



ITS Standard: Role-Based Access Control

Author: Dan Hamilton, Jared Kunkel, Matthew Kunkel, & Keela Ruppenthall

Date: 5/20/2016

Version: 1.0



1. Revision History

Version No.	Date	Description	Author
1.0	5/20/2016	Initial Release	Keela Ruppenthall

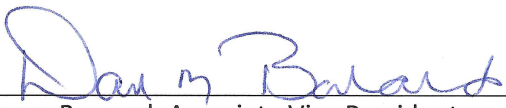
2. Approvals



 Mike Corwin, Associate Vice President 5/20/16
Date




 Tom Ambrosi, Senior Director and Chief Information Security Officer 5/20/2016
Date



 Dawn Barnard, Associate Vice President 5/20/16
Date



 Tony Opheim, Deputy CIO 5/20/16
Date



 Dr. Sasi Pillay, Chief Information Officer 6/1/16
Date



3. Table of Contents

- 1. Revision History ii
- 2. Approvals ii
- 3. Table of Contents iii
- 4. Introduction 1
- 5. Purpose 1
- 6. Scope 1
- 7. Related NIST Controls 1
- 8. Roles 2
 - Information Security & Privacy Committee 2
 - Sr. ITS Leadership 2
 - CISO / CIO 2
- 9. Standard 2
 - 9.1. Permissions Security Groups 3
 - 9.2. Role Security Group 4
 - 9.3. PowerShell Module 5
- 10. Review Cycle 6
- Appendix A: Glossary 7
 - Acronyms 7
 - Terms 7
- Appendix B: Review / Approval Comments 7**
- Appendix C: Naming Convention Examples 8**



4. Introduction

This standard describes the Washington State University (WSU) Information Technology Services (ITS) Role Based Access Control Model.

Role Based Access Control (RBAC) is essential for controlled access to resources at WSU as it enables governance, monitoring, and enforcement of segregated credential exposure, segregated credential use, and monitoring of appropriate tiered credential use.

This standard details an architecture designed to simplify access control and enable enhanced security administration for WSU users and resources.

5. Purpose

The primary purpose of this standard is to explain the details of WSU's RBAC Standard.

The secondary purpose of this standard is to provide a standardized naming convention to Directory Services Permission Groups and Roles.

6. Scope

This standard applies to all WSU owned or managed information systems which perform any of the following:

- Are physically connected to the WSU network
- Transmit and/or receive data over any portion of the WSU network infrastructure
- Process, store, or transmit WSU internal or WSU confidential data

This standard also applies to all WSU users that perform any of the following:

- Connect to the WSU network
- Transmit and/or receive data over any portion of the WSU network infrastructure
- Involved in processing, storing, or transmitting WSU internal or WSU confidential data

7. Related NIST Controls

WSU is required to comply with Federal and/or State laws and regulations related to information security, privacy and data confidentiality. This policy complies with regulations as defined by:

- FERPA
- HIPAA
- PCI DSS v3.1 – 7.1
- GLBA
- Washington State OCIO Policy 141 – Securing Information Technology Assets



This standard satisfies part or all of the following controls from NIST Special Publication 800-53 rev4:

- AC-2: Account Management
- AC-3: Access Enforcement
- AC-6: Least Privilege
- IA-4: Identifier Management

8. Roles

Security & Compliance Subcommittee

The Security & Compliance Subcommittee is responsible for commissioning the creation of an enterprise level access control standard for WSU systems and users. The Information Security & Privacy Committee reviews / modifies the draft WSU ITS RBAC Standard to ensure that the recommended strategy and architecture is sufficient to address the intended mitigations.

Sr. ITS Leadership

Sr. ITS Leadership reviews the draft WSU ITS RBAC Standard to determine the implementation feasibility of the recommended strategies and mitigations. Sr. ITS Leadership is also responsible for implementation support.

CISO / CIO

The CISO / CIO reviews and verifies that the WSU ITS RBAC Standard is consistent with applicable Federal and State laws, University policies, and that the recommended architecture provides sufficient mitigation of risk associated with system and user administration in the WSU Directory Services environment.

9. Standard

In the administration of technology at WSU, there are both organizational and functional roles that are created for various job functions and positions. The permissions to perform certain function are assigned to specific roles. WSU employees, students, and affiliates are assigned particular roles, and through those role assignments gain access to perform specific functions. Since people are not assigned permissions directly, but only acquire them through their role or roles, management of individual user rights is simply assigning appropriate roles to the user's account, and management of permissions is simply assigning permissions to roles. This model greatly simplifies common operations, such as onboarding a new employee, or changing someone's department, standing up a new service for operation, or auditing access to WSU resources.

