Cochise College
Administrative Policy

Category: Technology
Policy: 6060
Title: Third Party Management Policy

The purpose of this policy is to describe the information security requirements to be followed in the selection, management and monitoring of third party service providers at Cochise College. This policy also defines the information security requirements for contracts with third parties.

Procedure: 6060.1 Scope

All engagements involving third party access to college information processing facilities or assets with service providers, including vendors, consultants, and suppliers, shall be in accordance with this policy.

Procedure: 6060.2 Roles & Responsibilities

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

Management: Follows this policy for contracts with third parties. Appoints a point of contact for managing the relationship with the third party.

Technology Services Staff: Assists sponsors and owners of the business function to be outsourced with the due diligence required.

Procedure: 6060.3 Due Diligence

Sponsors of outsourced services and owners of business functions shall exercise appropriate due diligence in the selection of the service provider, including the following considerations:

- Types of data being accessed and methods of access
- Definitions of data ownership and disposition throughout service lifecycle
- Non-disclosure and acceptable use agreements covering college assets, including facilities, systems and data
- Service provider levels of security to be provided for protecting college assets
- Service provider physical and logical controls used to restrict and limit the access to college sensitive business information

- Legal requirements to be met, such as data protection compliance requirements or regulations
- Availability and levels of service to be maintained, including in the event of a disaster
- The right to audit and review of any recent audit reports
- Clear understanding of the service provider security and incident response policy and assurance that the provider shall communicate incidents promptly
- Required screening, training, experience and other obligations of service provider staff
- Conflict and defect resolution

Procedure: 6060.4
Contract Requirements

Arrangements involving third party access to college information processing facilities or assets shall be based on a formal contract. The contract will contain, or reference, all security requirements and the assigned responsibilities to ensure that there is no misunderstanding between the college and the third party.

The following terms shall be included in all third party contracts when deemed applicable to the service(s) being provided:

- A general policy on information security
- A description of each service to be made available
- The target level of service and unacceptable level of service
- Responsibilities with respect to legal and regulatory matters, including that the service provider will comply with US legislation, commerce and export control laws in securing the data, as well as relevant or mandated standards, including:
    - Family Education Rights And Privacy Act (FERPA)
    - Health Insurance Portability And Accountability Act (HIPAA)
    - Health Information Technology For Economic And Clinical Health Act (HITECH)
    - Higher Education Opportunity Act (HEOA)
    - General Data Protection Regulation (GDPR)
    - Gramm-Leach-Bliley Act For Disclosure Of Nonpublic Personal Information (GLBA)
    - Red Flag Rules (RFR)
    - Digital Millennium Copyright Act (DMCA)
    - Payment Card Industry Data Security Standards (PCI-DSS)

- Communications Assistance for Law Enforcement Act (CALEA)
- Americans with Disabilities Act (ADA)
- State Data Breach Notification Laws
- Other State Statutes Pertaining To Personal Information Protection

- Intellectual Property Rights (IPRs) and copyright assignment and protection of any collaborative work
- The right to monitor, and revoke, user activity
- The right to audit contractual responsibilities, or to have those audits carried out by a mutually agreed upon third party
- Service providers reporting requirements detailing controls affecting confidentiality, integrity and availability of college information, services and systems
- A requirement that all subcontractors be approved by the college and that the third party remain responsible for the acts of any approved subcontractors
- Any required physical protection controls and mechanisms to ensure that the controls are followed
- An acknowledgement that the service provider is responsible for the security company information including cardholder data the service provider processes, transmits or stores

Accounts used by vendors for remote maintenance (including remote access accounts) shall be enabled only during the time period needed where appropriate. Remote access shall be provided in accordance with Cochise College's *Remote Access Policy*.

For third parties with access to credit card data, a list of service providers shall be maintained and the PCI compliance status of each service provider should be verified at least annually.

Procedure: 6060.5
Compliance

This policy is a component of Cochise College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA, GDPR and other regulations.

Procedure: 6060.6
Exceptions

The Chief Technology Officer (CTO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made to the CTO.

Procedure: 6060.7
Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The college reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Procedure: 6060.8
Definitions

CIA Triad: Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Computer: Computers are defined as workstation, desktop or laptop system, typically intended for individual or personal use.

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Data Owner: College officials having direct operational-level responsibility for the management of one or more types of data.

User: Any Cochise College faculty, staff, student or partner who has been authorized to access any college electronic information resource.