Identity Management

Identity Management is the evaluation of how individuals enter and leave the various computing systems within Villanova University. The granting and removing of “digital privileges” can be thought of as a lifecycle. An understanding of this lifecycle and the supporting processes is required to insure that various “Digital Privileges” are granted or removed in an appropriate fashion as the individual moves through the various stages of the lifecycle. These digital privileges are a primary concern since they either grant access into designated systems or databases, or entail the provisioning of disk storage on various service systems like Email or Web services. A lack of understanding of this lifecycle can lead to security exposures or wasted resources as individuals move through or exit the system.

The first step in understanding the lifecycle is to identify the various stages or “roles” within it. In the case of an individual associated with Villanova, the identified stages were:

- Admissions Candidate
- Registered Student
- Affiliated Alumni
- Staff Employee
- Faculty Employee
- Special Cases

These “stages” or “roles” are differentiated by the amount of time spent occupying the role, or the level of service required to fulfill the role. For example, an Admission Candidate requires access to several Banner functions in order to check up on their admission status or financial aid information. This “candidate” role is limited in duration since there is a designated cycle point at which a candidate automatically becomes an admitted student. Once the individual becomes an admitted student, the Registrar becomes the steward of their Digital Entity. The duration of this role from a time perspective is not significant since other built in criteria such as inactivity automatically govern the exit conditions. The Alumni role, in contrast is essentially a perpetual role, and not constrained by as many rules as the student role. (Note: For our purposes, a steward is considered the department that defines the rules and conditions that govern a designated stage.)

Once the stages are established, a review of the entry and exit conditions for each stage is required. Special care must be paid to “digital entities” that maintain multiple roles. An example of this would be a staff member that decides to enroll as a student. Should the staff member terminate before the student role is completed, digital privileges must be updated to remove any staff related functionality without affecting the individual’s role as a registered student.

An example of these entry and exit conditions superimposed upon the predefined stages/roles is seen in the attached diagram entitled “Identity Management Lifecycle”. The gray box represents the various enterprise computing platforms that provide services to users, and host the Digital Entities. While a Digital Entity exists within the gray box, it is subject to the various rules and process flows defined by the various stewards. Within the gray box can be seen the identified stages along with their entry and exit conditions. An understanding of these conditions is necessary in order to provide automated services, and to insure
that there are no lurking security exposures or squandered resources in the backend systems and processes.

There are two primary repositories for storing an individual’s Digital Entity, the first is within the Banner system, and the second is within the LDAP directory environment. The location of these repositories is not as important as the fact that there are two separate repositories, each of which provides different digital privileges. Neither of these two repositories is “all inclusive” of Villanova’s digital population. There are instances where an individual should only exist in one or the other repository, for example a visiting scholar may not need access to Banner, but at the same time require a Villanova email address. Conversely, there maybe individuals that need to be in the Banner system, but do not require access to the resources provided through LDAP. The significance of these relationships becomes important when “automated processes” come into play and attempt to create, move, update, or remove Digital Entities within the system. A quick look at the “student lifecycle” will illustrate how these automated process come into play, and how they affect the digital privileges granted to an individual.