WSU implements its RBAC model using Directory Services users, groups, computers and permissions. Users are assigned a role or roles by becoming a member of role groups. Role groups are assigned permissions by becoming members of permission groups. Permission



groups are assigned access to resources by application or service access controls that are defined for the permission groups.

9.1. Permissions Security Groups

In order to achieve granular levels of delegation, we use permission groups that are assigned permissions on a single resource. This method creates more groups but very fine grained auditing and permission assignment. These groups then add one or many role groups as members to give permissions to that resource. RBAC groups follow a strict naming convention with defined abbreviations to make deciphering the group's purpose easier. Examples are provided in Appendix B.

Name Field - The name field can be broken into the format below.

Permission group name format: <Organizational Abbreviation>_P_<Type of Access>_<Level of Access>_<Resource>

- Organizational Abbreviation - The abbreviation that central HR uses for your Unit. The character limit is 2 to 7 characters.
- P – Group Type Identifier (P=Permission Group)
- Type of Access - The type of permission being granted, but not the level of access being granted. This field is limited to 3 characters.

Examples:

- APP=Application
- FSH=File Share
- SYS=System Access
- ADP= Directory Services Permission
- SPP=SharePoint Permission
- FWP=Firewall Permission
- GPO=Group Policy Object
- SQL=SQL Permission OTH=Other
- Level of Access - The level of access being granted to the resource, but not the type of access being granted. This field is limited to 2 characters.

Examples:

- UR= User - Has user level rights to the system this is contextual based on the type of system and may merit explanation in the description field.
- AM=Admin - Full administrative access or full control of the resource
- LA=Limited - Admin Limited administrative access or control of the resource
- RE=Read - Read access, cannot modify or influence. This usually implies the list permissions if applicable to the resource.
- WR=Write - Write data to the resource. This implies a blind write and thus it cannot 'modify' existing content.



- RW=Read/Write - Read and write. If required, clarify exactly what actions can be taken. This permission sometimes implies create or delete access depending on the resource
- CR=Create - Create new objects
- DE=Delete - Remove objects
- CD=Create/Delete - Create and remove objects
- MO=Modify - Modify existing objects. This usually implies read
- JO=Join - This refers to the Directory Services permission to join machines to the domain. It is an important enough permission to merit an explicit permission suffix.
- LK=Link - This refers to the Directory Services permission to link GPOs to the location. It is an important enough permission to merit an explicit permission suffix.
- DO=DBO - Database owner
- Resource - The lowest or most specific object the object is given too. This could be a system name or a name used to refer to a collection of servers, file shares, SharePoint sites or many other things. The HomePage attribute described later will have the full path of the object where needed.
- Department - The department field should be the verbose name of the unit or organization the permission group is owned by. This helps with naming drift that easily affects acronyms.
- Location – The Tier designation and classification of the resource. This is agnostic of resource type, and should describe what kind of account can access this permission level on that resource.
- HomePage - The Homepage attribute is used to record the full path of the resource. This can be used for OUs, File shares, web addresses etc. where it's intuitive. Use the format of the resource in this field which will clearly denote the resource type.
- Description - The description field has a character limit of 1024 characters and is used to define both the resource and scope of the permission with detailed precision and notes. These notes should contain any binding requirements for the group not implied in other places, for example if a system refers to it by DN etc., it may have reasons the access is needed for auditing purposes.

9.2. Role Security Group

WSU employees, students, and affiliates are assigned particular roles as part of their organizational position or functional job duties. These groups are the organization or functional groups where user objects are added to provide authorization to resources. For Tier 1 RBAC model they exist both in ad.wsu.edu and mgthub.local. These groups are created and managed by ITS. They will follow the standard naming convention given below:

Role group name format: <Organizational Abbreviation>_R_<Functional Role>_<Level of Access>

Examples provided in Appendix B.



- Organizational Abbreviation - The abbreviation that central HR uses for your Unit. The character limit is 2 to 7 characters.
- R – Group Type Identifier (R = Role Group)
- Functional Role - The functional role filled by those in the role. An employee may fill many functional roles and may be approvable for multiple RBAC Roles. These will be split as needed to meet requirements for Tier separation and access separation. Abbreviations that are industry standard can be used such as DBA or SharePointAdmin.
- Level of Access - The level of access follows the Tier and data/server classification model and naming. Refer to the location field described in the RBAC Permission Security Group and examples. This level of access description with the location attribute of all permission groups it's a member ensure requirements for Tier and classification separation are met.
- Description – A description of the role and any limits intended for that role.
- Location - The Tier designation and classification of the resource. This is agnostic of resource type, and should describe what kind of account can access the permission level on that resource. This will be the same as the suffix of the object name. It is made available in both places for user and programmatic readability.
- Department - The department field should be the verbose name of the unit or organization the permission group is owned by. This helps with naming drift that easily affects acronyms.

