third-party service providers managing systems on behalf of World Bank must contractually agree to adhere to World Bank's secure configuration standards or equivalent, verifiable standards.

Section 4: Configuration Management and Change Control

- **4.1 Configuration Management Database (CMDB):**
 - World Bank will maintain a CMDB or equivalent system to inventory all IT assets and their approved baseline configurations.
 - The CMDB will track key configuration attributes and relationships between assets.
- **4.2 Change Control for Secure Configurations:**

- All changes to production system configurations must follow World Bank's formal IT Change Management Policy.
 - Proposed changes must be assessed for their impact on the security posture of the system and the overall environment.
 - Security configurations must be reviewed and approved by designated security personnel (e.g., Security Manager or delegate) before implementation.
 - All configuration changes must be documented, tested in a non-production environment where feasible, and have a rollback plan.
 - Emergency changes must still be documented and reviewed retrospectively for security compliance.
- **4.3 Configuration Monitoring and Auditing:**
 - Automated tools will be used, where feasible, to continuously monitor systems for deviations from approved secure baselines (configuration drift).
 - Regular security audits (both internal and external) will include verification of compliance with secure configuration standards.
 - Identified deviations must be investigated, remediated in a timely manner based on risk, and documented.

Section 5: Vulnerability Management and Patch Management Integration

- **5.1 Vulnerability Scanning:**
 - Regular vulnerability scans will be performed on all IT assets to identify misconfigurations and known vulnerabilities.
 - Scan results will be used to validate the effectiveness of secure configurations and identify areas for improvement in baselines.
- **5.2 Patch Management:**
 - A robust patch management process, as defined in the Patch Management Policy, will be maintained to address vulnerabilities in operating systems, applications, and firmware.
 - Secure configurations should facilitate efficient patching by minimizing system complexity.

Section 6: Policy Review and Exceptions

- **6.1 Review Cycle:** This Secure Configuration Policy and all associated baseline documents will be reviewed and updated at least annually, or more frequently in response to new threats, vulnerabilities, significant system changes, audit findings, or changes in regulatory requirements.

- **6.2 Exception Process:** Any requests for exceptions to this policy or specific baseline configurations must be formally documented, justified, and submitted to the Security Manager for approval. The request must include a risk assessment detailing the potential impact of the deviation and any proposed compensating controls. Approved exceptions will be documented, time-limited where appropriate, and reviewed periodically.
-

Appendix A: Secure Configuration Simulation

Items/Scenarios for World Bank

1. **New Server Deployment:** A new Windows Server is being deployed for a Tier 2 application.
 - **Action:** Apply the World Bank Windows Server Secure Baseline (derived from CIS Level 2, NIST SP 800-123). Verify removal of default accounts and unnecessary services (e.g., disable Print Spooler if not needed).
2. **Firewall Rule Review:** A request is submitted to open a new port on the external firewall for a vendor connection.
 - **Action:** Review the request against the firewall configuration policy (least privilege, default deny). Ensure proper justification, source/destination IP restrictions, and logging are configured.
3. **Database Hardening Check:** Audit a production SQL Server instance.
 - **Action:** Verify that default SA account is disabled, strong passwords are enforced for DB accounts, TDE is enabled for sensitive databases, and audit logging is active for privileged operations.
4. **Application Configuration Audit:** Review the configuration of the Online Banking web application.
 - **Action:** Check for secure cookie settings (HttpOnly, Secure), enabled security headers (HSTS, CSP), and disabled directory browsing.
5. **Endpoint Security Configuration:** A new batch of laptops is being provisioned for employees.
 - **Action:** Ensure the standard corporate endpoint image, which includes OS hardening (CIS benchmarked), EDR client, full-disk encryption, and host firewall, is applied.
6. **Cloud IAM Policy Review (AWS/Azure):** Review IAM roles assigned to a new cloud-based financial analytics application.

- **Action:** Verify the principle of least privilege is applied to the role's permissions for accessing cloud resources (e.g., specific S3 buckets, specific EC2 instances).
7. **Vendor Baseline Application:** A new network switch from Cisco is installed.
- **Action:** Apply Cisco's hardening guidelines in conjunction with World Bank's network device baseline (e.g., disable Telnet, configure SSHv2, secure SNMPv3).
8. **Configuration Drift Detection:** A monitoring tool alerts that an unnecessary service (e.g., FTP server) has been enabled on a critical application server.
- **Action:** Investigate the change, determine if authorized, and revert to the secure baseline if unauthorized. Document the incident.
9. **Patch Management Compliance:** Verify that a set of critical servers have received the latest security patches within the timeframe specified in the Patch Management Policy.
- **Action:** Use vulnerability scan results or patch management system reports to confirm compliance.
10. **SSDLC Checkpoint:** A new custom financial reporting application is moving from development to UAT.
- **Action:** Verify that secure configuration checks (e.g., no hardcoded credentials, secure API configurations) have been completed as part of the SSDLC.
11. **Default Credential Scan:** Run a scan across the network to identify any devices or applications still using default administrative credentials.
- **Action:** Remediate any findings immediately.
12. **Service Account Review:** Review service accounts used by the Core Banking System.
- **Action:** Verify each service account has the minimum necessary privileges and that passwords are managed by the PAM solution.
13. **Wireless Network Security Configuration:** Audit the configuration of corporate Wi-Fi access points.
- **Action:** Ensure WPA3 (or WPA2-AES minimum) encryption is used, strong pre-shared keys or 802.1X authentication is implemented, and guest network is properly isolated.
14. **Remote Access Configuration (VPN):** Review VPN concentrator configuration.
- **Action:** Verify strong encryption ciphers, MFA enforcement for all VPN users, and split-tunneling is disabled (or strictly controlled if allowed).

15. **Operating System Logging Configuration:** Check if a selection of critical Linux servers are forwarding audit logs to the central SIEM as per the logging policy.
- **Action:** Confirm log agent functionality and SIEM ingestion.
16. **Firewall Egress Filtering Test:** Attempt to initiate an outbound connection from a test server in a restricted network segment to an arbitrary port on an external IP.
- **Action:** Verify the firewall blocks the connection as per the egress filtering rules defined in its secure configuration.
17. **Container Security Configuration (if applicable):** Review the security configuration of a Docker host or Kubernetes cluster.
- **Action:** Check for adherence to CIS Docker/Kubernetes benchmarks, such as restricting container privileges, using secure base images, and configuring network policies.
18. **Mobile Device Management (MDM) Policy Enforcement:** Verify that MDM policies (e.g., enforcing screen lock, encryption, remote wipe capability) are being applied to a sample of corporate mobile devices.
- **Action:** Check device compliance status in the MDM console.
19. **Unnecessary Software Removal:** Audit a sample of workstations for unapproved or unnecessary software installations.
- **Action:** Initiate removal if unauthorized software is found, based on the asset management and secure configuration policies.
20. **Physical Security Appliance Configuration:** Review the configuration of a physical security appliance (e.g., a dedicated HSM).
- **Action:** Verify administrative access controls, audit logging, and physical tamper-proofing mechanisms are correctly configured and active.