



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-02-01-2013

DIVISION OF INFORMATION TECHNOLOGY

Active Directory Standard

Date of Last Revision 03/17/2013

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Purpose

- a. To define an effective, scalable, secure and manageable Active Directory™ forest design and to facilitate one standardized infrastructure for the State's Active Directory™ which will reduce multiple sign-ons and reduce total cost of ownership for the State's network operations. The Division of Information Technology (DoIT) shall govern the implementation and operation of Microsoft's Active Directory™ on the State's enterprise network.

2. Definitions

- a. **Domain** - In Microsoft Active Directory, a logical collection of network objects (computers, users, devices) which shares a common directory database is defined as a domain. It provides access in a centralized management interface for computer, user accounts and group object for ease of administration. Each domain has its own security policies and security relationships with other domains.
- b. **Schema** - The definition of an entire Active Directory™ database; the universe of objects that can be stored in the directory is defined in the schema. For each object class, the schema defines what attributes an instance of the class must have, and what object class can be a parent of the current object base.
- c. **Domain Name Service** - Domain Name Service (DNS) is a hierarchical distributed database used for name/address translation and client server rendezvous. Domain Name Service is the namespace used on the Internet to translate computer and service names into TCP/IP addresses. Active Directory™ uses DNS as its location service which enables clients to find domain controllers using DNS queries.
- d. **Sub-Domains** - Any child of a domain zone.
- e. **Site** - A site is defined as one or more well connected TCP/IP subnets.

3. Scope

- a. This standard applies to any Agency's implementation of Active Directory™. This standard covers implementation of any Active Directory™ forest established on the State's enterprise network within a production environment. Although there are touch points between Active Directory™ and the RI.Gov Domain Naming Convention the two are not directly related.

4. Standard

a. Agencies, Political Subdivisions, and other entities participating in the State's Active Directory™ shall comply with all Active Directory™ prescribed standards, processes, and specifications defined by the Division of Information Technology. DoIT will develop specific procedures and sub-process that Agencies will follow to implement Active Directory™.

b. Structure

(i.) The initial design is structured to take advantage of the flexibility of domains and Organizational Units (OUs) in Active Directory™. An empty forest root is implemented to maximize security of the forest root; child domains will be created as necessary; and recognize the differing roles among the Division of Information Technology, Agencies. A single forest design is employed to reduce total costs, create a single Exchange organization, and ease administration. Child domains are used to separate administration of systems maintained by DoIT and their respective agencies. Toplevel Organizational Units (OUs) are created for each state agency in the accounts domain to allow application of separate group policy objects. All OU designs are governed by the Organizational Unit Standard and must be approved by the DoIT.

c. Single Forest

- (i.) There is one enterprise forest structure for the State of Rhode Island, with justified exceptions. DoIT is responsible for the availability of the State Forest infrastructure for Active Directory™ services and will retain control of the Forest Root Domain. DoIT will be responsible for maintaining Active
- (ii.) Directory™ services to ensure business continuity for each Agency.
- (iii.) Requests for enterprise Schema modifications and security policy changes must be approved and performed by DoIT.

d. Domain Plan

- (i.) There will be a single, dedicated root domain for any/all forests. This will provide a controlled environment for forest wide change management and limit the amount of replicated data. The root domain will contain no user accounts and will be used strictly as an empty domain to manage the schema, global catalog, site topology, security and enterprise policy.
- (ii.) DoIT will be responsible for the operation of the enterprise forest root domain.
- (iii.) Each Agency shall justify the creation of its own child domain under the enterprise forest root domain. Based on business requirements and upon approval of DoIT, Agency sub domains may be created.
- (iv.) All child domains established beneath the State's enterprise domain will be owned by DoIT and the Agencies will oversee management of their domains in compliance with current State Active Directory™ Standards. These child domains will be established within the State's single Forest as defined in the Forest Standard. The Agency domains will contain Agency owned and operated Application and Databases servers with respective administration accounts to maintain these servers only.

