

# *ACCESS.PSU.EDU Forest Polices: Table of Contents*

<b>SUMMARY</b> .....	<b>2</b>
<b>FOREST-WIDE POLICIES</b> .....	<b>2</b>
JOINING THE FOREST POLICY .....	2
LEAVING THE FOREST POLICY .....	3
NAMING CONVENTION FOR THE FOREST .....	4
SCHEMA EXTENSIONS POLICY .....	4
SECURITY POLICY .....	4
POLICY FOR MAKING ADJUSTMENTS TO CURRENT POLICIES AND PROCEDURES.....	5
<b>DOMAIN POLICIES</b> .....	<b>6</b>
DNS POLICY .....	6
CHILD DOMAIN POLICIES .....	6
WINS POLICY.....	7
DHCP SERVER AUTHORIZATION POLICY.....	7
ACTIVE DIRECTORY GROUP POLICY.....	7
<b>ADMINISTRATOR POLICIES</b> .....	<b>7</b>
GENERAL ADMINISTRATION POLICY .....	7
ENTERPRISE ADMINISTRATORS .....	7
DOMAIN ADMINISTRATORS.....	8
CHILD DOMAIN ADMINISTRATORS .....	8
OU ADMINISTRATORS.....	8
<b>MICROSOFT® SERVICES CURRENTLY SUPPORTED IN ACCESS.PSU.EDU</b> .....	<b>9</b>
EXCHANGE® POLICY .....	9
<i>Installing Exchange®</i> .....	9
<i>Policy on Creating and Moving Exchange® Mailboxes</i> .....	9
<i>Exchange® Server Maintenance</i> .....	9
SYSTEMS MANAGEMENT SERVER (SMS) POLICY .....	9
<i>SMS Naming Policy</i> .....	9
<i>Microsoft® Operation Management Server (MOM) Policy</i> .....	9
<i>Live Communication Server (LCS) Policy</i> .....	10
<b>APPLICATION FOR ENROLLMENT INTO THE ACCESS.PSU.EDU FOREST AS A CHILD DOMAIN</b> .....	<b>11</b>

# The ACCESS.PSU.EDU Forest Policies

## Summary

The purpose of offering Active Directory® services to Penn State colleges, departments, and academic units (referred to as units herein) is to provide the University community with maximum flexibility and control over their own Microsoft Active Directory®-based technology infrastructures. ASET/ITS is offering this service so that Penn State organizations may leverage their respective Windows® infrastructures with our core authentication (Kerberos 5) and authorization (LDAP) services for account management. This deployment of Active Directory® is integrated with the current, open standards-based infrastructure ASET/ITS uses for core digital credential management. This provides maximum flexibility for all units, Microsoft® dependent or not.

The goal of this working document is to facilitate the deployment process for sites currently engaged in designing an Active Directory® network. ASET/ITS primary intent is to guide units in evaluating the complicated design trade-offs associated with Active Directory® by providing detailed information about the cost and implications of different Active Directory® elements that would be the most difficult to change once deployed.

The intention of Penn State's ACCESS.PSU.EDU deployment plan is to create a stable infrastructure based on supported Microsoft® technologies, to promote autonomy among different Penn State units, either as Child Domains or Organizational Units (OUs) in the ACCESS Forest. Implementations such as account management in the OUs or Child Domains, group policies written and applied by the organization, and any technology that will not have an affect outside of a organization's scope, are up to the discretion of that unit.

## Forest-wide policies

### Joining the Forest Policy

All Penn State organizations may join the Forest. There are four options for working with Penn State Access Accounts. ASET/ITS **fully supports** two of those options:

1. An OU at the level of the Parent domain (OU) in ACCESS.PSU.EDU as:  
OrgUnit\ACCESS.PSU.EDU
2. A Child Domain in ACCESS as: ChildDom.ACCESS.PSU.EDU

ASET/ITS is responsible for backups and disaster recovery, monitoring, security updates, and patches for the ACCESS Domain and the ASET/ITS root domain infrastructure under ACCESS/PSU/EDU.

