Third Party Risk Management Policy

Revision History

Revision Date	Summary of Changes	Version	Updated By	Changes marked
3/15/23	Added History and Revision sections, Consolidated 3rd Party Service and Cloud Computing Policy	1.0	mchatzopoulos	N
5/25/23	Updated to include additional language dealing with SBOM and due diligence requirements	2.0	mchatzopoulos	N
1/30/24	Annual review completed	2.0	dstapleton	N/A
2/5/2025	Annual review and updates throughout	2.1	Dstapleton	N
5/22/2025	Re-classified prior to posting to Trust Center	2.2	Dstapleton	N

Document Properties

Status	Check Sharepoint for Status
Document Owner	CISO
Classification	Internal
Approval	CTO
Distribution	All employees

ProcessUnity reviews all policies annually per the Policy Management Policy. Below is an excerpt from the Policy Management Policy regarding policy review, distribution, and acknowledgement.

Annual Review

All policies are reviewed annually by the executive management team for accuracy and required changes. All information security (IS) policies must be reviewed by the Vice President of Information Security, Chief Information Security Officer, or the Chief Technology Officer to identify and make any changes required to ensure that the policies remain consistent with business objectives and emerging threats and best practices. Following the annual review, the policies must be re-approved by the Vice President of Information Security, even if no changes are required.

Distribution and Acknowledgement

Applicable policies, along with any associated Standards, Guidelines, Processes, and Procedures, must be made available to all ProcessUnity Workers. ProcessUnity Workers will be informed of any policy changes. ProcessUnity Workers will be required to acknowledge, read, and agree to abide by each Policy as defined by the executive management team:

- Upon hire
- Upon policy change
- Annually

Table of Contents

1. Overview

This policy aims to ensure that all engagements, contracts and agreements between the ProcessUnity and third parties meet acceptable levels of information security and privacy risk and include information governance processes to ensure that data entrusted to ProcessUnity is protected and managed in line with statutory requirements and best practices.

2. Purpose

This policy and supporting procedures are designed to provide ProcessUnity with a documented and formalized Third Party Risk Management policy that is to be adhered to and always utilized throughout the organization. Compliance with the stated policy and supporting procedures helps ensure the safety and security of ProcessUnity system resources.

Today's increased use of outsourcing to various third parties has created a true need for monitoring such entities for baseline compliance measures with regards to ProcessUnity's minimally accepted standards for security. Specifically, all outsourced processes, procedures, and practices relevant to ProcessUnity's business are to be monitored on a regular basis, which includes undertaking various measures on all third parties providing critical services. The subsequent policies and procedures relating to Third-Party Risk management initiatives for ProcessUnity strive to ensure the overall confidentiality, integrity, and availability of the organization's network and information.

3. Scope

This policy and supporting procedures encompass all system resources that are owned, operated, maintained, and controlled by ProcessUnity and all other system resources, both internally and externally, that interact with these systems.

This includes but is not limited to all vendors, contractors, consultants, partners, suppliers, third parties purchased software, cloud providers, and SaaS applications. For this document they will all be referred to as a "Third-Party".

4. Policy

It is the policy of ProcessUnity to effectively manage the lifecycle of all Third-Party relationships to responsibly steward resources and minimize the inherent risk associated with engaging third parties to perform services.

4.1. Third-Party Risk Management Program

It is the responsibility of the CISO to ensure the design, development, implementation, and monitoring of an enterprise program to manage the risk associated with third-parties. This program will have the following characteristics, at minimum:

- Ability to maintain an accurate inventory of third-parties under evaluation for use, approved for use, and no longer in use.

- Centralize the request, evaluation, approval, ongoing assessment, and offboarding activities related to third-parties.
- Communicate and train all applicable employees regarding their roles and responsibilities as they relate to third-party risk management.
- Identify, validate, measure, and treat risk associated with third-parties in a way that is consistent with ProcessUnity policy, applicable regulations, and contractual obligations.

