Identity Management:
Below is a description of the systems employed by National Louis University to handle the management of credentials for students, faculty, and staff. The identity creation process is anchored by our Banner ERP system, and is the central source of information for establishing identities for all NLU constituents. The same can be said for the disabling or removing of credentials for any specific constituent.

The NLU Identity and Access Management System includes:

- The management of a common digital identity and credential, the NLU ID, used for accessing campus services.
- A system that manages the provisioning and de-provisioning of access to technology resources.
- The web sign-on systems Shibboleth and CAS, to allow web application login using the NLU username and password.
- An Enterprise Directory Service, which provides a specialized database containing standard representations of information about people, groups, locations, services, and other resources. It includes:
    - Data integration with source systems such as Banner.
    - Authentication: the process of verifying whether or not a subject is who or what its identifier says it is. This is commonly done using a username and password.
    - Authorization: the process of determining an entity's eligibility to access an application or function or make use of a resource.

Furthermore policies to support the technology mentioned above, such as requiring password be changed every 90 days, and passwords meet strict complexity rules as shown below.

Network Security
While there is no possible way to guarantee that network resources will not be compromised, National Louis University proactively works to prevent cyber or network attacks.

- On a monthly basis we run a Network and Server Vulnerability scan which points to potential fail points that need to be addressed and patched.
- We have blocked direct access to INB (Internet Native Banner) outside of the university. In order to access INB from off of campus, users are required to access through 256bit encryption VPN (Virtual Private Network).
- In the interest of protecting date integrity we are continuing to create role based security for Banner
- SSL encryption is provided on every system which contains sensitive data PII
- Regular and systemic patching for servers and network
- Implementation of network tools to prevent intrusion
- Network Firewall
    - IPS (Intrusion Prevention System) which registers and blocks network traffic patterns that look suspicious
    - The Firewall also contains capabilities to manually block instantaneously IP's and URL's. This was used by during the recent network hacks from China on universities.
    - Content filtering vulnerabilities
- In addition to the technology, the staff is also trained to react proactively to network information. Within one hour of the Heartbeat Vulnerability being announced, NLU personnel were scanning our systems for the vulnerability and applied the patch as soon as it was available.