

Policy Number/Title:	7.1.02 Information Security – Asset Management
Effective Since:	07/10/2020
Last Revision Approved:	04/29/2020
Responsible Office:	Computing and Information Technology

1. Scope:

This policy applied to all Winthrop University information systems users and assets.

2. Definitions:

Brute force attacks: A method of accessing an obstructed device through attempting multiple combinations of numeric/alphanumeric passwords.

Data: A subset of information in an electronic format that allows it to be received or transmitted.

Authorization: Authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Authorization occurs within the context of authentication. Once a user has been authenticated, they may be authorized for different types of access.

Data (Classification Types):

1. **Public:** Information intended or required for sharing publicly. Examples of public information include information provided on a University website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the University.

2. **Internal Use:** Information that is used in daily operations of Winthrop University. Examples of internal use information include the Winthrop University organizational chart, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in little risk to the University.

3. **Confidential:** Confidential information refers to sensitive information in custody of Winthrop University. Examples of confidential information include credit card information (PCI-DSS compliance standards), draft documents, and legal matters. Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk



to the University.

4. Restricted: Restricted information is highly sensitive information in custody or owned by Winthrop University and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, student records covered by the Family Educational Rights and Privacy Act (FERPA), Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of Restricted data shall result in considerable risk to the University including statutory penalties.

Data (Transmission Types):

1. Data at rest: All data in storage, regardless of the storage device, that is not in motion. This excludes information traversing a network or temporarily residing in non-volatile computer memory. Data at rest primarily resides in files on a file system. However, data at rest is not limited to file data. Databases, for example, are often backed by data files, and their contents can be thought of as rows and columns of data elements instead of as individual files. Agency should consider all aspects of storage when designing an encryption solution.

2. Data in transit: All data not in storage, regardless of the storage device, that is in motion. This includes traversing a network or temporarily residing in non-volatile computer memory. Data in transit includes, but is not limited to: files sent through electronic mail, files sent across or through mobile devices (e.g thumbdrives) and/or data sent through internet file transfer protocols (e.g SFTP, ACH).

3. Degaussing: Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.

4. Data owner: The person who has been identified as having the ownership of the information asset.

5. Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily this principle limits the damage that can result from an accident or error. -This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks only for the minimum amount of time necessary. The application of this principle limits the damage that can result from accident, error, or unauthorized use or activity.

6. Media sanitization: Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed. There are different types of sanitization for each type of media including: disposal, clearing, purging and destroying.



7. Obfuscation: Data masking or data obfuscation is the process of de-identifying (masking) specific data elements within data stores. The main reason for applying masking to a data field is to protect data that is classified as personal identifiable data, personal sensitive data or commercially sensitive data; however, the data must remain usable for the purposes of undertaking valid test cycles.

8. Role-Based Access Control (RBAC): A role-based access control (RBAC) policy bases access control decisions on the functions a user is allowed to perform within an organization. The users cannot pass access permissions on to other users at their discretion. A role is essentially a collection of permissions, and all users receive permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy. Within an organization, roles are relatively stable, while users and permissions are both numerous and may change rapidly.

9. System Development Life Cycle (SDLC): The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system, is called the System Development Life Cycle (SDLC).

10. Multifactor (MFA) or Two-factor authentication (2FA): Authentication systems identify three factors as the cornerstone of authentication: Something you know (for example, a password); something you have (for example, an ID badge or a cryptographic key); something you are. Multi-factor authentication refers to the use of two of these three factors listed above.

3. Policy:

Asset Identification

3.1 Information System Component Inventory

3.1.1 Winthrop University shall document and maintain inventories of the important assets associated with each information system. Asset inventories shall include a unique system name, a data owner, a data classification, and a description of the location of the asset.

Examples of assets associated with information systems are:

(a) Information assets: databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information;

(b) Software assets: application software, system software, development tools and



utilities;

(c) Physical assets: physical equipment (e.g., computers, servers, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, switches), magnetic media (e.g., tapes and disks); and

(d) Services: computing and communications services.

3.1.2 Access to Winthrop University assets shall be requested via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.

3.1.3 Winthrop University shall periodically revalidate the asset to ensure that it is classified appropriately and that the safeguards remain valid and operative.

3.2 Security Impact Analysis

3.2.1 Winthrop University shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.

3.2.2 Winthrop University shall ensure that each asset is classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.

4. Procedures:

This section was intentionally left blank.

5. Resources:

NIST SP 800-53 Revision 4: CM 4 Security Impact Analysis

NIST SP 800-53 Revision 4: CM8 Information System Component Inventory

6. History of Revisions:

04/29/2020 Policy first established

7. Approvals:



Responsible Officer Signature/Date:

Vice President/Senior Administrator Signature/Date:

President Signature/Date: