Cochise College
Administrative Policy

Category: Technology
Policy Number: 6070
Title: Disaster Recovery Plan

The purpose of this policy is to define the Disaster Recovery Plan requirements for Technology Systems in the district. This policy provides for the continuity, restoration and recovery of critical data and systems in the event of a disaster.

Procedure: 6070.1
Roles & Responsibilities

Office of Technology Services (OTS) Team: College community members who have responsible for the fulfillment of assigned roles or functions related to the Disaster Recovery Plan/Procedure of College Data and applications. Responsibilities include:

- Creation, Maintenance, Updating and Testing of the Disaster Recovery Plan/Procedure document.
- Communicating resource needs to CTO for upkeep of Disaster Recovery systems.

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.

Teams Designated in Disaster Recovery Plan Procedure: The Disaster Recovery Plan/Procedure contains working teams related to Disaster Recovery Procedures. Their membership, roles and responsibilities will be documented in the Disaster Recovery Plan Procedure document.

Procedure: 6070.2
Disaster Recovery Plan Requirements

1. The Office of Technology Services shall create, maintain, update and test the Districts Disaster Recovery Plan Procedure (6070) on an ongoing continuous basis.

2. The Disaster Recovery Plan Procedure must cover the technological infrastructure, systems and data needed to continue business and academic operations in the event of a Disaster situation.

3. The Disaster Recovery Plan Procedure document will be a procedural document with the pertinent information needed to reestablish business and academic technological services, needed for operations to resume, following a Disaster.

4. Due to the sensitive nature of the information contained in the Disaster Recovery Plan Procedure document, it may only be shared with the appropriate Office of Technology Services personnel, Disaster Recovery Teams, District's Executive Team, Appropriate

Data Owners and Custodians, and the Districts Governing Board and any other entity or persons as determined by the CTO.

Procedure: 6070.3
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): 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): PCI-DSS is a set of comprehensive requirements for enhancing payment account data security**.**

Personally, identifiable information (PII): Any Cochise 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.