ADM 413
Security Policy #13

Implementation of New Technology and Vender Management

Purpose of Policy

The purpose of the policy is to describe the safeguards applicable to protect institution PII shared with third party vendors. Contracts must be reviewed to establish proper verbiage is included to ensure the third party vendor has evaluated that all risks are identified, mitigated, monitored and documented to protect the college form a third party breach. Management will also continue to monitor these third party contracts by requesting an information security policy and incident response plan.

Implementation of New Technology

Management understands that the environment is not stagnant, and that new technology, systems, and infrastructure will be implemented. Management has established procedures to aid in the evaluation of these new implementations to ensure that all risks are identified, mitigated, and monitored and included in existing risk assessment documentation. Initial risk assessments and due diligence will be conducted to evaluate the impact of the new implementation on the environment. Mitigating controls will be designed and implemented after approval from the appropriate level of Management. Applicable departments, relevant members of the affected user base, and members of IT and IS staff will be included in risk assessment procedures.

Vendor Management and Service Provider Oversight

The organization outsources various applications, technology, and functions to technology service providers and utilizes services from these vendors. The o or store varying amounts of constituent data or have remote access capabilities to the Organization's data, network infrastructure, and systems. Therefore, proper due diligence should be performed when the vendors are initially contracted and periodically thereafter.

Classification

Vendors will be classified according to the following criteria. These criteria will dictate the level of due diligence required prior to contracting and on an ongoing basis thereafter. This classification will be reviewed at least annually for existing vendor relationships and adjusted as necessary. See **Vendor Relationship Management spreadsheet** for a listing of all vendor relationships and the current classifications.

- **Critical**: These vendors have the highest-level of risk to the organization. These vendors meet one or more of the following criteria and will undergo the highest level of review at least annually:
    - Has regular access to sensitive constituent or organization data.
    - Has regular direct and/or unattended access to the organization's network.
    - Provides a critical service to the organization that would be hard to replace and detrimental if the vendor went under.
    - Is responsible for hosting critical data and maintains the responsibility for securing and backing up this data.

- **Significant**: These vendors are extremely important to the organization; however, the vendors do not meet the criteria of a critical vendor. These vendors will undergo a detailed review every three years.

- **Non-Critical**: These vendors present the lowest level of risk to the organization. These include a limited number of individuals, other than vendors and employees, that have access to organization premises and systems. These individuals include outside consultants, accountants, examiners, auditors, janitorial staff, and maintenance workers. These vendors will undergo the lowest level of review. If the vendors have access or potential access to organization systems or constituent data, or locations where these may be stored, review will include obtaining confidentiality agreements and reviewing procedures for notifying the organization of a potential issue, breach, or compromise of constituent or organization information. The sample Confidentiality Agreement can be found in **Appendix C**.

New Vendors

Upon selecting a new vendor, a complete risk assessment will be performed utilizing the New Product/Vendor Evaluation form in **Appendix D**. Depending on the services provided by the vendor and the level of access that the vendor has to sensitive data or Organization systems and infrastructure, the following areas will be reviewed:

- Financial viability
- Operational information
- Confidentiality practices
- Information security controls and cybersecurity preparedness
- Vulnerability management
- Insurance, with emphasis on cybersecurity coverage
- Incident response and breach notification
- Business continuity and disaster preparedness
- Compliance reports
- Vendor management and subcontractor relationships

Existing Vendors

Applicable vendors will also be reviewed annually to ensure ongoing oversight. Each year, management will examine existing contracts and will request and review information from all key vendors that have access to confidential data and/or provide significant services. The Annual Vendor Review Checklist in **Vendor Relationship Management spreadsheet** will be utilized to evaluate each vendor.

Oversight

The *Vendor Management Committee* will be responsible for overseeing the vendor management process. Once all documentation has been requested, received, and analyzed, Management will make the decision to approve the new relationship or extend, modify, or discontinue the existing relationship. A summary of the documents reviewed and Management's decision of the future of the relationship with the vendor presented annually to the *Vendor Management Committee* for final review and approval. The most recent approved vendor list can be found in **Vendor Relationship Management spreadsheet.**