Third-Party / Vendor Risk Management Policy

1.0 Purpose

Precision Computer relies on various third-party vendors and service providers to support its operations and deliver services effectively to its clients. Engaging with third parties inherently introduces risks, including security vulnerabilities, data breaches, operational disruptions, and compliance failures, which could impact both Precision Computer and its clients. The purpose of this policy is to establish a consistent framework for identifying, assessing, managing, and monitoring the risks associated with engaging third-party vendors, ensuring these relationships do not introduce unacceptable risks to Precision Computer or its clients' data and services.

2.0 Scope

This policy applies to all third-party relationships where the vendor:
* Accesses, processes, stores, or transmits Precision Computer confidential information or client data.
* Provides critical software, hardware, or services essential for Precision Computer's service delivery to clients (e.g., RMM, PSA, cloud hosting, data centers, security tools).
* Has direct or indirect connectivity to Precision Computer's internal network or management platforms.
* Represents Precision Computer or interacts directly with clients on Precision Computer's behalf.

This policy applies to all personnel involved in selecting, contracting, managing, and terminating relationships with third-party vendors.

3.0 Policy Statements

3.1 Vendor Identification and Inventory

* A central inventory of all third-party vendors falling within the scope of this policy must be maintained by the designated department (e.g., Procurement, Vendor Management Office).
* The inventory should include vendor contact details, services provided, data accessed/processed, criticality level, contract status, and risk assessment information.

3.2 Vendor Risk Assessment and Due Diligence

* **Initial Due Diligence:** Before engaging a new vendor or significantly expanding the scope of an existing relationship, a formal risk assessment and due diligence process must be conducted.

The depth of the assessment will be proportionate to the criticality of the service provided and the sensitivity of data involved.
* **Assessment Criteria:** Due diligence must evaluate, at a minimum:
  * The vendor's information security policies, practices, and technical controls.
  * Data privacy policies and compliance with relevant regulations (GDPR, CCPA, HIPAA, etc.).
  * Business continuity and disaster recovery capabilities.
  * Incident response procedures and breach notification history/capability.
  * Relevant security certifications (e.g., SOC 2 Type II, ISO 27001) or independent audit reports.
  * Financial stability and reputation.
  * Subcontractor (fourth-party) risk management practices.
* **Risk Tiering:** Vendors should be categorized into risk tiers (e.g., High, Medium, Low) based on the assessment results to determine the required level of ongoing monitoring and contract scrutiny.
* **Approval:** Engagement with new vendors, particularly those in higher risk tiers, requires approval from designated authorities (e.g., Security Team, Compliance, Legal, Senior Management) based on the satisfactory completion of due diligence.

3.3 Contractual Requirements

* Contracts with vendors falling under this policy must include specific clauses addressing information security and data privacy obligations, including:
  * Confidentiality requirements for Precision Computer and client data.
  * Data protection measures (encryption, access controls).
  * Breach notification timelines and procedures.
  * Right to audit or assess vendor controls (or review independent audit reports).
  * Compliance with applicable laws and regulations.
  * Limitations on liability.
  * Data handling upon contract termination (return/destruction).
  * Requirements for managing their own subcontractors (fourth-party risk).
* Contracts must be reviewed by Precision Computer's Legal counsel and Information Security representatives before finalization, especially for high-risk vendors.

3.4 Ongoing Monitoring

* Vendors, particularly those in higher risk tiers or providing critical services, must be subject to ongoing monitoring and periodic reassessment.
* Monitoring activities may include:
  * Reviewing updated SOC reports, security certifications, or penetration test results annually.
  * Monitoring vendor performance against SLAs.
  * Reviewing vendor security questionnaires periodically.
  * Tracking vendor security incidents or public breaches.
  * Conducting periodic risk reassessments (e.g., annually for high-risk vendors).

3.5 Vendor Access Control

*   If a vendor requires access to Precision Computer or client systems/data, such access must be strictly controlled according to the principles of least privilege, using secure authentication methods (including MFA where applicable), and subject to logging and monitoring, as defined in the relevant Access Control policies.

3.6 Incident Response Coordination

*   Procedures must be in place to coordinate incident response activities with vendors in the event of a security breach or service disruption originating from or affecting the vendor.
*   Contractual obligations regarding vendor cooperation during incidents must be clear.

3.7 Vendor Offboarding

*   When a vendor relationship terminates, a formal offboarding process must be followed.
*   This process must include:
    *   Revocation of all vendor access to Precision Computer and client systems/data.
    *   Confirmation of secure data return or destruction by the vendor according to contractual terms.
    *   Final settlement of accounts.
    *   Updating the vendor inventory.

4.0 Roles and Responsibilities

*   **Vendor Relationship Owner (e.g., Department Head, Project Manager):** Responsible for initiating vendor engagement, managing the ongoing relationship, participating in risk assessments, and coordinating offboarding.
*   **Procurement Department:** Responsible for managing the vendor inventory, facilitating contracts, and supporting due diligence.
*   **Information Security Team:** Responsible for defining security requirements, conducting or reviewing security risk assessments, approving security controls, and reviewing security clauses in contracts.
*   **Legal Department:** Responsible for reviewing and approving contract terms and conditions.
*   **Compliance Department (if applicable):** Responsible for ensuring vendor compliance with relevant regulations.
*   **All Personnel:** Responsible for reporting any unapproved vendor usage or observed vendor security concerns.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through audits of the vendor inventory, review of due diligence documentation and risk assessments, examination of vendor contracts, review of ongoing monitoring activities, and assessment of vendor incident handling.
5.2 Exceptions: Exceptions to this policy require documented justification, risk assessment, and formal approval from designated senior management and the Information Security Team.
5.3 Enforcement: Failure to follow this policy may expose Precision Computer and its clients to significant risk. Non-compliance by personnel may result in disciplinary action, up to and including termination.

6.0 Related Policies

* Information Security Policy (Overall)
* Data Classification Policy
* Client Data Management Policy
* Access Control Policy / Client System Access Control Policy
* Procurement Policy
* Incident Response Policy / Data Breach Response Policy
* Business Continuity / Disaster Recovery Policy

7.0 Definitions

* **Third-Party Vendor:** An external entity providing goods or services to Precision Computer.
* **Due Diligence:** The process of investigation and analysis performed prior to entering into an agreement with a third party to assess potential risks.
* **Risk Assessment:** The process of identifying, analyzing, and evaluating risks associated with a third-party relationship.
* **SOC 2 (System and Organization Controls 2):** An auditing procedure ensuring service providers securely manage data to protect the interests of their organization and the privacy of its clients.
* **ISO 27001:** An international standard for information security management systems (ISMS).

Revision #2
Created 1 May 2025 19:48:23 by Travis Woolery
Updated 16 September 2025 22:10:09 by Travis Woolery