ASET/ITS also **supports but is not directly responsible for** the administration of two additional options for joining ACCESS:

3. A one-way trust; ASET/ITS is only responsible for establishing the initial trust relationship
4. Joining the ACCESS Forest as an OU under an existing Child Domain

To join the domain, interested participants must complete the application form (included on the last page of this document) and e-mail it to <[WIN-AD@aset.psu.edu](mailto:WIN-AD@aset.psu.edu)>. The form

lists all requirements, including the designation of the organizational points of contact, each of whom will be responsible for the installation, operation, and maintenance of the Child Domain or OU. By joining the Forest, participants must agree to abide by all of the regulations and policies ASET/ITS has defined in this document, in addition to applicable security and computing policies, guidelines, and regulations already established at the University. Please refer to <<http://www.psu.edu/policies/>> for information.

Once the application is approved, each designated contact will receive an administrative account, which he/she will need to use for installation and administration of the Child Domain or OU. No matter which option is chosen, ASET/ITS endeavors to delegate complete administration roles and responsibilities for the Child Domain or OU to the designated points of contact. Child Domain or OU administration will be governed by the organization itself, provided that it will not negatively impact the rest of the Forest.

1. Organizational Unit (OU) in ACCESS/PSU/EDU: This option requires responsibility for client administration only. ASET/ITS handles all domain administration, inclusive of disaster recovery and account management; however, ASET/ITS currently does not offer a Domain Controller (DC) local to organizations' sites.
2. Child Domain under ACCESS/PSU/EDU: This option requires administration of the Child Domain, inclusive of client administration, all domain administration, disaster recovery planning, monitoring of events such as replication, and ensuring the security and stability of the data in the Child Domain. ASET/ITS monitors replication to the unit's machines from ASET/ITS machines but does not do so for machines in the domain. A unit's disaster recovery plan is handled through the unit itself and not through ASET/ITS. If a unit experiences an irrevocable disaster that presents an adverse impact on the Forest, ASET/ITS will orphan the domain. In addition, if a unit cannot recover in a timely manner, ASET/ITS will orphan the domain.
3. One-Way Trust from a separate AD Forest: This option gives units a direct trust to ASET/ITS-managed KDCs. Units are responsible for all administration tasks inclusive of user management, group management, disaster recovery, and all other administrative tasks. A One-Way Trust from other Penn State Forests requires the unit to be entirely responsible for their own systems. ASET/ITS only supports the actual trust relationship to the K5 server.
4. OU in Child Domain: This option requires units to work directly with the Child Domain Administrators concerning their respective policies. They are responsible for all their Child Domain Administration inclusive of disaster recovery as well as local and administrative account management. Child Domains may or may not offer the ability for OUs to create and maintain Domain Controllers. This, as well as any policy within their own Child Domain, is at the discretion of the unit's policies. In the case where the Child Domain adds another DC for an OU, the Enterprise Administrators for ACCESS.PSU.EDU must be involved.

### **Leaving the Forest Policy**

An organization is free to leave the Forest at any time. In order to leave the Forest, an administrative point of contact must send a request to <[win-ad@aset.psu.edu](mailto:win-ad@aset.psu.edu)> to arrange removal of either the Child Domain or the delegated OU. This must be done prior to the removal of the last Domain Controller for Child Domains and after the removal of the last object under a unit's OU. It is extremely important to the health of the Forest that this is arranged before a unit removes its final Domain Controller.

## Naming Convention for the Forest

In order to keep all names in the domain unique, each unit will be assigned a two-to-three letter prefix upon joining the ACCESS.PSU.EDU Forest. This prefix must be used for naming groups, computers, group policies, and other objects in Active Directory® created or owned by the unit. A list of prefixes is found at:

<[http://aset.its.psu.edu/docs/windows/active\\_directory/](http://aset.its.psu.edu/docs/windows/active_directory/)>. An administrative point of contact for an organization is responsible for ensuring that all machine names throughout the organization are unique.

