UF College of Pharmacy
UNIVERSITY of FLORIDA

Information Technology Department

Document Number:	IT-SEC-0008.001	**Document Name:** Data Security Standard	
Effective Date:	?	**Approval Date:** ?	
Document Type:	Standard	**Page Count:** 8	
Document Status:	?	**Document Category:**	IT – Security
Document Owner:	Lane Blanchard	**Document Version:**	1.4

1.0 Revision History

Version	Date	Author(s)	Change Description
0.0	7/15/2013	UF IT Security	Initial document adopted
1.0	10/17/2017	Lane Blanchard	First full document drafted from adopted document; Modifications for internal needs and requirements
1.1	12/15/2018	Lane Blanchard	NONE
1.2	11/05/2019	Lane Blanchard	NONE
1.3	01/15/2021	Lane Blanchard	Added link to UF Data Classification
1.4	04/04/2023	Lane Blanchard	NONE

2.0 Policy Approval

Name of Approver: Shaima Coffey

Title of Approver: ISA and Executive Director

Approval Date: ?

Information Technology Department

3.0 Purpose

Data of value (data that would be missed if lost) which cannot be easily recreated (as from an OS installation) must be backed up on a regular basis. An exception to this standard is provided if the cost of backing up exceeds the cost of restoration from a total loss. The University of Florida College of Pharmacy Information Security Manager (COP ISM) must ensure that a means of backing up and restoring vital data (including software) is provided and that access to data is restricted to authorized users and programs only.

Additionally, all data must be classified appropriately. Within a single system or application, each category of data may be treated differently. Factors which require consideration when classifying data include:

- Confidentiality: Preserving authorized restrictions on data access and disclosure including a means for protecting the privacy and proprietary data to uphold privacy and confidentiality laws.
- Integrity: Guarding against improper data creation, modification or destruction. Includes ensuring data non-repudiation and authenticity.
- Availability: Ensuring timely and reliable data access.

4.0 Details

4.1 Data Roles & Responsibilities

All data must have individuals assigned to roles of:

4.1.1 Data Owner

The UF College of Pharmacy Information Security Administrator (ISA) must ensure that Data Owner roles are assigned. The Data Owner for a data set is responsible for establishing policy related to the data set; creation, alteration, transmission and/or storage of assigned data that are used to carry out programs under their direction. The Data Owner must be established and documented for each client. The UF College of Pharmacy Information Security Manager (ISM) is responsible for ensuring that Data Owners receive specific instruction about their responsibilities.

Data Owner Responsibilities:

1. Apply the appropriate classification to the data according to this standard.
2. Determine the individuals to which the assigned data set should be available and accessible as well as permissions for data modification.

3. Ensure the appropriate security controls are in place commensurate with the classification designation to protect confidentiality, integrity, and availability.

4. Formally assign custodianship of the data resources, approve access to responsible custodians and ensure custodians are given appropriate authority to implement security controls and procedures.

5. Identify positions that require special trust. A position of special trust is one in which the incumbent can view confidential data, can alter sensitive data, or is depended upon for the continuity of data resources that are determined to be essential.

6. Maintain an accountability of who has access to their data and at least annually revalidating the access requirements.
7. Ensure appropriate review of data classifications are conducted at least annually to determine if the classifications are still appropriate and that the classifications are implemented in accordance with ***IT-SEC-0008 Data Classification*** LINK policy.

8. Ensure their data has an appropriate disaster recovery plan and is backed-up.

9. Ensure that, when necessary, data be irretrievably removed from physical storage media upon disposal or transfer in accordance with ***IT-GEN-0002 Asset Disposal***.

10. Ensure that Data Users are aware of their data protection responsibilities.

Examples of Data Owners: Directors, Operations Managers, Principal Investigators.

4.1.2 Data Custodian

Custodians provide technical facilities and support services to Data Owners and Data Users. Custodians implement security controls for data protection, and typically control physical access to data resources. When possible and reasonable, the roles of Data Owner and Data Custodian should not be held by the same individual. When the Data Owner is also a Data Custodian, they should not be the sole Custodian.

Custodian Responsibilities:

1. Assist Data Owners in data classification, disaster recovery planning, and cost effectiveness evaluation of security controls.

2. Implement the controls specified by the Data Owners at the server, operating system, network, PC, and application levels.

3. Confirm that the appropriate security controls are in place commensurate with the classification designation to protect confidentiality, integrity, and availability.

Examples of Custodians: Network managers, Server Managers, Webmasters, System Administrators, Managers of IT workers, and IT workers

4.1.3 Data Users

Users of data resources are individuals who create, access, or alter data.

Data User Responsibilities:

1. Know and comply with UF College of Pharmacy policies, standards and procedures.
2. Manage UF College of Pharmacy data and data resources responsibly.
3. Users must create, access, alter or delete data through specifically defined/provided interfaces.
4. Protect confidential and sensitive data in their entirety, regardless of the method of access.
5. Realize they are accountable for their actions relating to data resource security.

Examples of Users: Staff, students, vendors, visitors, contractors

4.2 Data Classifications

4.2.1 Open Data- Data, which if available to the public, will not harm an individual, group, or institution. Data in this classification must:

- Be labeled appropriately.
- Reside on an appropriately secured host.
- Have appropriate integrity protection.
- Have redundant systems to maintain availability as appropriate.
- Be retained according to public record requirements.
- Have an appropriate recovery plan.

