**Account Authorization Guidelines**

**Authorization**

Authorization is a process by which a system determines if the client has permission to use a resource or access a file. It is usually coupled with authentication so that the server has the assurance of who the client is that is requesting access. The type of authentication required for authorization may vary; only passwords may be required in some cases, but passwords and 2-Step Login will be required for tasks that require a higher level of user assurance.

**Principle of Least Privilege**

Individuals should be granted the least access sufficient to complete their University responsibilities. Individuals that are granted privileged access accounts should use the least privileged account for day-to-day activities; privileged accounts should only be used when the elevated privilege is required by the system or application. For more information please see the [Privileged Access Standard](#).

**Updating User Access**

**Authorization Methods**

The University requires that the proposed solution meet the University identity access management [Account Authentication Standard](#). The following approved methods of authorization are listed in preference. If a service does not apply good authorization practices then it is possible that all users in our directory servers (200,000+) will have access to the application.

- Shibboleth Attributes
- Using Active Directory Groups
- Using 389 LDAP Groups
- Local to the Application (If local authorization is used in any capacity, it must be approved by The Information Security Office)

**Granting Access:**

- The Data Owner and Service Owner should agree on what criteria determines the membership of each user group. For a high-level overview of possible populations and their classification please see [EduPerson Codes (Albany)](#).
- If the application has different security roles, the Data Owner and Service Owner should agree on the access role a group receives.

**Removing Access:**

Appropriate procedures should be put into place to ensure the access is revoked when no longer needed.

- The access of users should be evaluated and updated regularly against the eligibility criteria for a security role.
- The Service Owner should determine if a retention period is needed and if so, what is it? E.G. Financial records may need to be maintained.
- Do accounts need to be purged from the system? E.G. Number of licenses consumed.

**Access Review**

User, privileged, and shared accounts should be periodically reviewed, at least annually.

**Glossary of Terms**

- **Access and Compliance Agreement** - A document required by ITS and Internal controls to ensure you understand your responsibility when accessing the University resources and data.
- **De-Provisioning** - The process of removing access from an individual when their status at the University changes and no longer makes them eligible.
- **Data Owners** - The person who is responsible for a certain type or classification of data at the University. E.G. The Registrar is responsible for student data.
- **Service Owner** - The department or person who is responsible for the application and maintaining security for data contained therewithin.
- **Security roles** - A grouping of access controls that is assigned to one or more individuals.
- **User security** - The ability to read or modify the information contained in an application E.G Update a student's grade within IAS.

For more information please see:

- [Identity and Access Management Best Practices](#)
• Account Authentication Standard