pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Active Directory Architecture

ITP Number ITP-APP030	***Effective Date*** November 20, 2009
Category Application	***Supersedes***
Contact RA-itcentral@pa.gov	***Scheduled Review*** October 2022

1. Purpose

This Information Technology Policy (ITP) establishes policy regarding the Commonwealth's Microsoft Active Directory infrastructure.

2. Scope

This ITP applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth as outlined in the Responsibilities Section.

3. Policy

The Office of Administration, Office for Information Technology (OA/OIT) provides Active Directory services for agencies under the governor's jurisdiction. This ITP addresses the Active Directory infrastructure that has been established for agency use within this environment.

OA/OIT maintains two (2) Active Directory implementations or forests:

CWOPA (or PA.LCL)

APPS (or APPS.STATE.PA.US)

- The CWOPA forest shall be used for internal resources such as, but not limited to, employee security principles (user accounts), security and distribution groups, workstations, servers, Exchange servers, and all objects or services required to support the Commonwealth's standard desktop environment. Only intranet accounts will be granted access to this forest and its resources. Intranet accounts are assigned to Authorized Users under the governor's jurisdiction.

- The APPS forest shall be used for line-of-business and portal applications. This forest shall also be used for applications requiring access by business partners, constituents, or any entity that is not under the governor's jurisdiction. Intranet, extranet, and Internet users may access resources in this forest. Extranet accounts are business partners and other Commonwealth entities not under the governor's jurisdiction. These users are sponsored and managed by Commonwealth agencies under the governor's jurisdiction. Internet users are self-managed, self-registered users who access Commonwealth Web sites for personal business (e.g., applying for hunting licenses).

- All agencies under the governor's jurisdiction shall maintain their intranet user accounts (security principles and distribution groups) and resources (Windows workstations, Windows servers, printers, and other related peripherals) as members of the CWOPA (PA.LCL) forest. This design is known as the Consolidated Forest Architecture; and is illustrated in Figure 1 below.

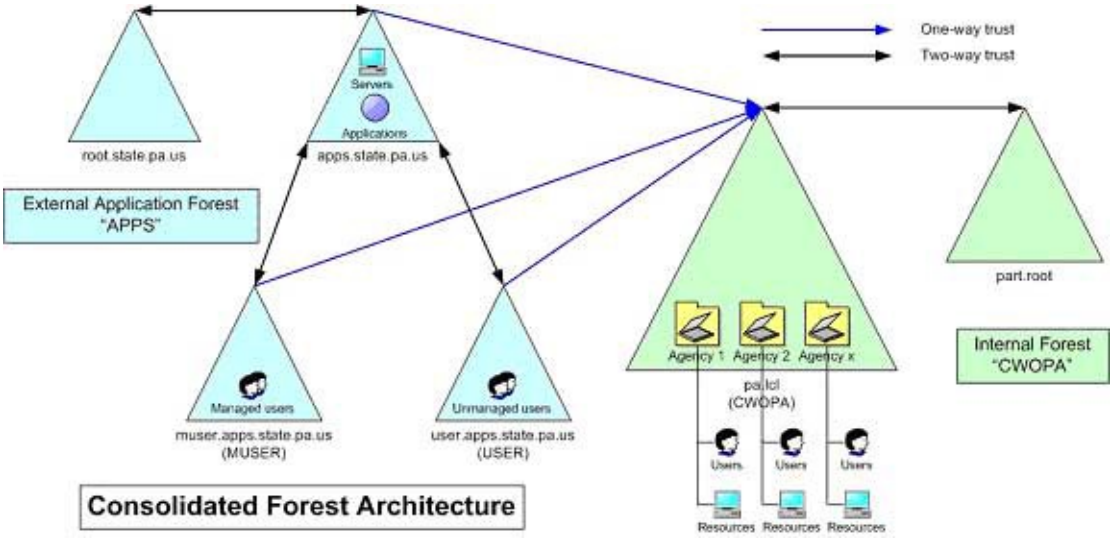

Figure 1 - Consolidated Forest Model

Note: Technical specifications for the CWOPA forest can be found on IT Central on the Enterprise Messaging page. Technical specifications for the ESF forest can be found on IT Central under the Microsoft Active Directory title: *EDC Active Directory Rules of Engagement*

Recognizing the potential need for higher levels of security than natively inherent in the Consolidated Forest Architecture, the Resource Forest Architecture is also supported.

- In addition to the CWOPA and APPS Forests which OA/OIT maintains for the Consolidated Forest Architecture, agencies may have an agency-specific resource forest. The purpose of the resource forest is to contain all agency resources (Windows workstations, Windows servers, printers, and other

related peripherals) and to isolate them from management or access by the CWOPA enterprise administrators, reducing potential security breaches. (See Figure 2.)

- All agencies with a resource forest shall maintain their intranet user accounts (security principles and distribution groups) in the CWOPA (PA.LCL) forest.

