Cochise College
Administrative Policy

Category: Technology
Policy Number: 6068
Title: Backup and Retention

The purpose of this policy is to define the backup and retention requirements for College Application Servers and Data. This policy provides for the continuity, restoration and recovery of critical data and systems.

Procedure: 6068.1
Roles & Responsibilities

Technology Services (TS) Team: College community members who have responsibility for the fulfillment of assigned roles or functions related to backup and retention of college data and applications. TS responsibilities include:

- Following the policies and backup procedures established by the appropriate Information Security Team
- Complying with federal and state laws, regulations, and policies associated with the college data used
- Implementing safeguards prescribed by the Information Security Team for Data backup and retention

Information Security Team: The Information Security Team is responsible to ensure compliance with this policy as a component of the college's information security program.

Procedure: 6068.3
Backup and Retention Requirements

1. **On-Premise Servers**

   a. All on-premise servers shall be backed up to two separate network attached storage (NAS) units, in two different locations.

   b. ITS Department will take regularly scheduled backups of all files and data that are stored on college servers.

   c. Servers and Data shall be backed up to server room storage in accordance with their specified backup classification.

2. **Off-Premise Hosted Servers**

   a. Snapshot backups of all Virtual Machines (VMs) shall be undertaken on a regular basis.

b. Backups saved at service providers (e,g Microsoft Azure or Amazon Web Services storage facilities) shall be retained in accordance with their specified retention classification

3. Monitoring

a. The system administrators shall monitor the system backup processes to ensure that college applications servers and data are appropriately captured. Any issues resulting in servers not getting backed up must be communicated to the Chief Technology Officer (CTO) as soon as possible.

Procedure: 6068.4
Definitions

User: Responsible for maintaining the confidentiality, integrity, and availability of college data they manage and for following all college policies, procedures, and standards related to the data security classification and security level, including applicable state and federal laws, and contracts.

Family Education Rights and Privacy Act (FERPA): FERPA deals with student "education records," defined to mean (with a few exceptions) records containing information directly related to a student that are maintained by a school or its agent.

General Data Protection Regulation (GDPR): Enacted by the European Commission to strengthen and unify data protection and privacy for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU.

Gramm-Leach-Bliley Act for Disclosure of Nonpublic Personal Information (GLBA): Requires financial institutions safeguard nonpublic customer data, limit disclosures of such data, and notify customers of their information sharing practices and privacy policies.

Health Insurance Portability and Accountability Act (HIPAA): Deals with the protection of personally identifiable information relating to health care. HIPAA applies to "covered entities," which includes health care providers who transmit information in electronic form regarding certain standard transactions (generally related to billing). Many institutions of higher education contain units that are covered entities, and some institutions are covered entities in their entirety.

Payment Card Industry Data Security Standards (PCI-DSS): A set of comprehensive requirements for enhancing payment account data security**.**

Personally, identifiable information (PII): Any college information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form.