4.2. Initial Risk Assessment and Vendor Selection

The selection process for new vendors is to consist of exhaustive measures for ensuring all relevant risk areas have been thoroughly assessed by ProcessUnity, which can include, but not limited to, the following measures:

- Review of all applicable financial documentation, such as financial statements, etc
- Identification and inclusion of all regulatory requirements and standards that are applicable due to the nature of the third party service, types and sensitivity of data being shared, and any other relevant inherent risk factors. For example, understanding data ownership, storage, and transfer implications due to a regulation such as the GDPR.
- Experience and overall business expertise, aptitude, strength, and knowledge of senior management and all other relevant personnel
- Reputation within the industry and from the general public
- Alignment of vision, strategies, and overall goals with each organization
- Operational capacity and scalability
- Use of, and potential risks associated with, other third-parties by the vendors themselves (i.e., sub servicers, sub-processors, fourth-parties, etc.)
- Inquiry into any past, present or expected legal issues, constraints, or concerns
- Underwriting criteria
- Insurance coverage
- Training or documentation on how to best use the product or service in order to maintain an acceptable level of security
- Assessment of operational, business specific, and information security and privacy policies, procedures, and practices, particularly documentation pertaining to incident response, security awareness, business continuity and disaster recovery planning (BCDRP)

- Evaluating the necessity of implementing measures to guarantee ProcessUnity's continued access to its own data and any customer data stored by the vendor, in case the vendor becomes insolvent or ceases operations.
- Identification of the necessary, applicable security and privacy controls for the vendor, taking into account any shared responsibilities between the vendor, ProcessUnity, and ProcessUnity customers
- Assessment of the implementation and effectiveness organizational-wide system of internal security and privacy controls
- Architectural review to include, when applicable, logical diagrams depicting the application or service, infrastructure, code base (SBOMs are acceptable), and data flows

These measures are subject to change based on the criticality of the vendor to ProcessUnity and its subsequent services.

4.3. Contractual Requirements

Once vendors have been selected for providing services to ProcessUnity, comprehensive procedures are to be undertaken regarding all contractual documentation. These steps and related documentation may include the following, depending on the characteristics of the third party services being procured:

- A formalized and written contract has been produced, one that dutifully identifies roles, responsibilities, obligations, and expectations from all relevant parties.
- The contract has been approved by senior management throughout ProcessUnity, which includes all major stakeholders, such as board of directors, audit committee personnel, equity owners, officers, - as applicable – and all other relevant personnel. This also requires addressing the following issues regarding stakeholders:
    - Are they aware of the risks when entering contractual agreements with such vendors?
    - Are there any financial relationships or associations with such vendors?
    - Were all due diligence findings and documentation presented clearly and in a timely manner to such individuals?
- Comprehensive and appropriate review has been undertaken by legal counsel, with all issues, constraints, and concerns addressed as necessary.
- Defined operational, performance, and other necessary baseline standards for services to be performed have been contractually defined.
- Service Level Agreements (SLA's) have been defined within the Contracts.
- Security requirements for the Third-Party are clearly stated to ensure that their work is consistent with ProcessUnity policies and external requirements.

  - These requirements should be inclusive of any that pass through ProcessUnity from our customers, and should propagate to the vendor's third-parties if they sub-contract any relevant portion of the service

- Fees paid for stated services along with other financial considerations have been defined.
- Regulatory compliance audits and mandates, such as annual financial statement audits, annual operational and security assessments (i.e., SOC 1 SSAE 16, SOC 2 | SOC 3 AT 101, PCI DSS, etc., ISO 27001) have been successfully completed, are maintained, and evidence can be shared with ProcessUnity.
- Data Processing Agreements (DPA) or Standard Contractual Clauses (SCC) have been included, if applicable.
- Non-Disclosure Agreements (NDA) have been put in place before giving access to ProcessUnity systems and data.
- Contracts that include exchange or storage of Confidential data have confidentiality agreements to be executed by the vendor, identify applicable ProcessUnity policies and procedures to which the vendor is subjected, and identify security incident reporting requirements.
- Information security protection measures are included, regarding the safety and security of sensitive and confidential information, such as Personally Identifiable Information (PII), and any other variant thereof.
- Numerous other legal issues are addressed, including, but not limited to, the following: resolution measures, indemnification, continuation of services, default, intellectual property.

