Prescott College	**Policy Number:** *1220* **Policy Category:** *Information Technology Policies* ***Vendor Management Policy*** **Policy Summary:** *This policy establishes the requirements for third-party service providers to ensure the safety and protection of Prescott College information.*	
	Approval Date: *09/11/23*	**Effective Date:** 09/11/23
Policy Owner: *Vice President, Finance & Administration*	**Scheduled for Review:** *Fall 2028*	

Policy Statement

The policy applies to all vendors and partners who have the ability to impact the confidentiality or integrity of Prescott College's technology, business processes or sensitive information.

Assessments

- Vendors granted access to Prescott College Information Resources must sign the Vendor Non-Disclosure Agreement/Business Associate Agreement.
- Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.
- High risk findings must be followed up to verify remediation.
- A vendor risk assessment must be performed on vendors with physical or logical access to confidential information, college networks or that are considered critical vendors for specific business functions.
- Risk assessments must be performed on all requested cloud providers before approval.
- Vendors with PCI DSS compliance requirements must have their status reviewed on an annual basis.

Management

- Vendor agreements and contracts must be reviewed by the Director of IT and the Vice President Finance and Administration prior to execution and/or renewal.
- Vendor agreements and contracts must specify:
    - The Prescott College information the vendor should have access to,
    - How Prescott College information is to be protected by the vendor,
    - How Prescott College information is to be transferred between Prescott College and the vendor,
    - Acceptable methods for the return, destruction or disposal of information in the vendor's possession at the end of the contract,
    - Minimum information security requirements,
    - Incident response requirements,

    - Right for Prescott College to audit vendor.
- If a vendor subcontracts part of the information and communication technology service provided to Prescott College, the vendor is required to ensure appropriate information security practices throughout the supply chain and to notify Prescott College.
- The vendor must only use Prescott College Information Resources for the purpose of the business agreement.
- Work outside of defined parameters in the contract must be approved in writing by the appropriate Prescott College point of contact.
- Vendor performance must be reviewed annually to measure compliance to implemented contracts. In the event of non-compliance with contracts, regular meetings will be conducted until performance requirements are met.
- Vendor's major IT work activities must be entered into or captured in a log and available to Prescott College IT management upon request. Logs must include, but are not limited to, events such as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Any other Prescott College information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
- Vendor personnel must report all security incidents directly to the appropriate Prescott College IT personnel within the timeframe defined in the contract.
- Prescott College IT will provide a technical point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.
- Vendors with logical access to information resources must provide non-repudiation authentication mechanisms.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Prescott College or destroyed within 72 hours.
- Upon termination of contract, vendors must be reminded of confidentiality and non-disclosure requirements.
- Upon termination of contract or at the request of Prescott College, the vendor must surrender all access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Prescott College IT management.

References

- ISO 27002: 7, 13, 15, 16
- NIST CSF: DE.CM
- Vendor Non-Disclosure Agreement/Business Associate Agreement

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Reason for Policy

Prescott College utilizes third-party products and services to support our goals and business functions. This Vendor Management Policy establishes the requirements for ensuring third-party service providers will preserve and protect Prescott College information.

Responsibilities	
For following policy:	Any college employee that interacts, sets up or manages any Prescott College vendors.
For enforcement of policy:	Director of Information Technology
For oversight of policy:	Vice President, Finance & Administration
For procedures implementing the policy:	Deputy, Chief Operating Officer
For notification:	Policy Librarian

Revision History