Responsible Use of University Computing Resources Policy Document

Secure Directory Services Access Policy for User Authentication and Authorization

1.0 Purpose

Montclair State University maintains two primary directory services for user login authentication and authorization: Sun Enterprise Directory (LDAP-compliant directory) and Microsoft ActiveDirectory. All faculty, staff, and currently-enrolled students have a unique "NetId" based on their lastname plus first initials (plus digit for student accounts) and an encrypted password.

2. Scope

Any in-house developed or third-party vendor applications, either hosted at the University or provided as a Software as a Service, that need to perform user login authentication/authorization against the University's LDAP and/or ActiveDirectory services must do so using industry-standard secure access protocols. In-house or third-party vendor applications, toolsets, or programming libraries may not record or archive MSU NetID passwords, either in encrypted or non-encrypted form, on any server or storage medium. Any web form that provides a login page for users to enter their NetID and password must be served over a secured HTTPS connection using an SSL certificate issued by an industry-recognized Certificate Authority.

University data security policies require that all data communications between applications and the directory service that pass authentication information (i.e. usernames/passwords) -must- occur over a secure connection. The preferred security mechanism is "LDAP over SSL" (LDAPS) but the application should also be capable of supporting StartTLS (LDAP ver. 3) as the University will be converting to that mechanism in the future.

3. Policy

All applications developed in-house or delivered by a third-party vendor will be audited by IT security personnel prior to production deployment to ensure that the above data communications policy guidlelines have been met. Periodic audits may occur after application deployment to ensure that compliance is maintained.