- (v.) There will be no accounts in the domain administered exclusively by an outside vendor. Each agency will have an Organizational Unit (OU) structure within this domain that will contain the Agencies users, computers, file and print servers. The Agencies will manage their OU structure through their authorized child domain.

e. Domain Control and Security

- (i.) Membership in the dedicated enterprise forest root domain Schema, Enterprise and Domain Administration groups is restricted and controlled by DoIT and implemented by DoIT. DoIT will maintain a high level of security on all levels to ensure only properly authorized changes are implemented.

f. Domain Name Service (DNS) Zones

- (i.) See Domain Name Service Standard.

g. Organization Unit (OU)

- (i.) Each Agency manages its objects in the directory, while the Division of Information Technology (DoIT) manages the configuration of the directory service. The Agency is responsible for completing an initial OU design based on Active Directory™ standards. All designs must be submitted to DoIT for approval.

h. Organizational Control

- (i.) The (Agency's) child domain owner/designatee is responsible for all Organization Units (OU's) which include objects within their sub-domain.

i. Sites Plan

- (i.) The Site Plan defines an Active Directory™ site as a set of well-connected Internet Protocol (IP) subnets.
- (ii.) All sites are to be designed by the Agency or Agencies affected in conjunction with the DoIT. Agencies' will design a site topology that reduces Wide Area Network (WAN) utilization during Active Directory™ replication and client logon.
- (iii.) The Agency or Agencies affected are responsible for the submission of the site topology design to DoIT.
- (iv.) Any Wide-Area-Network (WAN) design changes shall be reported to the Active Directory™ administrative group.

j. Site Control

- (i.) The Agency's responsibilities include communication and coordination on the following:
 1. Changes to site topology
 2. Location of domain controllers

k. Backup and Disaster Recovery

- (i) Backup and recovery of the forest root domain will be the sole responsibility of DoIT. The backup and recovery of the child domains will be the sole responsibility of the agencies.

l. Active Directory™ Replication

- (i) Replication of the enterprise forest root domain will be the responsibility of DoIT. Agencies are responsible for the replication of Active Directory™ within their sub-domain and the communication to the enterprise.

m. Active Directory™ Domain Naming

- (i) The name of each child domain under ri.gov will consist of the acronym that has been selected for the Agency (i.e. DOR.RI.GOV). These child domains will only be granted based on special requirements demonstrated within RPC request. Any agency that cannot demonstrate any special requirements that would require the creation of a child domain shall be placed within an organization unit under enterprise.ri.gov domain.

1. All Departments and/or Divisions not currently named, will be created at the time of migration or creation. All department and subdepartment identification must be approved prior to use.

Department	Department Identification	SubDepartment Name	SubDepartment Identification	Example
Department of Behavioral Healthcare, Development Disabilities & Hospitals	BHDDH			
	BHDDH	Administration	ADM	BHDDH-ADM-XXXX
	BHDDH	Behavioral Healthcare	BH	BHDDH-BH-XXXX
	BHDDH	Development Disabilities	DD	BHDDH-DD-XXXX
	BHDDH	Community Living & Support	CLS	BHDDH-CLS-XXXX
	BHDDH	Eleanor Slater Hospital	ESH	BHDDH-ESH-XXXX
Department of Business Regulations	DBR			
	DBR	Director's Office	DIR	DBR-DIR-XXXX
	DBR	Division of Regulatory Standards, Compliance and Enforcement	RSCE	DBR-RSCE-XXXX
	DBR	Banking	BANK	DBR-BANK-XXXX
	DBR	Commercial Licensing	CL	DBR-CL-XXXX
	DBR	Racing & Athletics	RA	DBR-RA-XXXX
	DBR	Design Professionals Division	DP	DBR-DP-XXXX
	DBR	Insurance Regulation Division	IR	DBR-IR-XXXX
	DBR	Securities Regulation Division	SR	DBR-SR-XXXX
	DBR	Board of Accountancy	OMB	DBR-OMB-XXXX
	DBR	Office of Health Insurance Commissioner	RITS	DBR-RITS-XXXX
Department of Children, Youth & Families	DCYF			
	DCYF	Central Management	CM	DCYF-CM-XXXX
	DCYF	Child Welfare	CW	DCYF-CW-XXXX

