Category 1 Security Controls Standards

Category 1 data is comprised of Personally Identifiable, Regulated, or University Declared data.

The following constitute the minimum security controls required for repositories containing Category 1 data.

Physical Controls

Physical controls apply to access to the physical resource where the data resides.

- Locked, caged racks
- Escorted physical access
- Logging of physical access
- Periodic review of physical access for the purpose of determining renewal or expiration.

Administrative Controls

Administrative Controls are intended to manage, monitor, and maintain privileged access to the data. Privileged access consists of the ability to:

- Modify application code that uses the Category 1 data
- Directly access database tables and fields external to the database management system application layer
- Authenticate or sudo to root or administrator on the system hosting or containing Category 1 data
  - Approval: requests for privileged access must be reviewed and approved by the Data Owner, or their designee.
  - Documentation: A master list of individuals with privileged access to the resource must be maintained. This should include the methods used to gain privileged access (e.g., Kerberos, SSH).
  - Review: Periodic review of who has privileged access must be conducted and changes made to reflect the current status of individuals with privileged access. The process includes reconciling master lists with actual access levels.

Technical Controls

Technical controls are applied directly to the data, itself.

- Systems must comply with the Standards for Connecting Servers to the University Network.
- Data must be encrypted at rest.
- Data must be encrypted in transit, both in physical transport and network communications.
- Multi-Factor Authentication, when available, must be used for privileged access accounts.
- Network filtering should be at the most restrictive level required to assure regulatory compliance.