Status Pending PolicyStat ID 16423644

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

Media Protection Procedure, 5.11.01

PROCEDURE DESCRIPTION

Improperly secured media containing confidential information represents a risk to Yavapai College (the College) and its constituents, ranging from competitive disadvantage to loss of revenue to reputational harm to fiscal penalties. Due care must be exercised in creating, storing, and handling media – whether electronic or otherwise.

All employees, partners, contractors, guests, and others provided explicit or incidental access to data or media containing data (electronic or otherwise) at a "Sensitive" or more restrictive classification (refer to "Information Security Data Classification Policy and Handling 5.11" for details).

PROCEDURE RESPONSIBILITY

The Chief Information Officer (CIO) and Chief Information Security Officer (CISO) are responsible for continuous review, evaluation, and auditing of this procedure. All employees are responsible for implementation, support, and notification of suspected or actual violations, whether intentional or not.

PROCEDURE

I. Responsibility Statement

The responsibility of the owner, creator, or custodian of any given media (whether electronic or otherwise) is to identify the data classification standard that the media is subject to and to take appropriate precautions in the storage and management thereof. Should any question arise regarding who the media owner, creator, or custodian is, the College's designated Risk Manager will make a final determination. The Information Technology Services Department (ITS) will provide technical controls to assist data owners and custodians in properly securing their data in order to abide by this and other relevant procedures and policies.

II. Physical Media

It shall be the responsibility of each department or functional area which may have occasion to create or make use of physical media of a “Sensitive” or more restrictive classification to establish provisions for the secure access, storage, and destruction of said media. This shall include maintaining an inventory of such media and an access log (automatic or manual) for individuals accessing the media. Auditing of inventory should be conducted by the department not less than annually, and any media which cannot be located must be immediately reported to the College’s Risk Manager.

III. Electronic Media

By default, the College disallows the storage of “Sensitive” or more restrictive classification data on removable media. Any such data must be stored solely on an approved network share or in the College’s secure file storage system. Data stored on an approved network share or in the College’s secure file storage system is encrypted at rest and either encrypted in transit or subject to Access Control List (ACL) restrictions to mitigate the risk of misuse. Users requiring access to network shares or secure file storage may request access via the College’s Access Management System. All access is subject to periodic review and annual positive enrollment (confirmation of continued business need).

If a specific business need dictates, storage of “Sensitive” or more restrictive electronic data on a workstation or laptop is permissible only upon consent and acknowledgment of both the department head and CIO or CISO. Approval will be granted only if the workstation or laptop utilizes whole-disk encryption meeting or exceeding FIPS 140-2/3 Level 1 requirements.

A. Removable Media

At no time is any employee of the College authorized to copy “Sensitive” or move restrictive classification data to any removable media without the prior written consent of the CIO or CISO. Should any such consent be granted, storage of restricted data is only permitted on approved removable media devices that are specifically inventoried and authorized by the ITS department. These devices will make use of disk/device encryption. Violations of this procedure must be immediately reported to the CIO or CISO.

B. International Travel

Due to variations in international law related to encryption and limitations on rights at border control checkpoints, no “Sensitive” or more restrictive data is permitted to be stored on any device which transits across an international border, even if the device was otherwise approved for storage of “Sensitive” or more restrictive classification data. Should a business need exist to access such data while on international travel status, access will only be granted via approved remote access services and no data is permitted to be downloaded or stored on the local device.

C. Data Classification – Media Identification

Although recommended, no requirement exists for media (electronic or otherwise) to be marked with a specific classification unless that media is being copied to a removable device or otherwise departing a College-controlled environment. Departments and functional areas may institute a more restrictive policy for either electronic or physical media. Once copied to a removable device, the device must be clearly marked with the letter and/or color designator for the most restrictive classification of data contained on the removable device (refer to “Information Security Data Classification and Handling Policy”).

D. Device Sanitization

Device Sanitization for Re-Use, Disposal, or Destruction – All removable media and disk drives (regardless of the technology employed) will be subject to media sanitization meeting or exceeding NIST SP 800-88 r1 (or newer) requirements before they can be re-used or released from College control (e.g., sold, donated, or otherwise disposed of in a form intended to retain at least limited functionality).

IV. Non-Compliance

Users or devices which do not comply with this procedure will be disallowed access to “Sensitive” or more restrictive classification media. Users may be subject to formal disciplinary measures, up to and including termination of employment (employees), termination of any active contracts (partners/vendors), and in severe violations, referral to law enforcement for potential prosecution.

V. Media Protections by Type

A. Public Data

1. Color Code: Green (marking of media for this classification is generally not performed)

2. Encryption: Not Required

3. Storage and Erasure: Any storage is acceptable; no special erasure/re-use precautions

B. Internal Data

1. Color Code: Yellow (marking of media for this classification is optional)
2. Encryption: Preferred, but not required for storage or transmission
3. Storage and Erasure: All network storage is acceptable; Re-use is permitted

C. Sensitive Data

1. Color Code: Orange (marking required where feasible)
2. Encryption: REQUIRED – at rest and in transit (external); Limited portable storage
3. Storage and Erasure: Only specially designated network storage may be used – no local storage is permissible; Approved/designated FIPS 140-2/3 validated automatically encrypting removable media is the only permissible removable media authorized for storage of sensitive data

D. Restrictive Data

1. Color Code: Red
2. Encryption: REQUIRED – at rest, in transit
3. Storage and Erasure: Only specially designated network storage may be used – no local storage is permissible; Approved/designated FIPS 140-2/3 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.

DEFINITIONS

Definition: FIPS 140-2/3 Federal Information Processing Standard detailing requirements for cryptographic technologies

REFERENCES

NIST 800-53 r4 MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7

RELATED POLICIES

Information Security Data Classification and Handling: 5.11

Technology Resource Standards: 5.27

PROCEDURE HISTORY

New 4-11-2023

Approval Signatures

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