Status **Pending** PolicyStat ID **16423477**

Origination	N/A
Last Approved	N/A
Effective	Upon Approval
Last Revised	N/A
Next Review	3 years after approval
Owner	Clint Ewell: VP-Finance & Administrative Services
Area	5.0 Administrative Services

Information Security Data Classification and Handling, 5.11

PURPOSE

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

This standard is intended to assist the College employees in classifying data for the purposes of determining its need for protection and associated practices to protect data while in transit or at rest.

POLICY APPLICATION

This policy applies to all of the College faculty, staff, and student employees.

OPERATIONAL POLICY

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

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

I. Public Data

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

A. Sharing Restrictions: None - Data owner or custodian should confirm data as public.

B. Disclosure Risk: None

C. Required Training: None

D. Protective Measures: None

Examples: Catalog/Directory data, published website content, press releases, public financial data, etc.

II. Internal Data

Data that generally requires the College 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" for additional information on the storage of this data.

A. Sharing Restrictions: Generally, there are no sharing restrictions. External sharing requires a valid documented request reviewed by the data owner and/or Office of the President.

B. Disclosure Risk: Low risk of liability or associated costs

C. Required Training: Security Awareness Training (annual)

D. Protective Measures: Physical/Logical Access Controls; Multi-Factor Authentication

Examples: Email, voicemail, office documents on network shares, files accessible via Intranet or secure YC remote access services so long as they do not contain regulated data

III. Sensitive Data

Data subject to regulatory, legal, contractual, or policy protections related to sharing or use, or data that requires notification to third parties should confidentiality be breached. Additionally includes data that is of a security-sensitive nature. This data requires special handling – refer to the "Media Protection Procedure" for additional details.

A. Sharing Restrictions: No sharing without the prior written consent of the data owner, relevant regulatory contact, or CISO

B. Disclosure Risk: Could result in significant legal, financial, or regulatory exposure risk

C. Required Training: Security Awareness Training (annual), Protecting Information (annual)

D. Protective Measures: Physical/Logical Access Controls; Multi-Factor Authentication; Mandatory Encryption; Data Loss Prevention; Automated Data Inventory and Classification Tools; Data Owner(s)/Custodian(s)

Examples: Any CUI, FERPA, HIPAA, PCI, 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.)

IV. Restricted Data

Data that 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. This data requires special handling – refer to the "Media Protection Procedure" document for additional details.

A. Sharing Restrictions: Sharing, even within the institution or functional area, is disallowed by default. Explicit written permission from the data owner (generally the Chief Information Officer (CIO), Chief Financial Officer (CFO), or the Executive Leadership Team (ELT)) is required for any sharing.

B. Disclosure Risk: Could cause severe harm to the institution

C. Required Training: Security Awareness Training (annual), Protecting Information (annual), Individual Training/Discussion (as appropriate)

D. Protective Measures: Physical/Logical Access Controls; Multi-Factor Authentication; Mandatory Encryption; Data Loss Prevention; Automated Data Inventory and Classification Tools; Data Owner(s)/Custodian(s), Privileged Accounts; Separation of Duties (as applicable)

Examples: Encryption keys, institutional banking/financial credentials, privileged account manager (PAM) data, enterprise backup systems, Active Directory database files, and enterprise database files containing SPII.

V. Data Asset Protection by Classification Level

A. Public Data Protection: Generally, this data has no specific protection requirements.

B. Internal Data Protection: Technological best practices are employed to ensure internal data is only accessed by authorized individuals. The College 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.

C. 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 (data custodian) and/or data owner. Sensitive

Data must not be moved to alternative media/systems/mobile devices or utilized via unauthorized methods.

D. 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 operational policies. Additionally, all users must accept a formal usage agreement annually, and are required to complete annual training related to information security topics.

E. Sensitive Data Labels: When available, sensitive data classification labels and/or watermarks should be utilized on both electronic and hard-copy documents. This applies to all data classification types.

VI. Clean Desk – Clear Screen

The College employees must protect college information (internal, sensitive, restricted) when leaving their work area. This helps ensure that information is protected from unauthorized use.

A. Users must "log off' or "lock" their computers when their workspace is unattended.

B. All internal, sensitive, or restricted data must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.

C. All internal, sensitive, or restricted data must be stored in lockable drawers or cabinets. File cabinets must be locked when not in use or when not attended.

D. Keys used to access internal, sensitive, or restricted data must not be left in an unattended work area.

E. Passwords must not be posted on or under a computer or in any other accessible location.

F. Copies of documents containing internal, sensitive, or restricted data must be immediately removed from printers or other devices.

VII. Non-Compliance

Complaints or allegations of a violation of these standards will be processed through the College Human Resources policies for employees. Contractors or others who violate these standards will be subject to any enforcement actions outlined within relevant contracts and written agreements.

DEFINITIONS

Definition: Chief Information Security Officer (CISO) Responsible for managing the institutional risk assessment efforts, including developing data collection methods, reporting and metrics on key risk areas, identification of corrective action, and coordination with Data Custodians, Data Owners, Risk Managers, and the CIO on risk mitigation and resolution.

Definition: Data Custodian The person responsible for administering the system of record or data

system to ensure the availability of the data and to assist in ensuring the integrity and confidentiality of the data. Typically, this is an Information Technology Services (ITS) employee.

Definition: Data Owner The person responsible for ensuring the accuracy, relevance, and utility of a given dataset. This role is also responsible for complying with records retention/destruction requirements and monitoring and maintaining access controls to the data. Typically, this is the department head or senior responsible person for a program area.

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

Definition: Gramm-Leach-Bliley Act (GLBA) Among other things, it sets standards for the handling of customer financial data.

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

Definition: Payment Card Industry (PCI) Among other things, sets standards for storage, transmission, and handling of health information.

Definition: 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.

Definition: Sensitive Personally Identifiable Information (SPII) Includes any subset of PII that could be used to facilitate identity theft, 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.

Definition: Controlled Unclassified Information (CUI) Includes government-created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies.

RELATED PROCEDURES

Media Protection Procedure, 5.11.01

RELATED POLICIES

Performance Expectations and Corrective Action: 2.21

Electronic Communications: 5.29

Retrieval, Disclosure, and Retention of Records: 5.28

RELATED INFORMATION

There is no related information.

POLICY HISTORY

Formerly 2.3.10: Use of College Communication Resources, Adopted 1/25/2000

Renamed 5.27: Technology Resource Standards, 6/20/2013

Revised 12/2/2014

Revised 8/20/2019

Revised to "Operational" Policy and revised owner 3/5/2021

Transferred to PolicyStat 12/1/2021

Approval Signatures

Step Description	Approver	Date
Approval	Patrick Burns	Pending
Approval	Clint Ewell: VP- Finance & Administrative Services	Pending