Authentication Standard

Syracuse University – Information Technology and Services
Information Security Standard – S0107

1.0 Scope

This standard applies to all university owned and operated IT systems and services, to any research or commercial system that offers services to the campus or the Internet. It is not required for privately owned devices or other systems intended for personal use but is recommended.

2.0 Purpose

The purpose of this standard is to define user authentication/access and administrative authentication/access to Syracuse University IT systems in scope.

•User Authentication/Access: access to the application or service by end users who have no special rights on the system or ability to change the underlying system configuration. This is what most users think of when they "log on" to a system or service.

•Administrative or Management Authentication/Access: access to an application, system, or service that allows full or extensive control, such that configuration changes can be made or that allows changes to the security configuration of databases, applications, services, or underlying operating systems.

Enacting this standard protects SU IT systems from being compromised.

3.0 Standard

3.1 User Authentication Standard:

For all IT services providing accessing to any non-public Syracuse University Data (as defined per Syracuse University IT security Standard), all users must authenticate by providing a set of credentials. Each user of an IT service must be represented by a unique identifier (user name) and associated proof of identity (e.g. Password). These credentials may be reusable (e.g., static password) or variable (e.g., one-time password) or a combination of both (static and variable) based on the level of the data accessed.

Also authentication processes must protect the credentials from interception in a form that could be reused to impersonate the user. Weak credentials, such as clear text passwords, must never be used over insecure network links without adding encryption.

All authentication successes and failures must be logged and include login times.

The system should rely on a centrally-provided and provisioned authentication source, rather than using local account databases. Central authentication services ensure more rigor

in assigning and removing accounts and credentials and make auditing for security problems more cost-effective.

The current complexity requirement for NetID passwords is:

- The password length must be between 8 and 16 characters.
- It cannot be a word or acronym found in a common English dictionary.
- It cannot contain your NetID.
- It must differ from last 3 passwords you have used.
- Password can be changed anytime and must be changed minimum once every year.
- The password must include
- at least one lowercase letter (abcdefghijklmnopqrstuvwxyz)
- at least one uppercase letter (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
- at least one number (1234567890)
- at least one non-alphanumeric character from this list:
- ` ! # $ & * ( ) - _ = \ | [ ] ' ; : / ? . ,

3.2 Administrative Authentication Standard

Administrative access to a server must follow the user access requirements listed above. In addition:

- Unnecessary administrative accounts must be removed or disabled.
- Default passwords must be changed.
- Syracuse University two factor authentication (DUO service) should be used to secure administrative access wherever possible.
- Administrative access/terminals must never be left open and unattended. Use of locking screen savers and other methods must be used, even when the server is in a secure room.
- Management interfaces must never be directly exposed to the Internet. Use of VPN or some other protective method must be used for off-campus access to these interfaces.
- Servers should only be accessed over the network from “known secure” devices. Loss of a single administrator password to a key logger can have devastating effects on a system.
- Passwords for administrative accounts must be 15 character or longer if technically possible and changed every year. They must minimally meet or exceed the complexity requirements used within the provisioned “NetID” accounts.
- Many administrative systems use shared passwords for specific functions. Such passwords must be changed whenever someone knowing the password leaves the associated administrative role or the password is compromised.
- Never use a NetID password for accessing administrative functions.

- Embedded clear text passwords should be avoided. When this is necessary, careful use of access controls must be applied to prevent widespread access to the password. Such passwords need to be changed in the same way as any administrative password: whenever someone who knows the password changes roles, the password must be changed.

4.0 Exceptions

4.1 Public or anonymous access to SU IT system

Public or anonymous access is acceptable only for data classified as public as defined in Syracuse University IT security Standard. Any system that provides anonymous or guest access must document the types of access provided, assess the risks posed, and ensure that a process is developed for regular review and removal of unneeded guest accounts.

4.2 De-centralized Accounts use and management

If and when a local account database is used, the system operator is responsible for requiring passwords at least as complex as the NetID standard, and for timely de-provisioning of unnecessary or obsolete accounts. "Timely" will reflect the local environment and processes that surround the system. Please use SSL 3.0 or TLS 1.0 or higher communication and ensure that the passwords stored locally are irreversibly hashed (SHA2 or higher). The password entry should always be masked as a default. For reference refer to ADTT guidelines for server configuration. This is subject to review by the ISO

5.0 Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Standard: Syracuse University Information Security Standard	http://its.syr.edu/security/standards/ITSecurity-standard.pdf
ADTT Server Defaults (site password protected)	https://itscis.syr.edu/Docs/Post/375/Active-Directory-Server-Defaults
Contact: Information Security Officer	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.04
Effective Date:	February 1st, 2016
Date of Last Review	January 25th, 2016
Date of Next Mandatory Review	January 25th, 2017