Standard Operating Procedure (SOP)

Asset and Configuration Management Procedures

This SOP defines the **Asset and Configuration Management Procedures**, detailing the systematic process for tracking, managing, and maintaining all IT assets and configuration items throughout their lifecycle. It covers asset identification, configuration baseline establishment, change control, documentation, and audit processes to ensure accuracy, integrity, and security of information systems. The objective is to optimize asset utilization, reduce risks associated with unauthorized changes, and support effective IT service management and compliance requirements.

1. Purpose

To establish standardized procedures for managing IT assets and configuration items, ensuring their accuracy, security, traceability, and optimal utilization across all organizational units.

2. Scope

This SOP applies to all IT assets and configuration items (CIs) owned, operated, or managed by the organization, including but not limited to hardware, software, network devices, virtual assets, and cloud resources.

3. Definitions

- **Asset:** Any resource or component (hardware, software, data, etc.) with value to the organization.
- **Configuration Item (CI):** Any asset or component under configuration management control.
- **Configuration Management Database (CMDB):** A repository that stores information about CIs.
- **Baseline:** A formally agreed snapshot of configuration items at a specific point in time.

4. Roles and Responsibilities

Role	Responsibility
Asset Manager	Oversee asset management activities, maintain accurate records, lead audits.
Configuration Manager	Ensure integrity of CIs, manage baselines, oversee change control.
IT Staff / Owners	Report asset changes, maintain documentation, follow procedures.
Auditors	Conduct periodic asset and configuration audits for compliance and accuracy.

5. Procedures

1. **Asset Identification and Registration**
    - All new IT assets must be tagged and registered in the CMDB upon receipt or deployment.
    - Asset records must include unique ID, description, location, owner, status, and configuration details.
2. **Configuration Baseline Establishment**
    - Establish configuration baselines for all significant assets/CIs.
    - Record all baseline attributes and approval signatures in the CMDB.
3. **Change Control**
    - No asset or configuration change is permitted without proper authorization via a formal Change Request (CR).
    - Impact analysis and approval must precede all changes. Update the CMDB post-implementation.
4. **Documentation and Recordkeeping**
    - Maintain up-to-date documentation for all assets and CIs, including licenses, warranties, and support

    contracts.
    - Update documentation promptly following asset changes or lifecycle events (e.g., disposal, transfer).

5. **Audit and Review**
    - Conduct periodic audits (at least annually) to verify the accuracy and completeness of asset and CI records.
    - Investigate and resolve discrepancies. Report findings to IT management.

6. **Lifecycle Management**
    - Manage assets and configurations through procurement, deployment, maintenance, retirement, and disposal in accordance with security and compliance mandates.

6. Compliance and Exceptions

- All personnel must adhere to this SOP. Exceptions must be pre-approved by the IT Manager and documented with justification.
- Non-compliance may result in disciplinary action and/or security incident reporting.

7. References

- ISO/IEC 20000 - IT Service Management
- ISO/IEC 27001 - Information Security Management
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems
- Organizational Asset Management Policy

8. Revision History

Date	Version	Description	Author
2024-06-01	1.0	Initial SOP release	IT Governance Team