Document title: **[IT Configuration Management Policy – Oct 2022]**

Approval date: **[October 2021]**

Purpose of document: **[Govern and describe IT configuration management within AUC]**

Office/department responsible: **[Office of Information Security]**
Approved by: **[Iman Megahed, AVP for Digital Transformation & Chief Strategy & Knowledge Officer]**

Document classification level: **[PUBLIC]**

Document accessible: **[https://www.aucegypt.edu/about/university-policies]**

Document includes: **[Policy and approvers]**

Related documents/see also: **[Change management policy, Digital computing asset management policy, Digital asset disposal policy, Cloud hosting policy, Information security policy, Patch management policy]**

IT Configuration Management Policy

Policy Statement

Configuration Management is the discipline that identifies, records, controls, and reports on the IT infrastructure components such as hardware, software, documentation, services, personnel, and any other items (known as Configuration Items-CI's) and verifies the completeness and correctness of the configuration items.

Reason for Policy/Purpose

The purpose of an effective and efficient IT Configuration Management includes:

- To provide accurate IT infrastructure information to stakeholders.
- To monitor and control IT infrastructure.
- To provides a foundation for Incident Management, Problem Management, and Change Management.
- To collect inventory for all IT assets, configurations, and relationships.
- To verify the configuration item records against infrastructure.
- To provides a comfort level to the business in terms of assets and expenditures at an accurate level.
- To assist in the IT business resilience building.

Who Approved This Policy

Iman Megahed, AVP for Digital Transformation & Chief Strategy & Knowledge Officer

Who Needs to Know This Policy

AUC Staff and Faculty

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

Contacts

Responsible University Official: Wessam Maher, Chief Information Security, and Risk Officer.
Responsible University Office: Office of Information Security

If you have any questions on the policy, you may send an e-mail to infosec@aucegypt.edu

Definitions

Term (alphabetical order)	**Definition as it relates to this policy**
Configuration Item (CI)	Any Component that needs to be managed to deliver an IT Service. Information about each CI is recorded in a Configuration Item record within the Configuration Management System. Examples such as software version, software-enabled features, hardware capability, hardware configuration, software configuration, connectivity configuration, access-list…etc.
Configuration Management	The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their relationships. This information is managed throughout the lifecycle of the CI.
Configuration Management Database (CMDB)	A database used to store Configuration Records throughout their Lifecycle.
Configuration Management System (CMS)	Configuration Management System is a set of tools and Configuration Management Databases used to manage Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes, and Releases;
IT Infrastructure	All of the hardware, software, networks, facilities, etc., required to develop, test, deliver, monitor, control, or support IT Services.
RFC	Request For Change

Policy/Procedures

Configuration Management Database

The objective is to implement a CMDB that will provide a single source of information about the components of the IT environment. This information will be used to improve system reliability, availability, and control. By establishing a database to track IT components, known as configuration items (CIs), configuration management will verify that only authorized components are used in the IT environment; this is an important aspect of control because an unauthorized component could introduce undocumented issues that could be detrimental and/or have difficult-to-trace effects on related components in the production environment.

High-Level Control Objective

IT will exercise controls over the IT processes for managing the configuration that satisfies the information security and regulatory requirements to account for IT components, prevent unauthorized alterations, verify physical existence, and provide a basis for sound Change Management function by implementing procedures that allow for:

- Asset and Configuration ownership and tracking.
- Configuration change management
- Checking for unauthorized configuration items
- Software, hardware, and configuration interrelationships and integration
- Use automated tools as possible.

