Information Security Data Classification Standard

Issue Date: 07/23/2014
Revision Date: 2018-APR-05
Expiration Date: N/A
Category: ITS Standard

1.0 – Overview

Yavapai College (YC) collects, produces, and utilizes different type of data to order to fulfill its mission and vision. Federal and state laws, as well as College policy, mandate privacy and protection of certain types of data. In order for the College to protect its constituents it must protect sensitive information. Classifying data aids in determining how informational assets need to be protected.

2.0 – Purpose

This standard is intended to assist YC employees to classify data for the purposes of determining its need for protection.

3.0 – Scope

This standard can be used to classify any data asset that is stored or transmitted by or to YC. This standard only applies to both electronic and physically stored data.

4.0 – Protection Classification

Data is classified for protection into four categories: Public, Internal, Sensitive, and Restricted.

4.1 - **Public Data**: Data that falls into this category can be used without restriction and is assumed to be in the public domain.

Sharing Restrictions:	None, assumed public
Disclosure Risk:	None
Required Training:	None
Protective Measures:	None
Color Code:	Green (marking of media for this classification is optional)
Encryption:	Not Required
Storage and Erasure:	Any storage is acceptable; no special erasure/re-use precautions
Examples:	Catalog/Directory data, published website content, press releases, public financial data, etc.

4.2 – **Internal Data**: Data which generally requires a network account or explicit permission to access. This data is used in the routine operations of the College. Confidentiality of 'Internal Data' is preferred, but may not be necessary. This is the default classification level for all data not otherwise classified. Note: this information may be subject to disclosure per a valid public records request (see Policy 5.28 – Retrieval, Disclosure and Retention of Records). Refer to the "Media Protection Procedure" document for additional information on storage of this data.

Sharing Restrictions:	Generally, no internal sharing restrictions. External sharing requires valid written request, review by CISO and/or assigned data custodian.
Disclosure Risk:	Minimal risk of liability or associated costs
Required Training:	Security Awareness Training (annual)
Protective Measures:	Physical/Logical Access Controls; Multi-Factor Authentication
Color Code:	Yellow
Encryption:	Preferred, but not required for storage or transmission
Storage and Erasure:	All network storage is acceptable; Re-use is permitted (see Media Protection Procedure for erasure details).
Examples:	Email, voicemail, office documents on network shares, files accessible via Intranet or remote access services.

4.3 – **Sensitive Data**: Data subject to regulatory, legal, contractual, or policy protections related to sharing or use, or data which requires notification to third-parties should confidentiality be breached. Additionally includes data which is of a security-sensitive nature. Refer to Policy 5.30 – Clean Desk and Clear Screen for additional details. This data requires special handling – refer to the "Media Protection Procedure" document for additional details.

Sharing Restrictions:	No sharing without prior written consent of the data owner or CISO
Disclosure Risk:	Could result in significant legal, financial, or regulatory exposure risk
Required Training:	Security Awareness Training (annual), Protecting Information (annual)
Protective Measures:	Physical/Logical Access Controls; Multi-Factor Authentication; Mandatory Encryption; Data Loss Prevention; Automated Data Inventory and Classification Tools; Data Custodian(s)
Color Code:	Orange
Encryption:	REQUIRED – at rest and in transit (external); Limited portable storage
Storage and Erasure:	Only specially designated network storage may be used – no local storage is permissible; Approved/designated FIPS 140-2 validated automatically encrypting removable media is the only permissible removable media authorized for storage of sensitive data (see Media Protection Procedure for sanitization/re-use details).
Examples:	Any FERPA, HIPAA, PCI, ARS, or GLBA-regulated data, including (but not limited to) government identification numbers (e.g. SSN, passport or driver's license number), credit card and banking information, tax information, health records, or any other personally identifiable information. EXCLUDES FERPA "Directory Data". Additionally includes emergency operations and incident response plans, relevant physical and logical design documentation (e.g. blueprints, network diagrams, etc.)

4.4 – **Restricted Data**: Data which is routinely limited to need-to-know scope and which is both critical to daily operations and for which loss of integrity, availability, or confidentiality could cause significant or irreparable harm to the institution. Refer to Policy 5.30 – Clean Desk and Clear Screen for additional details. This data requires special handling – refer to the "Media Protection Procedure" document for additional details.