## Schema Extensions Policy

All schema extensions must be requested by filling out this form. The request will be reviewed and accepted or declined. Schema extension testing will take place in the pre-production environment and will be approved or denied based on the results of the testing. Testing will last a minimum of three months and will continue until all potential conflicts/problems are identified. Approval is based on the overall impact to the Forest. Overall impact is based on, but not limited to, the following criteria:

- Privacy:** Sensitivity to the privacy of personal data, per University and federal policy and law regarding institutional data, is mandatory. Please refer to <<http://www.psu.edu/registrar/conf.html>>.
- Appropriateness:** Conflicts regarding data locality are inevitable. ASET/ITS needs to preserve the existing authoritative data sources while balancing the flexibility that a schema extension may create. Data belonging in the Penn State Online Directory (LDAP) should be added there rather than in Active Directory®; this prevents ASET/ITS from creating conflicting and redundant sources of data.
- Correct ACLs:** The default ownership and security ACLs of objects and attributes implemented by the schema change should be set correctly.
- Conflict:** Data in Active Directory® should not conflict with directory objects or attributes.
- Interference:** Schema extensions must not interfere with existing production services such as Exchange®, LCS, SMS, etc.
- Sustainability:** Sustainability includes items such as the number of added attributes and the load generated on the resources.

## Security Policy

Implementations of services that will affect the Forest must be tested first in the pre-production environment. The ultimate goal is to allow organizations and Child Domains the ability to use any of the supported Microsoft® servers and technologies that are safe and stable for the entire community.

The “WIN-AD” Team, will periodically conduct audits of the Forest to ensure compliance with Penn State policies for the security and safety of the entire Active Directory® community whose production systems rely upon these services. Any Child Domain is

welcome to test the effectiveness of their respective backup and disaster recovery systems in the ASET/ITS testing environment. The Enterprise Administrators for ACCESS.PSU.EDU also offer to conduct periodic site visits to any unit running from ACCESS to help determine strengths and weaknesses at a location and to help units work successfully under ACCESS.

ACCESS Enterprise Administrators also reserve the right to take action to isolate any organization or Child Domain in the event of an emergency or in the event that a violation of security has occurred, after notifying and working with the unit (just as Penn State Security Operations and Services currently notifies responsible administrators and requests compromised machines to be removed temporarily from the network until they have been secured). This type of action will be handled in accordance with Penn State policies and guidelines.

Enterprise Administrators will work with any unit in the Forest in the event of an emergency, but ultimately, the WIN-AD Team is responsible for ensuring the stability and security of the entire Forest and will take steps to ensure that a unit's production systems are not endangered by any unforeseen event.

### **Policy for Making Adjustments to Current Policies and Procedures**

The WIN-AD Team will periodically host "Town-Hall" and update meetings open to the public but specifically targeted for the needs of current subscribers in ACCESS.PSU.EDU. These forums will be designed to allow open discussion and debate of any current procedures and policies. Any unit within the Forest may recommend changes and modifications, either minor to their own scope or large-scale to a Forest-wide schema change.

Current information is documented at: <<http://aset.its.psu.edu/docs/windows/>>. This site will provide, in addition to the existing overview information, "How To" information, and a Web version of this policy document, required practices associated with subscription to the Active Directory® service. Required practices, in this context, are the policies essential to maintaining the security and stability of the system, inclusive of existing Penn State policies and guidelines. Also included will be suggested Best Practices - a recommended list of resources and operating guidelines and procedures for the Active Directory® community at Penn State.

The WIN-AD Team reserves the right to final decision making in order to preserve the health and security of the entire Forest. Any unit is welcome to test and prove or debate a change by first testing it in the pre-production environment hosted by ASET/ITS for this purpose. Cutting-edge technology will be relegated to the true beta testing environment before being allowed to run in the pre-production environment. Implementations that require schema changes or anything with Forest-wide impact must first be tested within the pre-production Forest by the organizations making the request and any other interested parties.