	DCYF	Day Care	DC	DCYF-DC-XXXX
	DCYF	Office of the Director	DIR	DCYF-DIR-XXXX
	DCYF	Foster Care	FC	DCYF-FC-XXXX
	DCYF	Juvenile Corrections	JC	DCYF-JC-XXXX
	DCYF	Licensing & Permanency Support	LPS	DCYF-LPS-XXXX
	DCYF	Office of Management Information Systems	MIS	DCYF-MIS-XXXX
	DCYF	Office of Management and Budget	OMB	DCYF-OMB-XXXX
	DCYF	Rhode Island Training School	RITS	DCYF-RITS-XXXX
	DCYF	Support Services	SS	DCYF-SS-XXXX
Department of Environment Management	DEM			
	DEM	Coastal Resources	CR	DEM-CR-XXXX
	DEM	Division of Forest Environment	DOF	DEM-DOF-XXXX
	DEM	Administrative Adjudication	AAD	DEM-AAD-XXXX
	DEM	Agriculture	AGR	DEM-AGR-XXXX
	DEM	Air Resources	AIR	DEM-AIR-XXXX
	DEM	Criminal Investigation	CI	DEM-CI-XXXX
	DEM	Director's Office	DO	DEM-DO-XXXX
	DEM	Emergency Response	ER	DEM-ER-XXXX
	DEM	Human Resources	HR	DEM-HR-XXXX
	DEM	Legal Services	LGL	DEM-LGL-XXXX
	DEM	Licensing & Registration	LR	DEM-LR-XXXX
	DEM	Management Information Systems	MIS	DEM-MIS-XXXX
	DEM	Management Services	MS	DEM-MS-XXXX
	DEM	Office of Compliance & Inspections	OCI	DEM-OCI-XXXX
	DEM	Office of Technical & Customer Assistance	OTCA	DEM-OTCA-XXXX
	DEM	Office of Waste Management	OWM	DEM-OWM-XXXX
	DEM	Office of Water Resources	OWR	DEM-OWR-XXXX
	DEM	Planning & Development	PD	DEM-PD-XXXX
	DEM	Strategic Planning & Policy	SPP	DEM-SPP-XXXX
	DEM	Fish & Wildlife	FW	DEM-FW-XXXX
	DEM	Law Enforcement	LE	DEM-LE-XXXX
	DEM	Parks & Recreation	PR	DEM-PR-XXXX

Department of Human Services	DHS			
	DHS	Child Care	CC	DHS-CC-XXXX
	DHS	Center for Child and Family Health	CFH	DHS-CFH-XXXX
	DHS	Office of the Director	DIR	DHS-DIR-XXXX
	DHS	Financial Management	FM	DHS-FM-XXXX
	DHS	Fraud, Collections, Claims & Recovery Unit	FRED	DHS-FRED-XXXX
	DHS	Division of Health Care Quality	HCQ	DHS-HCQ-XXXX
	DHS	Individual and Family Support	IFS	DHS-IFS-XXXX
	DHS	Legal Services	LS	DHS-LS-XXXX
	DHS	Long Term Care and GPA Services	LTC	DHS-LTC-XXXX
	DHS	Management Services	MS	DHS-MS-XXXX
	DHS	Office of Child Support Services	OCSS	DHS-OCSS-XXXX
	DHS	Office of Institutional and Community	OIC	DHS-OIC-XXXX
	DHS	Office of Rehabilitation Services	ORS	DHS-ORS-XXXX
	DHS	Systems and Data	SD	DHS-SD-XXXX
	DHS	SNAP	SNAP	DHS-SNAP-XXXX
	DHS	Veterans Home	VH	DHS-VH-XXXX
	DHS	Veterans Memorial Cemetery	VMC	DHS-VMC-XXXX
Department of Labor and Training	DLT			
	DLT	Labor Market Information	LMI	DLT-LMI-XXXX
	DLT	Temporary Disability Insurance	TDI	DLT-TDI-XXXX
	DLT	Unemployment Insurance	UI	DLT-UI-XXXX
	DLT	Workers' Compensation	WC	DLT-WC-XXXX
	DLT	Workforce Development	WD	DLT-WD-XXXX
	DLT	Workforce Regulation and Safety	WRS	DLT-WRS-XXXX
Department of Administration	DOA			
	DOA	Office of Accounts and Control	AC	DOA-AC-XXXX
	DOA	Office of Budget	BGT	DOA-BGT-XXXX
	DOA	Bureau of Audits	BOA	DOA-BOA-XXXX
	DOA	Capitol Police	CAP	DOA-CAP-XXXX
	DOA	Capitol Projects	CP	DOA-CP-XXXX