Sharing Restrictions:	Sharing, even within the institution or functional area is disallowed by default. Explicit written permission from the data custodian (generally the CIO, CFO, or ELT) is required for any sharing.
Disclosure Risk:	Could cause severe or irreparable harm to the institution
Required Training:	Security Awareness Training (annual), Protecting Information (annual), Individual Training/Discussion (as appropriate)
Protective Measures:	Physical/Logical Access Controls; Multi-Factor Authentication; Mandatory Encryption; Data Loss Prevention; Automated Data Inventory and Classification Tools; Data Custodian(s), Privileged Accounts; Separation of Duties (as applicable)
Color Code:	Red
Encryption:	REQUIRED – at rest, in transit; RECOMMENDED – in use - if supported
Storage and Erasure:	Only specially designated network storage may be used – no local storage is permissible; Approved/designated FIPS 140-2 validated automatically encrypting removable media is the only permissible removable media authorized for storage of sensitive data. Removable media must be permanently destroyed upon end-of-life.
Examples:	Encryption keys, institutional banking/financial credentials, privileged account manager (PAM) data, enterprise backup systems, Active Directory database files, enterprise database files containing SPII.

5.0 – Protecting Data Assets by Category

5.1 – Public Data Protection: Generally this data has no specific protection requirements.

5.2 – Internal Data Protection: Technological best practices are employed to ensure internal data is only accessed by authorized individuals. YC protects access to this information by following access procedures, provisioning processes, role management, and prompt removal of access. Access to this data via public request must follow YC Policy 5.28.

5.3 – Sensitive Data Protection: This data is limited to a small subset of authorized users only. Authorized users, generally users of the enterprise resource planning (ERP) system, must comply with the following: Federal and state laws, institution policies, and any departmental or functional area policies. In addition, all users must accept a formal usage agreement on an annual basis. Finally, all users must formally request access which must be approved by their supervisor and by an access manager and/or data custodian. Sensitive Data must not be moved to alternative media/systems/mobile devices or utilized via unauthorized methods (see YC Policy 5.30 and Policy 5.32).

5.4 – Restricted Data Protection: This data is limited to authorized users only. Authorized users, generally select IT, Facilities, and Business Office staff, must comply with federal and state laws, institution policies, and any department or functional policies as well. Additionally, all users must accept a formal usage agreement annually, and are required to complete annual training related to information security topics.

6.0 – Complaints and Violations

Complaints or allegations of a violation of these standards will be processed though YC's Human Resources Policies for employees.

7.0 – Definitions

CISO – Chief Information Security Officer

Data Owner/Data Custodian – The named individual ultimately responsible for managing a given set of data.

FERPA – Family Educational Rights and Privacy Act – Among other things, addresses privacy and sharing of student data and educational records.

FIPS 140-2 – Federal Information Processing Standard detailing requirements for cryptographic technologies.

GLBA – Gramm-Leach-Bliley Act – Among other things, sets standards for handling of customer financial data.

HIPAA – Health Insurance Portability and Accountability Act – Among other things, sets standards for storage, transmission, and handling of health information.

PCI – Payment Card Industry – Refers to Data Security Standards (DSS) for payment transactions.

Personally Identifiable Information (PII) – Includes any information that could be used to personally identify any individual whose information is maintained by the institution. This information may be subject to controls under FERPA, HIPAA, GLBA, or other regulations or statutes.

Sensitive Personally Identifiable Information (SPII) – Includes any subset of PII that could be used to facilitate identity theft or which could result in substantial inconvenience or harm to an individual. Specifically, this includes (but may not be limited to) information including: Social Security Numbers (SSNs), financial information (including bank/credit/debit account details), government-issued identification (e.g. Passports, Driver's Licenses, etc.), medical records or other health data, and any stored biometric data.

8.0 – Revision History

Author	Date	Version	Reason
P. Burns	07/23/14	1.0	Initial Creation
PB/SH	07/24/14	1.1	Minor Changes
P. Burns	05/24/15	1.2	Minor Changes
P. Burns	05/28/17	1.3	Minor Changes
S. Hagan	06/10/2017	1.4	Minor Changes
S. Hagan	01/29/2018	1.5	Significant Updates to section 4 and 5.
S. Hagan	03/07/2018	1.6	Clarification of PII/SPII; Added “Definitions”
S. Hagan	04/05/2018	1.7	Clarified encryption requirements

9.0 – Inquiries

Direct inquiries about this procedure to:

Patrick Burns
Chief Information Officer – Yavapai College
E-mail: Patrick.burns@yc.edu
Voice: (928) 776-2055

Yavapai COLLEGE