Data Access Standard
Syracuse University – Information Technology and Services
Information Security Standard – S0106

1.0 Scope

This standard applies to all faculty, staff, or contracted 3rd parties accessing data on any systems operated by Syracuse University, or accessing any of the University's data on systems operated by contracted 3rd parties.

2.0 Purpose

Syracuse University's data can be accessed from on and off campus using a number of different methods. These differing methods allow different levels of access from a variety of endpoints which each may present different levels of risk. The purpose of this standard is to provide guidance for different levels of convenient yet secure access to Syracuse University data using any approved method of access.

Risk is the primary factor in determining the requirements for the different levels of data access. Risk is the product of the ***probability*** of a particular ***threat*** causing some negative ***business impact.*** For the purpose of this standard, we consider these variables in the following way.

- **Threat**: Threats are made up of current attack trends, criminal activity and accidental misuse of systems. To simplify risk assessment, we consider the threat to be a constant.
- **Probability**: In this context, the probability of a threat impacting the university is most affected by the type of system being used to access data, and where that data is stored. In general, systems that are unmanaged and/or unsecure have a higher probability of exposing data than systems that are managed by IT staff and securely configured. In addition, a service that allows data to be locally stored on an endpoint raises the probability of exposure, especially if the endpoints are laptops or other mobile devices.
- **Business Impact**: Business impact is most affected by the type of data exposed. Since the University does not have a viable way to determine what type of data is accessed by any of the access methods used, we assume the data may be classified as *Confidential* as defined by *Syracuse University Information Security Standard.*

3.0 Standard

This standard defines the following three types of access; ***basic, elevated with a managed endpoint,*** and ***elevated with an unmanaged endpoint***. The standard further defines the requirements for each of the three types of access.

3.1 Basic Access

Basic Access is defined as any service that is available from on or off campus requiring nothing more than a NetID and password to gain access. If any additional requirements must be met to access the service (such as firewall rules, or additional permissions), it is NOT categorized as Basic Access. While these services are not risk free, they generally present a lower risk to the University.

While it is always preferred that a managed endpoint be used for all types of access, unmanaged and personally owned systems can be used for Basic Access as long as they have the following security configurations in place:

- Desktops and Laptops:
  - Have unique usernames and passwords configured for each user of the system.
  - Have patches and updates applied automatically.
  - Be running anti-malware software with updates being applied automatically (either as provided by the operating system or a 3rd party product).
- University owned laptops must also have full disk encryption enabled
- It is HIGHLY recommended that personally owned laptops have full disk encryption enabled.
- Mobile devices (smart phones/tablets)
  - Must require a PIN, password or biometric logon at the device level, (i.e. not just at the application level)

Examples of Basic Access include but are not limited:

- On campus Ethernet and wireless
- Standard VPN (SURA without elevated access)
- Terminal Server (TS.SYR.EDU)
- DatAnywhere web access (Does NOT include DatAnywhere with Sync enabled)
- Exchange
- MySlice portal
- Blackboard

3.2 Elevated Access with a managed endpoint.

Endpoints that are managed by ITS or by a school or unit's local IT staff may allow for access to additional services. *Managed* means that the configurations of the systems are known and maintained by IT staff. This is usually done by utilizing enterprise management tools (such as Active Directory or other tools), but IT staff may choose to manually manage the endpoint. Accessing these *elevated services* generally presents more risk to the university and therefore typically requires additional controls be in place such as firewall rules, a VPN connection or additional permissions within AD or the systems being accessed. In the case of elevated access

with a managed endpoint, the IT staff responsible for the management of the endpoint can enable and/or authorize the access with no additional requirements to the user, but the granting of that access must be able to be audited.

Examples of Elevated Access with a managed endpoint include but are not limited to:

- DatAnywhere without Sync option enabled.
- AD DirectAccess

3.3 Elevated Access with an unmanaged endpoint.

Systems that are NOT managed by ITS or by a school or unit's local IT staff are considered unmanaged endpoints. These are typically personally owned systems or systems that fall outside of the normal process or procedures of university owned endpoints. While these systems can be used for elevated access, they present a significantly higher risk to the university. As a result, users wishing to utilize these systems for elevated access must attend Information Security Awareness Training as documented at https://its.syr.edu/infosec/remoteaccess.html

Examples of Elevated Access with an unmanaged endpoint include but are not limited to:

- SURA VPN with elevated access (including Vendor VPN access).
- DatAnywhere with Sync option enabled.

4.0 Exceptions

Exceptions will be considered on case-by-case basis, and must be approved by the Information Security Officer. (see below)

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
ITS Information Security Secure Access Process	https://its.syr.edu/infosec/secureaccess.html
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.0
Effective Date:	April 1 2016
Date of Last Review	March 31 2016
Date of Next Mandatory Review	June 30 2017