	DOA	Central Business Office	CBO	DOA-CBO-XXXX
	DOA	Director's Office	DIR	DOA-DIR-XXXX
	DOA	Division of Information Technology	DoIT	DOA-DoIT-XXXX
	DOA	Office of Energy Resources	OER	DOA-OER-XXXX
	DOA	Facilities Management	FM	DOA-FM-XXXX
	DOA	Human Resources	HR	DOA-HR-XXXX
	DOA	Legal Services	LS	DOA-LS-XXXX
	DOA	Office of Digital Excellence	ODE	DOA-ODE-XXXX
	DOA	Office of Library Services	OLIS	DOA-OLIS-XXXX
	DOA	Office of Management and Budget	OMB	DOA-OMB-XXXX
	DOA	Statewide Planning	PLA	DOA-PLA-XXXX
	DOA	Public Safety Grant Administration	PSGAO	DOA-PSGAO-XXXX
	DOA	Office of Purchases	PUR	DOA-PUR-XXXX
	DOA	Sheriffs	SHE	DOA-SHE-XXXX
	DOA	Training Office	TRAIN	DOA-TRAIN-XXXX
	DOA	Workers' Compensation	WC	DOA-WC-XXXX
Department of Corrections	DOC			
	DOC	Director's Office	DIR	DOC-DIR-XXXX
	DOC	Division of Administration	ADM	DOC-ADM-XXXX
	DOC	Division of Rehabilitative Services	RS	DOC-RS-XXXX
	DOC	Adult Correctional Institutions	ACI	DOC-ACI-XXXX
	DOC	Support Services	SS	DOC-SS-XXXX
	DOC	Parole Board	PB	DOC-PB-XXXX
	DOC	Victims Information & Notification Everyday	VINE	DOC-VINE-XXXX
Department of Health	DOH			
Department of Revenue	DOR			
	DOR	Director's Office	DIR	DOR-DIR-XXXX
	DOR	Division of Motor Vehicles	DMV	DOR-DMV-XXXX
	DOR	Legal Services	LS	DOR-LS-XXXX
	DOR	Employer Taxation	ETAX	DOR-ETAX-XXXX
	DOR	Municipal Finance	MF	DOR-MF-XXXX
	DOR	Office of Revenue Analysis	ORA	DOR-ORA-XXXX
	DOR	Division of Taxation	TAX	DOR-TAX-XXXX
Department of Transportation	DOT			
	DOT	Audit Unit	AUD	DOT-AUD-XXXX

	DOT	Capital Programming Section	CAP	DOT-CAP-XXXX
	DOT	Construction Unit	CON	DOT-CON-XXXX
	DOT		CSP	DOT-CSP-XXXX
	DOT		CSV	DOT-CSV-XXXX
	DOT	Design Office	DES	DOT-DES-XXXX
	DOT	Director's Office	DIR	DOT-DIR-XXXX
	DOT	Environmental Office	ENV	DOT-ENV-XXXX
	DOT	Final Review Unit	FIN	DOT-FIN-XXXX
	DOT	Fleet Operations Section	FLT	DOT-FLT-XXXX
	DOT		FNL	DOT-FNL-XXXX
	DOT	Human Resources	HR	DOT-HR-XXXX
	DOT	Intermodal Planning Unit	INT	DOT-INT-XXXX
	DOT	Legal Services	LEG	DOT-LEG-XXXX
	DOT	Materials Office	MAT	DOT-MAT-XXXX
	DOT	Maintenance	MNT	DOT-MNT-XXXX
	DOT	Office of Highway Safety	OHS	DOT-OHS-XXXX
	DOT	Public Affairs	PA	DOT-PA-XXXX
	DOT		POL	DOT-POL-XXXX
	DOT	Real Estate Section	REL	DOT-REL-XXXX
	DOT	Survey Office	SRV	DOT-SRV-XXXX
	DOT	Traffic Management Center	TMC	DOT-TMC-XXXX
Emergency Management Agency	EMA	-----	---	EMA-XXXX
Governor's Office	GOV	-----	---	GOV-XXXX
Lt. Governor's Office	LTG	-----	---	LTG-XXXX
Office of the General Treasurer	GT	-----	---	GT-XXXX
Boards and Commissions	Department ID	SubDepartment Name	SubDepartment ID	Example
Municipal Police Training Academy	MPTA	-----	---	MPTA-XXXX
Coastal Resources Management Council	CRMC	-----	---	CRMC-XXXX
Water Resources Board	WRB	-----	---	WRB-XXXX
Board of Elections	BOE	-----	---	BOE-XXXX
Human Rights Council	HRC	-----	---	HRC-XXXX
Office of Child Advocate	OCA	-----	---	OCA-XXXX
Department of Public Utilities Commission	DPUC	-----	---	DPUC-XXXX
Ethics Commission	ETHICS	-----	---	ETHICS-XXXX