Enterprise Administrators will work toward maintaining the proper stewardship of the Active Directory® domain, providing stability and conflict resolution. In order to reasonably protect the services and interests of all organizations represented in the Forest, it may be necessary to re-evaluate the deployment of any technology that results in instability of the entire system or that fails to pass testing during the pre-production phase.

## Domain Policies

### Domain Trusts Policy

Domains outside the Forest will not be allowed to maintain or create a trust relationship with the ACCESS domain, except for those domains that are in the process of migrating to the tree. The ACCESS domain will not trust domains outside the Forest for any other reason. Domain migrations should occur in a timely manner to reduce a prolonged security risk via the trust, and the trust relationship will not be allowed for an indefinite period of time. Child Domains may trust a domain external to the Forest, but only for migration reasons.

### DNS Policy

Each Child Domain is responsible for the installation, operation, and maintenance of their respective DNS servers. These DNS servers will be responsible for the five domain sub-zones that contain SRV records. These include:

- \_msdcs.yourdomain.access.psu.edu
- \_tcp.yourdomain.access.psu.edu
- \_udp.yourdomain.access.psu.edu
- \_sites.yourdomain.access.psu.edu
- DomainDnsZones.yourdomain.access.psu.edu

Each Child Domain and OU is responsible for the maintenance of DNS records for individual machines that reflect the organizations hierarchy. The machine DNS suffix will not match the Active Directory® domain name. For example: a machine in the ACCESS.PSU.EDU domain would be called **dc-ws1.access.psu.edu** in a Microsoft-centric environment. In this environment, a machine in the ACCESS.PSU.EDU domain would be called **dc-ws1.aset.psu.edu**. The machine name **dc-ws1.access.psu.edu** can be maintained by the organization or by ASET/ITS, whichever way is permitted per the organization's setup decision. However, the organization will install, operate, and maintain the five domain sub-zones listed above on their respective DNS servers.

### Child Domain Policies

- A Child Domain must have a minimum of two full-time IT administrators as points of contact for the domain.
- The Child Domain must provide IP address information for a minimum of two servers to operate as the Domain Controllers for the Child Domain. The equipment used must meet minimum recommended hardware specifications from Microsoft® for Windows® 2003 servers. At minimum, the following information is required:
  - Server contact(s) and location; a backup contact
  - Hardware and operating system/version
  - Main functions and applications, if applicable
- The Domain Controllers may operate only as Domain Controllers. This means that the only services they can run are Kerberos, LDAP, and DNS.
- Additional software may not be installed on the Domain Controllers.
- Each Child Domain is responsible for the installation, operation, and maintenance of

their respective Domain Controllers. This includes, but is not limited to, patching, upgrading, and recovering the domain.

- The Child Domain must have a published disaster recovery plan. This plan must include at least Active Directory® database corruption, data corruption, and hardware failure.
- Any Child Domain is welcome to test the effectiveness of their respective backup and disaster recovery systems in the separate testing environment maintained by ASET/ITS.

### **WINS Policy**

A Child Domain may install, operate, and maintain a Domain's own WINS server. This server must be configured to replicate with a WINS server in the root domain ACCESS.PSU.EDU. An OU may setup client machines to use one of the WINS servers in the ACCESS.PSU.EDU domain.

### **DHCP Server Authorization Policy**

DHCP server authorization requests must be sent to <[win-ad@aset.psu.edu](mailto:win-ad@aset.psu.edu)>. Requests will be processed and units will receive a confirmation e-mail from a WIN-AD Team member. Active Directory® requires any DHCP or RRAS servers to be authorized before they can be functional anywhere in the Forest.

### **Active Directory Group Policy**

It is the intention of the WIN-AD Team to not force group policies down to an OU or Child Domain; however, the WIN-AD Team reserves the right to do so as necessary. Any group policies applied to the Domain user's OU containing all skeleton accounts may be overridden in an organization.

