SMG 3210.11

FDA STAFF MANUAL GUIDES, VOLUME III - GENERAL ADMINISTRATION

INFORMATION RESOURCES MANAGEMENT

INFORMATION TECHNOLOGY MANAGEMENT

ACTIVE DIRECTORY AND MICROSOFT GROUP POLICY OBJECTS POLICY

Effective Date: 05/04/2017
Changed: 05/17/2017

1. PURPOSE

The purpose of the Food and Drug Administration's (FDA) Active Directory (AD) and Group Policy Objects (GPO) policy is to outline requirements for managing and implementing specific configurations for users and computers within FDA's Site and subsidiary Domains and Organizational Units (OU) and registering them within the Microsoft Active Directory system.

2. BACKGROUND

In order to effectively document and control the multiple information technology (IT) entities (users, computers and servers) within the FDA, a standard policy for defining the management of entities within the FDA is required. The management of entities defined as policies) allow options for security, software installation and maintenance, scripts, and folders in a directory system. Additionally a defined architecture for domains and OUs within the FDA allows permissions to be given or taken away for defined subsets of entities.

This document provides a guideline for creating, maintaining and removing entities and groups of entities in the FDA computing network via AD and GPO. This function is the responsibility of the AD GPO support team within the Implementation Branch (IB).

3. POLICY

The following requirements must be followed for managing Active Directory and Group Policy Objects:

A. All new, modified, restored or deleted AD GPO requests must be handled by submitting a Request for Change (RFC) to the Infrastructure Change Control Board (CCB).

B. All AD GPO requests must be in compliance with FDA IT Security policies. If a waiver/exception is required, the FDA IT Security waiver/exception process must be followed.

C. Once a change has been approved, the IB AD GPO support team will implement the request according to the requirements.

D. The IB AD GPO support team will ensure that all AD best practices are followed regarding systems security and strict change control procedures. The IB AD GPO support team will monitor all entities for unauthorized access and modifications and enforce proper RFC submissions to track and control all change requests.

E. The IB AD GPO support team will ensure that information collected and managed will be structured to clearly align with the data requirements of the IT Cost Allocation Process, particularly for those Centers such as OC that require granularity to the Office level.

4. RESPONSIBILITIES

A. FDA Chief Information Officer (CIO).

The FDA CIO provides leadership and direction regarding all aspects of the Agency's information technology (IT) programs and initiatives including operations, records management, systems management, information security, strategic portfolio, and executive coordination and communication activities.

B. FDA Chief Information Security Officer (CISO).

The FDA CISO, appointed by the CIO, serves as the Agency focal point to direct, oversee, and approve the IT security requirements.

C. Deputy CIO, Office of Technology and Delivery (OTD).

The Deputy CIO, OTD is responsible for the execution and implementation of infrastructure operations and application services policy and procedures throughout the FDA enterprise.

D. Office of Information Management and Technology (OIMT), Implementation Branch (IB)

IB AD GPO support team has the overall responsibility for the management and daily maintenance of the AD and all AD GPO requests. Additionally, all changes will be recorded and stored for a minimum of 3 years to meet federal retention mandate.

5. PROCEDURES

This Staff Manual Guide governs the AD GPO process for additions and changes. Specific AD Account procedures can be found in the Division of Infrastructure Operations Services Guide version 3.0 (revised August 21, 2013).

6. REFERENCES

Division of Infrastructure Operations Services Guide – Aug 2013
http://inside.fda.gov:9003/oc/officeofoperations/officeofinformationmanagementtechnology/officeofinformationmanagement/ucm144368.htm

IT Change Control Board (CCB) Overview – April 2015
http://inside.fda.gov:9003/ProgramsInitiatives/CommitteesWorkgroups/ITChangeControlBoard/default.htm

FDA IT Security Waiver Request Process – June 2016 (inside.FDA / Information Technology > Information Security > Communications & Resources > Process and Procedures)

Security Waiver Request – June 2016 (inside.FDA / Information Technology > Information Security > Communications & Resources > Process and Procedures)

Security Waiver Checklist – June 2016 (inside.FDA / Information Technology

> Information Security > Communications & Resources > > Process and Procedures)

End-Of-Life Security Waiver Request – June 2016 (inside.FDA / Information

Technology > Information Security > Communications & Resources > Process and Procedures)

FDA IT Security Policies – June 2016
http://inside.fda.gov:9003/it/ITSecurity/Home/default.htm

7. EFFECTIVE DATE

The effective date of this guide is May 4, 2017.

8. Document History - SMG 3210.11, Active Directory and Microsoft Group Policy Objects Policy

STATUS (I, R, C)	DATE APPROVED	LOCATION OF CHANGE HISTORY	CONTACT	APPROVING OFFICIAL
Initial	04/25/2017	N/a	OO/OIMT/OIM/OTD/ DIO/EIOS/NCOB/ENCT	Todd G. Simpson, FDA Chief Information Officer
Change	05/17/2017	Sect. 2; Sect. 3.D and E; Sect. 4.D.; Sect. 6.	OO/OIMT/OIM/OTD/ DIO/EIOS/NCOB/ENCT	Todd G. Simpson, FDA Chief Information Officer

Back to General Administration, Volume III (2000-3999)