Role Design
Standard
Effective Date: April 23, 2015

Authority & Alignment

Authority: D1200 Code of Conduct; D3300 Internal Controls; D8010 Information Security and Identity Management

Alignment:
International standards – Cobit, ANSI INCITS 359-2004 for Information Technology – Role Based Access Control

Overview

This standard is designed to set out the requirements for the management of roles, responsibilities, access privileges and levels of authority and outlines activities that are designed to:

1. Manage the business roles, responsibilities and levels of authority and segregation of duties needed to support the business process objectives.
2. Authorize access to any information assets related to business information processes. This ensures that the business knows where the data are and who is handling data on its behalf.

MacEwan University (the "University") manages roles, responsibilities, access privileges and levels of authority through role based access controls (RBAC). The basic concept of RBAC is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by being members of roles.[1]

Scope and Definitions

This standard applies to all business processes and applications at the University. It also applies to administrative and privileged system access.

Permissions (Permission List): Permission is an approval to perform an operation on one or more RBAC protected objects.
Role: A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.
System Owner: Synonymous with Data Owner. A person who is responsible for the overall development, integration, modification, or operation and maintenance of the information system and is used in relationship to change control, system and data access, Service Level Agreements, and a sustainment and security partnership with the information technology service provider. More specifically, System Owners:

1. Establish and communicate service level requirements with IT.
2. Define the functions, procedures, reports and audit requirements of the system.
3. Ensure an adequate training plan is prepared and delivered to the system users.
4. Ensure the design, development and testing of the system leads to appropriate functional standards.

[1] ANSI INCITS 359-2004 for Information Technology – Role Based Access Control; p2;

5. Working with IT, authorize system changes. (outages, changes, emergency changes, etc.)
6. Working with IT, manage and authorize access to data.
7. Working with IT, maintain and review data security and integrity.
8. Define, approve and manage user access and permissions.
9. Participate in governance and planning activities to inform enterprise architecture.

Compliance & Exceptions

Responsibility for compliance with University policies and standards extends to all members of the University community as defined in D1200 Code of Conduct – Employees. Non-compliance may create risk for the University and will be addressed accordingly (see clause 4.5.1 "Respect for the law and university governance" of the university's policy D1200 Code of Conduct – Employees for additional guidance).

Standard Requirements

System Owners will[2]:

1. Allocate roles and responsibilities based on approved job descriptions and approved business process activities.
2. Allocate levels of authority for approval of transactions, limits and any other decisions relating to the business process, based on approved job roles.
3. Allocate access rights and privileges based on only what is required to perform job activities, based on pre-defined job roles.
4. Periodically review roles to ensure that the access is appropriate.
5. Allocate roles for sensitive activities so that there is a clear segregation of duties.
6. Provide regular awareness and training regarding roles and responsibilities so that everyone understands their responsibilities; the importance of controls; and the integrity, confidentiality and privacy of the University's information in all its forms.
7. Use the System Change Management process to review and approve new or modified roles or permission lists for implementation in production
8. Maintain design details of roles and permission lists in spreadsheets or other suitable form.

Related Content

Type	***Title***
Procedure	MacEwan PeopleSoft Security Design
Standard	Segregation of Duties Standard
Standard	Information Security Framework Standard

Measurement

- ✓ Risk assessments leading to operational reviews.
- ✓ Change Requests for new roles or permission lists.
- ✓ Documentation of modifications to existing roles and changes to the dynamic assignment of roles.

Contact

Director, IT Compliance and Information Security Office

[2] 1 through 6: COBIT 5 Enabling Processes © 2012 ISACA. All rights reserved.