Application Access Provisioning - Overview and Requirements

Overview
The UAccess Access Provisioning Tool (APT) is used to request access to, as well as removals from, all UAccess Systems. Access may be requested for Employees, Students, or Designated Campus Colleagues (DCCs). This Quick Reference Guide will help you through the process.

Understanding the Access Request Process Workflow Roles
Several functional participants are involved in the provisioning process. Timely completion of each step in the process is critical to successful and timely provisioning. In some cases, prerequisites may be required to be completed involving additional groups.

Home
Access request and approval processes begin with the APT which also contains links to training and documentation info, Frequently Asked Questions, and APL delegation requests.

Access Provisioning Tool v3
- Submit Access Request (Add or Remove)
- Approve and Monitor Requests
- Training and Useful Links
- Frequently Asked Questions
- Manage Access Provisioning Liaison Authorizations
- Role Details
Requirements

- A valid NetID.
- Completion of the online Acceptable Use Policy agreement.
- Applicable training. Some roles require the completion of training before a role can be provisioned. It is best if training occurs prior to a request being created. This helps ensure the request is provisioned in a timely manner.
- Other prerequisites may be required depending on the requested roles.

Once the Subject User has completed all prerequisites, login to the request application.

Understanding the Relationship between Systems and Roles

1. **System** (e.g. UAccess Employee) will represent an independent Enterprise Application or may represent a logical grouping of functionality within an Enterprise Application system.

2. **Subject** (e.g. Time and Labor) is a logical grouping of related functionality within a System. A System may have multiple Subject Areas.

3. **Role** (e.g. Time Approver) represents a collection of components (menu items, pages, fields, functions and capabilities) necessary to allow desired functionality. A Subject area may have multiple Roles.

4. **Row Level Security** (e.g. Department IDs) defines a set of ‘data’ that is allowed to be viewed or processed against, by the Role’s functions and capabilities. The Row Level Security in the Access Request process is intended to represent an organizational unit, i.e., a college or department. A Role may require one or more Row Level Security.