Activities

The basic activities structure of Configuration Management are as follows:

1. **Planning**: Studying and defining the purpose, scope, objectives, policies, and procedures, and the organizational and technical context for Configuration Management.
2. **Identification**: Selecting and identifying the configuration structures for all the infrastructure's CI's, including their "owner", their interrelationships, and configuration documentation. It includes allocating identifiers and version numbers for CI's, labeling each item, and entering it into the Configuration Management Database (CMDB).
3. **Control:** Ensuring that only authorized and identifiable CI's are accepted and recorded, from receipt to disposal. It ensures that no CI is added, modified, replaced, or removed without appropriate controlling documentation, e.g., an approved Change request and an updated specification.
4. **Status accounting:** The reporting of all current and historical data concerned with each CI throughout its life cycle. This enables Changes to CI's and their records to be traceable, e.g., tracking the status of a CI as it changes from one state to another, for instance: "under development, under test, live or inactive."
5. **Verification and audit:** A series of reviews and audits that verify the existence of CI's and check that they are correctly recorded in the Configuration Management system.

Selection of Configuration Items to be managed

The components that will be managed by the Configuration Management function will be selected, considering the business relevance and importance of the component and the relationship(s) it has with other components within the IT environment. The priority Components to be managed will be for those that:

- Are necessary for the effective operation of AUC business.
- Support the provision of IT services.
- Can be seriously impacted by changes to other components within the environment.
- Found to be necessary in case of disaster recovery and business continuity scenarios.

The decision to include a component in the CMDB will be reviewed at periodic intervals by the Configuration Manager in conjunction with IT management. Any suspicious change should be reported instantly to the information security office.

Configuration Management Governance:

1. The final step in any approved IT change "for more information, kindly refer to Change Management policy" there will be an update and verification of the CMDB. The configuration manager will oversee the verification of CIs in the change record.

2. The access to the CMDB will be restricted according to business requirement needs.

3. All defined assets comprising the end-to-end delivery of any defined digital service will be documented in the CMDB.

4. The CMDB will maintain asset and configuration information to support internal and external IT Service Management and functional stakeholders.

5. The Configuration Management process will remain refreshed in terms of identified process improvement opportunities and continually improved and optimized over time. An annual review is recommended.

6. Configuration Management will provide accurate configuration information to the organization and will ensure that any discrepancy is corrected when found. Typically, this will involve notification to the Asset Manager.

7. All changes documented within the CMDB are required to result from RFCs managed through the Change Management process or through approved automated discovery, update, and audit methods that can be verified.

8. Retired CIs should be retained within the CMDB and have their status updated.

9. All system and application administrators shall follow information security office configuration and architecture hardening baselines/guidelines.

Configuration Recording

Procedures will be in place to ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition. These procedures will also provide for the authorized disposal of configuration items. Procedures will also be in place to keep track of changes to the configuration (e.g., new item, change status).
Logging and control will be an integrated part of the configuration recording system, including reviews of changed records.

Configuration Baseline

Configuration baselines are approved standards that IT is committing to implement to comply with standards, regulatory, and information security guidelines.

IT management will ensure that a baseline of configuration items is kept as a checkpoint to return to after changes.

Status Accounting

IT management will ensure that the configuration records reflect the actual status of all configuration items, including the history of changes.

Configuration Control

These are the procedures that will ensure the existence and consistency of recording of the IT configuration and periodically checking.

Any unauthorized/intentional false configuration change on AUC assets is prohibited and penalized as per AUC internal disciplinary processes.

The use of personal and unlicensed software on AUC-owned digital assets is prohibited. IT management will periodically check the organization's digital assets for unauthorized software. Compliance with the requirements of software and hardware license agreements will be reviewed on a periodic basis.

Configuration Management Procedures

Configuration management procedures will be established to ensure that critical components of the organization's IT resources have been appropriately identified and are maintained. There will be an integrated process whereby current and future processing demands are measured and provide input to the IT resource acquisitions process. Note that the Configuration Management process is embedded in the Change Control Process, including rollback procedures.

Software Accountability

The software will be labeled, inventoried, and properly licensed. Library management software will be used, when possible, to produce audit trails of program changes and to maintain program version numbers, creation-date information, and copies of previous versions.

Roles

IT leadership should appoint the below roles to execute and maintain the processes: -

1. Configuration Manager
2. Configuration Administrator

History/Revision Dates

Origination Date: October 2021

Last Amended Date: October 2021
Next Review Date: October 2025