These measures are subject to change based on the criticality of the vendor to ProcessUnity and its subsequent services.

4.3.1. Third-Party Reporting Requirements

- In the event of a breach of the security of the sensitive data, the vendor is responsible for immediately notifying and working with the ProcessUnity Incident Response Team (PIRT) regarding the investigation, notification, recovery, and remediation.
- Security reporting requirements in the contract must also require the vendor to report all suspected loss or compromise of sensitive data exchanged pursuant to the contract within 48 hours of the suspected loss or compromise.
- The vendor, in partnership with ProcessUnity, is responsible for notifying all persons whose sensitive data may have been compromised because of the breach as required by law.
- When necessary, based on the criticality of the vendor, contracts shall require the vendor to produce reports focusing on four primary potential risk areas if requested:
  - Unauthorized Systems Access

  - Compromised Data
  - Loss of Data Integrity
  - Inability to Transmit or Process Data
  - Exception Reporting

- Any exceptions from normal activity are to be noted in the reports, reviewed, and the appropriate responses determined.

4.4. Subsequent Risk Assessments and Reviews

- Security reviews for Vendors will cover each individual use case or service provided by the third-party and are required upon a new solution acquisition, material changes in scope or use cases for current solutions, and material changes in system design or controls, business transfer, merger, or acquisition.
- Periodic review of a vendor's security posture and continued compliance will be conducted as needed, based upon changes in system use, design or controls, contract renewal or business transfer, merger, or acquisition.
- Third parties must perform or undergo periodic security reviews throughout the lifecycle of the relationship in order to ensure compliance with security requirements.
- Periodic review of the adherence to any SLA's of the Third Party should be conducted regularly, in most cases at least annually.
- Knowledge of alternate suppliers or vendors should there be a need to migrate if the Third-Party does not meet their requirements or our needs should be maintained.
- Upon contract termination, ProcessUnity must work with the third party to have its data returned or destroyed.

4.5. Direct Third-Party Access

Any Third Party that may have direct access to ProcessUnity information or assets must comply with the following requirements. For clarity, direct access is defined as access to primary data stores in ProcessUnity's production application.

- Each service provider must provide ProcessUnity with a list of all staff working to provide services to ProcessUnity. The list must be updated and provided to ProcessUnity within 24 hours of staff changes.
- Each service provider staff member with access to Confidential Information must be cleared to handle that information. Third-party access to Confidential Information shall be activated only when needed. Access shall be deactivated after services have been provided. IDs used by vendors to access, support, or maintain system components via remote access shall only be enabled during the time period needed and disabled when not in use. Third-party service provider access to Information Systems shall be monitored during use.
- Service providers with remote access to customer premises (e.g. for support of remote devices or servers) must use a unique authentication credential with multifactor authentication.

- Service provider personnel must report all security incidents directly to the appropriate ProcessUnity personnel. If service provider management is involved in ProcessUnity security incident management the responsibilities and details must be specified in the agreement.
- Service provider must follow all applicable ProcessUnity change control processes and procedures.
- When applicable, regular work hours and duties will be defined in the agreement. Work outside of defined parameters must be approved in writing by appropriate ProcessUnity management.
- All service provider maintenance equipment on the ProcessUnity network that connects to the outside world via the network, telephone line, or leased line, and all ProcessUnity IT service provider accounts will remain disabled except when in use for authorized maintenance.
- Service provider access must be uniquely identifiable and password management must comply with the ProcessUnity Password Policy. Service provider's major work activities must be entered into the Third-party Service Provider Log Form and made available to ProcessUnity management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Upon departure of a service provider from the agreement for any reason, the service provider will ensure that all Sensitive Information is collected and returned to ProcessUnity or destroyed within 24 hours. Upon termination of service provider or at the request of ProcessUnity, the service provider will return or destroy all ProcessUnity information and provide written certification of that return or destruction within 24 hours.

4.6. Exceptions

Exceptions to this policy should be submitted to the VP of Information Security for review and approval. If an exception is requested a compensating control or safeguard should be documented and approved.

5. Procedures

Please see the ProcessUnity Third Party Risk Management Procedures.

6. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.