Fire Safety Board	FSC	-----	---	FSC-XXXX
State Fire Marshal	SFM	-----	---	SFM-XXXX
Governor's Commission on Disability	GCD	-----	---	GCD-XXXX
Historical Preservation Heritage Commission	HPHC	-----	---	HPHC-XXXX
Mental Health Advocate	MHA	-----	---	MHA-XXXX
Public Utilities Commission	PUC	-----	---	PUC-XXXX
Commission on the Deaf & Hard of Hearing	CDHH	-----	---	CDHH-XXXX
Commission on Women	RICW	-----	---	RICW-XXXX
State Council on the Arts	RISCA	-----	---	RISCA-XXXX

- (ii.) The workstation names will be a maximum length of 15 characters and constructed as follows; The first 3 or 4 characters will be the agency code followed by a hyphen the next 3 or 4 characters will be the agency unit/section, again followed by a hyphen, with the remaining 5 to 7 characters being a Department defined unique identifier and must be consistent throughout the department.
- (iii.) Workstation names must be available and maintained for review.
- (iv.) Domain Naming shall include Department/Division acronym which shall be assigned by the AD Group, followed by State Root Domain placeholder (i.e. DOR.RI.GOV). Maximum values apply and should not exceed 15 characters. No special characters shall be used.
- (v.) Sites shall be named with a string containing a maximum of 255 characters and constructed as follows (working from the left); The city name, a hyphen, and the site street/location. The string shall not contain blanks or special characters and all words will be separated by hyphens. Site links will follow the Sites Naming Conventions and contain both site points within its name.
- (vi.) The User login name/User Principal Name (UPN) is formatted as first name, “.”, full last name @ State Root Domain name (i.e. john.doe@ri.gov). Duplicates should be handled by the following in sequence; add a dot “.” and middle initial, then append dot “.” and a sequence number if still not resolved (john.a.doe@ri.gov or john.a.doe.1@ri.gov). User accounts require the following attributes be filled in using the following formats; First Name, Last Name, and Initials. The display name is formatted as Last name, First name followed by middle initial for duplicate display names. If there are duplicates even with middle initial add agency or other identifier to eliminate duplicates. The following fields are required to be filled out for every user account. Display Name, Address City, State, Zip Code, Company to contain the DoIT maintained Agency codes, Department to contain agency division or work group as defined by each agency,

Office Phone number, and E- mail address. Other phone/pager/fax numbers must be populated if exists.

- (vii.) Service Accounts should begin with “svc-“agency code prefix (e.g., dot) followed by a hyphen and a name that describes the service it supports (e.g., Svc-dot-Meterman). The Description should contain the ID of the owner/requestor of the service account. The account options User cannot change password and Password never expires should be selected.
- (viii.) User E- mail Address Standard format should match the User Login Naming Convention followed by the Agency Identifier and @ ri.gov, for example john.doe@ri.gov.
- (ix.) Generic E-mail Addresses Standard format is as follows; Agency code, dot “.”, Department acronym, optional dot “.”, optional custom field (i.e. doh.hr.resumes@ri.gov). Mail enabled accounts may be created and then disabled to keep users from logging on the domain with the account.
- (x.) Agency Specific Group Naming Standard format is as follows; Department Identifier, dash, SubDepartment(s) if required, dash, Group Identifier, underscore “GROUP”. Example (DOT-MIS-TECH_GROUP)
- (xi.) Group Policy Object Naming Standard format is Department Identifier, dash, SubDepartment(s) if required, dash, Group Identifier, underscore “GPO”. Example (DOT-MIS-TECH_GPO)
- (xii.) Printer Naming Standard is Department Identifier, dash, SubDepartment(s) if required, dash, Group Identifier, underscore “PRT”. Example (DOT-MIS-LJ4_PRT)

n. Server Naming Conventions

- (i.) Naming Convention: DEPARTMENT-FUNCTION-IDENTIFER
 - “DEPARTMENT” = 3-4 characters, Use Department Abbreviation Above
 - “-“ = 1 character separator.
 - “FUNCTION” = 2-4 characters, description of the server, must follow pre-authorized standards.
 - “-“ = 1 character separator.
 - “IDENTIFER” = 2-6 characters, Department defined unique identifier for server.
 - NOTE: The entire name cannot exceed 15 characters (NETBIOS limit)
- (ii.) In cases where the server is multi-functional, the highest priority function takes the name, e.g., a combined domain controller and WINS server will be coded as DC.