9.3. PowerShell Module

Installation of the Directory Services PowerShell Module and is a prerequisite for successful implementation of this Standard.

The PowerShell Module is available for download via the Remote Server Administration Tools (RSAT) which is a Windows Server component that allows administrators to run snap-ins and tools on a remote computer to manage features, roles and role services. The software includes tools for Group Policy Management.

Once the PowerShell Module is installed a PowerShell session can be used to execute the following commented out script:

```
## Import-Module ActiveDirectory $DisplayName = "ITS_P_FSH_RW_ITSDATA-AdminServ"
$HomePage = "\\ITSDATA\AdminServ" $Name = "ITS_P_FSH_RW_ITSDATA-AdminServ"
$Location = "Tier1-HIGH" $Department = "Information Technology Services" $Path =
"OU=Permissison,OU=Groups,OU=Information Services,OU=WSU,DC=ad,DC=wsu,DC=edu"
$Description = "Group has Read Write access to the adminserv share on ITSDATA. This
storage is for sensitive data and reserved for tier1 credentials in a HIGH role."
```

```
New-ADGroup -DisplayName $DisplayName -GroupCategory Security -GroupScope 2 -
HomePage $HomePage -Name $Name -OtherAttributes @{Location=$Location;
Department=$Department} -Path $Path -Description $Description
```




10. Review Cycle

This policy will be reviewed by ITS at least once annually.



Appendix A: Glossary

Acronyms

Acronym	Definition
CISO / CIO	Chief Information Security Officer / Chief Information Officer
GPO	Group Policy Object
IT	Information Technology
ITS	Information Technology Services
NIST	National Institute of Standards and Technology
RBAC	Role Based Access Control
WSU	Washington State University

Terms

Term	Definition
Directory Services	A naming space database responsible for authentication and authorization of computers and users

Appendix B: Review / Approval Comments

Comment	Author of Comment



Appendix C: Naming Convention Examples

Permissions Security Groups:

Example 1:

Name: ITS_P_FSH_RW_ITSDATA-AdminServ Department: Information Technology Services
Location: Tier1-HIGH HomePage: \\ITSDATA\AdminServ Description: Group has Read and Write access to the AdminServ share on ITSDATA. This storage is for sensitive data and reserved for Tier1 credentials in a HI role.

Example 2:

Name: ITS_P_ADP_MO_SomeApp Department: Information Technology Services Location: Tier1-LOW HomePage: ad.wsu.edu/WSU Authorization Groups/Enterprise Groups/Provisioned Groups/SomeApp Description: This group can read and modify inside this AD location. This group is delegated rights to modify existing security group membership inside this OU. This group is referred to by DN in a linux application if any name changes or moves occur it must be updated (here give a system name)

Example 3:

Name: ITS_P_ADP_LA_Application-Groups Department: Information Technology Services
Location: Tier1-HIGH Homepage: ad.wsu.edu/Secured Accounts/Application Groups/
Description: This group has permission to read, write, create, delete for OU and group objects. Because of the breadth of this permission LA is used

Example 4:

Name: ITS_P_SPP_RE_IS-WSU-EDU Department: Information Technology Services Location: Tier2 HomePage: https://is.wsu.edu Description: This group has read access to is.wsu.edu and is given to tier 2 credentials.

Example 5:

Name: ITS_P_SYS_AM_2003AppServ Department: Information Technology Services Location: Tier1-LOW HomePage: Description: This permission is for Tier1 low credentials. It has windows administrative rights to these systems. (List of Server Names)



Role Security Groups:

Example 1:

Name: ITS_R_SharePointAdmin_Tier1-LOW Department: Information Technology Services
Location: Tier1-LOW Description: This role has permissions to SharePoint servers and farm administration. This farm does not contain or provide access high level assets, and therefore meets the low level of data classification specifications.

Example 2:

Name: ITS_R_DBA_Tier1-HIGH Department: Information Technology Services Location: Tier1-HIGH
Description: This role has access to Databases that meet the high level of data classification specifications.

Example 3:

Name: ITS_R_DBA_Tier1-LOW Department: Information Technology Services Location: Tier1-LOW
Description: This role has access to Databases that meet the low level of data classification specifications.

Example 4:

Name: DEPT_R_Admin_Tier1-LOW Department: University Department Location: Tier1-LOW
Description: This role has administrative access to systems that meet the low level of data classification specifications.