- As the establishment and maintenance of a resource forest requires significant resources of time and infrastructure, the implementation of this option should not be taken lightly and should only be considered in instances when the agency is capable of implementing and supporting such an infrastructure. Any requests to implement a resource forest will be treated through the waiver process as described below.

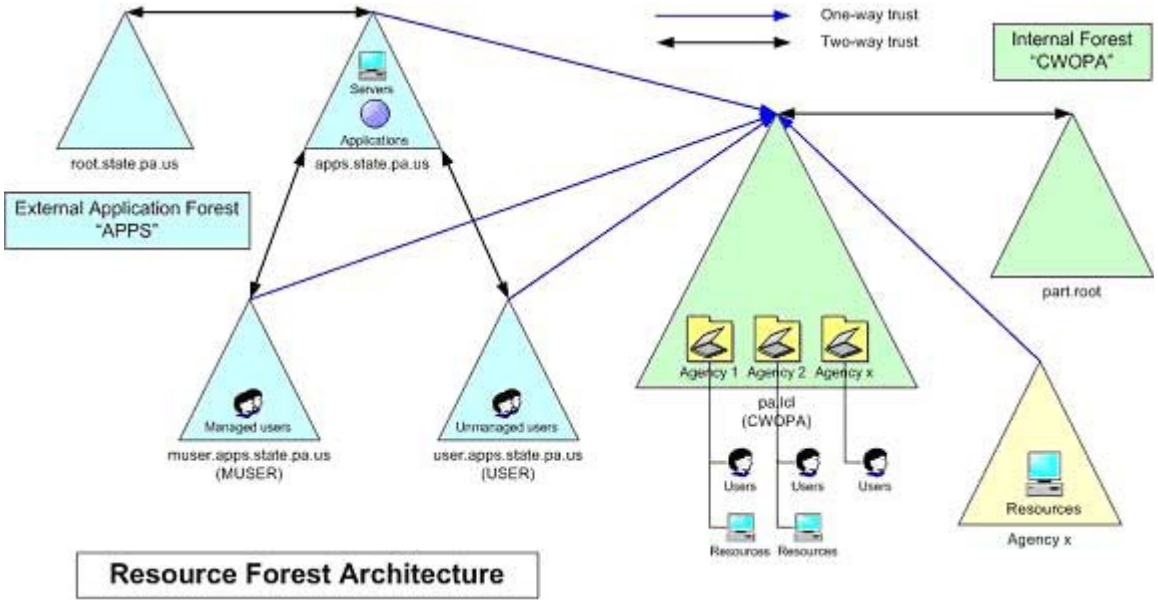

Figure 2 - Resource Forest Model

4. Exemption from this Policy

OA/OIT recognizes that some agencies may have unique Active Directory requirements that are not currently met. Establishing enterprise-wide distributed computing standards is critical if agencies are to use desktop software and collaboration tools effectively and efficiently. Therefore, OA/OIT strongly encourages agencies not to seek exceptions from this policy.

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the enterprise IT policy waiver process outlined in ITP-BUS004 *IT Policy Waiver Review Process*.

If a waiver is granted, the only supported alternative to the Consolidated Architecture is the Resource Forest Architecture as described above.

Criteria for Waivers:

Waivers will primarily be considered for legislative mandates or extreme security concerns if:

- Requirements cannot be mitigated by other means; **or**,
- Cost of mitigation outweighs the cost of a separate architecture; **or**,
- Requirements are not addressed by ongoing or planned OIT enterprise projects.

OA/OIT will review the request and schedule discussions with agency representatives to further understand the request and work collaboratively with the requesting agency to determine the best architecture for the Commonwealth that meets all necessary requirements.

Waiver Approval:

If a waiver request has been approved, the agency shall ensure the following:

- The cost of the approved alternative solution shall be the requesting agency's responsibility, including expenses for the centralized infrastructure, agency-specific components, initial deployment and any additional costs to future enterprise initiatives resulting from the exception.

- The agency resource forest shall follow the technical specifications set forth for the CWOPA forest and adhere to all enterprise standards.

- The agency resource forest shall be subject to the specifications set forth for the Commonwealth's identity management infrastructure. This includes the provisioning and maintenance of user accounts as well as the maintenance of authorizations assigned to those accounts.

5. Responsibilities

5.1 Agencies shall comply with the requirements as outlined in this ITP.

5.2 Third-party vendors, licensors, contractors, or suppliers shall comply with the requirements as outlined in this ITP if they leverage CWOPA for authentication.

6. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- ITP-BUS004 *IT Policy Waiver Review Process*

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	11/20/2009	Base Document	
Revision	10/25/2010	ITB Refresh	
Revision	04/2/2014	ITP Reformat	
Revision	07/14/2014	Removed ITP-PRO001 as waiver reference, inserted ITP-BUS004 as waiver reference	
Revision	10/12/2021	• Third-party vendors added to Scope and Responsibilities • Links updated throughout policy • Scope, Exemption, Related ITPs, Authority and Publication Version Control Sections updated to match current boiler plate language	Revised IT Policy Redline <10/12/2021>