Identity Access and Management Policy

Information/Background:

Identity and Access Management is a comprehensive and unified approach to managing the identities of persons and processes issued by the University for the purpose of granting and controlling access to information resources. It is vital to have accurate and timely information regarding the roles and relationships of all constituents of the University at Albany in order to effectively manage access to information assets. It is equally important for data owners of employee and student information to understand their roles and responsibilities with regards to Identity and Access Management.

Rationale:

This policy aids the University at Albany in adhering to more stringent regulations, e.g., FERPA, to effectively manage access to licensed digital content and software, and to participate in federated online services that support collaborative research. It will also facilitate an understanding of the intrinsic role the University's offices and departments play in the establishment, continuation and discontinuation of access to campus and federated online services.

Policy Statement:

Identity and Access Management is based on the following principles:

- **Identity**: Every person who is a student, employee or affiliate of the University is assigned a unique online identity (PIN, Albany ID and NetID). A password is established by the individual for the purpose of authenticating to their assigned identity. PINS and passwords are confidential and must not be shared with anyone.
- **Role**: An individual’s role (e.g. student, faculty, staff, etc.) at the University governs their access to online services.
- **Status**: The establishment, continuation and discontinuation of access will be based on an individual’s status at the University (e.g. employed, terminated, registered, alumni, etc.).
- **Access**: Access to online services is granted based on the ‘least privilege’ principle (see ‘Access Control Security Domain’ in the Information Security Domains, Supporting Protocols, Standards, and Procedures as dictated by the University’s Information Security Policy).

This policy stipulates that the identities, roles and statuses of individuals at the University at Albany are verified and accurate prior to the issuance of their electronic identifiers (PIN, Albany ID and NetID). Information stored in the Integrated Administrative Services (IAS) system (Human Resources and Student Records) will be used as the System of Record for determining an individual’s identity, role and status. In turn, the role and status will be used for granting and removing an individual’s access to all online services.

Scope:

This policy applies to all constituents of the University at Albany who have been granted identifiers for the purpose of using University at Albany IT resources and federated online services.

Authorities for Identities, Roles and Statuses:

- **Students**: The Registrar’s Office is the steward of student records as they are recorded in IAS. As such, they are accountable for ensuring that the information regarding the student’s identity, role, and status at the University are accurate.

- **Employees**: The University at Albany has two offices with Human Resources responsibilities: the Office of Human Resources Management and Research Foundation Human Resources. These offices are the stewards of employee records as recorded in the University’s System of Record, IAS. As such, they are accountable for ensuring that the information regarding employee’s identities, roles, and statuses at the University are accurate. Other hiring offices (University Auxiliary Services, UAlbany Foundation, and the employing University departments) are accountable for the timely reporting of changes to roles or statuses of their employees to their respective Human Resource department.

- **Emeriti**: Individuals are identified as emeriti within IAS upon retiring from the University as a member of United University Professions or Management Confidential. They are individually accountable for reporting to Information Technology Services whether they want to retain their electronic identifiers and access to applicable University online services.

- **Externals**: Individuals who are not employed by the University or affiliated corporations (e.g. vendors, contractors, and media) will not receive personal electronic identifiers. They will be granted temporary access to online services based on a written request from the department with which they are most closely associated.

Privacy:

Electronic Identifiers are assigned to an individual who is then responsible for their use. To ensure privacy and security of electronic information, PINS and passwords are confidential and must not be shared with anyone.
Guidelines, Standards and Procedures:

The Office of the Chief Information Officer shall establish guidelines, standards and procedures as may be appropriate for the implementation of this policy.

Account Authentication Standard
Account Authorization Guidelines
Privileged Access Standard

Related Documents:

Federated Online Services
InCommon.org
University at Albany Information Security Policy
University at Albany Information Security Domains, Supporting Protocols and Procedures

Need more help? Contact the ITS Service Desk.