Examples of Open Data: Seminar schedules, press releases, job announcements, advertisements

4.2.2 Sensitive Data

Data, which if available to unauthorized users, may harm an individual, a group of individuals, or the institution, but is not Restricted Data as defined below. Data in this classification must meet all the requirements for Unrestricted Data and must:

- Have a clearly defined purpose.
- Be easily identified.
- Have appropriate classification documentation.
- Have individuals assigned for Data Owner and Data Custodian roles.
- Have a clearly defined and documented user access list.
- Have appropriate documentation available to users that explains their obligations to protect the data.
- Be available only to those who are authorized.
- Be stored and transmitted securely to prevent unauthorized access.
- Be rendered unreadable prior to disposal.
- Have other protection as required by law, University of Florida policy, standards, and procedures, College of Pharmacy policy, standards, and procedures.

Examples of Sensitive Data: Staff salaries, infrastructure diagrams such as building and network, strategy documents, financial information, purchasing information, policies, standards, and procedures, business recovery plans, system configurations, emergency response plans, emergency equipment inventories

4.2.3 Restricted Data

Data with the highest level of protection includes, but is not limited to, data restricted by law, data restricted by legal contracts, security-related data such as passwords and risk assessments, and intellectual property. Data in this classification must meet all the requirements of Sensitive Data and must:

- Require authorization and authentication to view, change or delete.

Examples of Restricted Data: Social security numbers, passwords, credit card numbers, bank account numbers, security plans and assessments, protected health information, and other personally identifiable information.

4.3 Data Classification Guidelines

The standard for Data Classification includes the following:

4.3.1 Data description:

- What is the function or purpose of the data?
- How is it identified?
- Is it mission critical data?
- Is it system/application or user data?

4.3.2 Roles and to whom they are assigned:

- Who is the Data Owner?
- Who are the Data Custodians?
- Who are the Users?

4.3.3 Restrictions for data retrieval:

- Does access to the data need to be restricted? If so, to/from whom?
- Is the data protected by law, such as FERPA, GLBA and HIPAA?
- Is it exempt from public records law? Security-related data must be restricted. This includes but is not limited to passwords, vulnerability assessments, and physical facility diagrams.
- Is there potential harm from unauthorized access to the data?
- Is there any reason this data should be publicly accessible?
- Who is authorized to create, view or modify this data?

4.3.4 Protection methods for access, storage, and/or transmission:

Note: Specific technical details of methods used to protect data should not be made available to the general public.

- Will the data be stored on an appropriately secured host?
- Will the data be secured by appropriate host system security access restrictions, such as file permissions, Access Control Lists or passwords?
- Will application-level security, such as .htaccess or the myUFL portal, be employed?
- How will unauthorized access to the data be prevented?
- How will integrity of the data be ensured?
- Will it be distributed in electronic format?
- Should it be encrypted for storage and/or transmission? (This would apply to such data as passwords and data transmitted over wireless networks.) Will the data be accessed via clear-text transmission protocols?
- Are the host system's security mechanisms adequate for the sensitivity of the data, or should additional methods, such as encryption, be employed?
- Is the security of the transmission path adequate for the sensitivity of the data, or should additional methods be employed? (For instance, end-to-end encryption such as VPN, SSH, SSL or TLS should be used routinely on wireless networks.)

4.3.5 Labeling requirements:

Note: Protection method(s) should never be included as part of the data or its label.

- Should the Data Owner be identified on the label?
- Should the entire classification be included on the label?
- Should the distribution restrictions be included on the label?
- Should the disposal restrictions be included on the label?
- Should the creator be identified on the label?
- Should relevant dates be included on the label?

4.3.6 Availability requirements including archiving and retention:

- What harm will be done if the data is not available? Do availability requirements change with time?
- What redundant systems are necessary to guarantee that the data will be available for its intended purpose? (Such as RAID, redundant network connection, UPS, etc.)
- How is data restored if something happens to it? (Such as operations procedures, back-ups, etc.)
- How quickly must data be restored if something happens to it?
- Is appropriate recovery documentation available?

4.3.7 Disposal methods:

- Does the data require special disposal methods? (Such as rendering it unreadable or shredding before disposal)
- Do persistent copies of the data (such as backups) need special attention?
- Are there legal considerations for records-retention?

4.4 Data Security Procedures

THE UF College of Pharmacy ISA must ensure specific data security procedures are written for their organization.

5.0 Scope

Data security involves resources and processes beyond the scope of the UF College of Pharmacy Security Standard. This standard attempts to address only the electronic and technological aspects of data security that involve UF College of Pharmacy IT workers, those that have authority over data stored on systems managed by IT workers, and users of such systems.

6.0 Related Policies

- ***IT-SEC-0008 Data Classification Policy*** LINK

7.0 Definitions

College of Pharmacy ISM As defined in the IT-SEC-0001 Information Security Charter, the College of Pharmacy ISM has the responsibility to advise the administration of security implementations consistent with UFIT policies, standards, and procedures.

8.0 Supporting Information

No additional supporting information was provided.