Cochise College
Administrative Policy

Category: Technology
Policy Number: 6071
Title: Incident Response

The purpose of this policy is to define the Incident Response requirements for Technology Systems in the district. This policy provides for the establishment of a clear command and control center, to rapidly mitigate exposure, maximize cooperation, and to efficiently coordinate response activities.

Procedure: 6071.1
Roles and Responsibilities

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

Incident Response Team (IRT): is responsible for managing and investigating all real and potential computer and information security-related incidents.

Procedure: 6071.2
Incident Response Requirements

1. The IST shall create, update and review the Districts Incident Response and Security Incident Reporting and Response Procedures on an ongoing continuous basis.

2. The Incident Response and Security Incident Reporting and Response Procedures will include steps to Identify, Investigate, Contain, Remediate, Follow up and Report as appropriate when all detectable real and potential computer and information security-related incidents occur.

3. Due to the sensitive nature of the information contained in the Incident Response Plan and Security Incident Reporting and Response document, it may only be shared with the appropriate Office of Technology Services personnel, IRT, IST, 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: 6071.3
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 that 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): 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.