Server Function Code	Function Identification	Example
Development	DV	ENT-DV-DB001
Testing	TST	ENT-TST-DB001
Training	TRN	ENT-TRN-DB001
User Acceptance	UAT	ENT-UAT-DB001
Immediate Release (Patch Management)	IR	ENT-IR-DB001

Production Systems		
Server Function Code	Function Identification	Example
Anti-Virus Server	AV	ENT-AV-001
Application Server	AP	ENT-AP-001
Database Server	DB	ENT-DB-001
DHCP Server	DHCP	ENT-DHCP-001
Domain Naming Service Server (DNS)	DNS	ENT-DNS-001
Domain Controller Server	DC	ENT-DC-001
VMWare ESX Virtual Host	ESX	ENT-ESX-001
File Server	FS	ENT-FS-001
Gateway Server	GW	ENT-GW-001
Mail/Messaging Server	MAIL	ENT-MAIL-001
Print Server	PS	ENT-PS-001
Proxy Server	PX	ENT-PX-001
Remote Access Server	RAS	ENT-RAS-001
Remote Installation Server	RIS	ENT-RIS-001
Remote Desktop Server	RD	ENT-RD-001
Terminal Server	TS	ENT-TS-001
Utility/Monitoring/Administration Server	UT	ENT-UT-001
Web Server	WEB	ENT-WEB-001
WINS Server	WINS	ENT-WINS-001
WSUS Server	WSUS	ENT-WSUS-001

- (iii.) For servers that are utilized by multiple department use ENT as the Department Identifier. In these cases, the identifier must contain an application identifier, example ENT-AP-RIFANS01.
- (iv.) For Development, Testing, Training, User Acceptance, and Immediate Release servers, the identifier must contain server function. Example ENT-DV-DB01 for an enterprise development database server.

o. Availability

- (i.) Any domain within the Active Directory structure must contain at least two domain controllers which reside in two physical locations.
- (ii.) Any domain controller must be backed up daily. Backup media must be retained for a minimum of 30 days. Backup media must be sent to an offsite location within 3 business days. Backup media must be protected by either software or hardware encryption. Tape access is limited to authorized personnel. An approved disaster recovery plan must be in place. The plan should include “mission critical” agencies at a minimum. The plan should include scenarios for; No equipment; No equipment and no people; No access to equipment. The plan must be tested at least once a year, without prior notice to the recovery team. The plan must include a specified offsite location that meets industry standards for disaster recovery. An overall summary report of AD status (including backup status) must be available to authorized personnel for viewing at any time. A full detailed report must be available upon request.

p. Auditability

- (i.) Logs must be maintained for a minimum of 6 months. Logs will be available to internal auditors. Exception reports from the logs will be reviewed daily and a report of summary of exceptions will be available to designated agency representatives. Logs must be replicated hourly to another location that is accessible only by executive-level security personnel. Logs should be renamed during the replication process to prevent overwriting in the replicated location. Log size should be set according to need, so that events within the last 60 days are easily accessible from the primary log file. The outsource vendor will provide a list of resources against current user access levels at least once a year and on demand by the agencies. The outsourced vendor will respond to log file inquiry requests within 2 business days, and provide weekly reports of failed login attempts to agency designee. The vendor will notify the affected agency immediately of repeated failed attempts. Events to be Logged includes Success and Failure Auditing for logins at the root forest level and/or where all user accounts are located, success and failure auditing for Object Access at the domain level, all user account changes (e.g., passwords), and schema modifications. There will be internal auditors. Agencies and auditors will have view of only privileges for OUs in the accounts domain.

5. Exceptions

- a. Requests for variance and exceptions to this standard must be submitted to the State CIO and approved.

6. Signatures

_____ Assistant Director of Planning, Policy & Technology	_____ Date
_____ Director of Operations	_____ Date
_____ Chief Information Officer	_____ Date
_____ Director, Department of Administration	_____ Date