## **Administrator Policies**

### **General Administration Policy**

A user's Penn State Access Account will not be delegated any administrative rights. Rather, a special administrative account must be created and the appropriate rights will be delegated to this account.

### **Enterprise Administrators**

Currently, there are two Enterprise Administrators. These administrators are responsible for the underlying Forest infrastructure. This level of authority mandates a high level of responsibility, including being subject to an audit. Actions of the Enterprise Administrators are audited and available for review by Penn State Security Operations and Services. Members of this group are restricted to select WIN-AD Team members only.

### **Domain Administrators**

In the ACCESS.PSU.EDU domain, there are no members of the Domain Administrators. The Enterprise Administrators are tasked with all duties related to domain administration. Within a Child Domain, there will be members of this group. These members carry a high responsibility and must be audited. Membership must be carefully considered.

### **Child Domain Administrators**

The WIN-AD Team has created a group called Child Domain Administrators. This group is responsible for installing a Child Domain as well as setting Exchange® mailboxes. The members of this group are limited to the two points of contact for each Child Domain.

### **OU Administrators**

OU Administrators are limited to only objects under their respective OU. These include user object, computer object, and OU containers. They have the ability to link GPOs to containers, as well as set permissions on any object under their OU. An OU administrator will not have administrative rights above their respective OU, with the exception of the “PSUComputers” container. This is the container where computer accounts may be added and then moved at another time by the creator of the account. OU Administrators have the right to create computer accounts in this container, but only the creator has the ability to move the account.

## **Microsoft® Services Currently Supported in ACCESS.PSU.EDU**

### **Exchange® Policy**

#### **Installing Exchange®**

In order to install an Exchange® server, a units must send a request to <[win-ad@aset.psu.edu](mailto:win-ad@aset.psu.edu)>. Upon approval, the organization will receive a delegated Exchange® Administration group, an Exchange® Administration account, and the domain point of contact will be added to the Exchange® users group. This group has the necessary privileges to set mailboxes for users, but does not have privileges to administer the Exchange® server. The Exchange® Administrative account will have the permissions to administer the Exchange® server but not to change permissions on the Exchange® server. This will limit administrators to only their respective administrative groups and will not permit access to other organizations' Exchange® servers.

#### **Policy on Creating and Moving Exchange® Mailboxes**

Mailboxes will be available on a first come, first served basis. The first organization to assign a user a mailbox on their respective Exchange® server assumes complete responsibility for the client. The Exchange® Administrator who creates the account implies their agreement to handle all support dealing with a client's mailbox as well. A unique client account may only have one mailbox located on one Exchange® server in the Forest. This means that mailboxes cannot be moved or deleted by the administrators without some coordination and communication across the Forest groups. In order to move a mailbox, the administrator losing the client, the administrator requesting the client, and the client must send a request to <[win-ad@aset.psu.edu](mailto:win-ad@aset.psu.edu)>.

#### **Exchange® Server Maintenance**

An organization is responsible for proper maintenance of their respective Exchange® server, including backups, patching, a disaster recovery plan, and support for the client mailboxes.

### **Systems Management Server (SMS) Policy**

#### **SMS Naming Policy**

SMS site names will correspond with an organization's assigned prefix.

#### **Microsoft® Operation Management Server (MOM) Policy**

Not available at this time.

**Live Communication Server (LCS) Policy**  
Not available at this time.

## **Application for Enrollment into the ACCESS.PSU.EDU Forest As a Child Domain**

---

**Organization Name:**

**Name of Child Domain:**

**DNS Name of first DC (must resolve to valid IP):**

(Example: DC=cwcdc1.aset.psu.edu, Domain=CWC.ACCESS.PSU.EDU)

### **1<sup>ST</sup> Point of Contact**

Name:

Office Address:

Office Phone Number:

Mobile Phone Number:

E-mail Address:

### **2<sup>nd</sup> Point of Contact**

Name:

Office Address:

Office Phone Number:

Mobile Phone Number:

E-mail Address: