Information Security Policy

Revision History

Revision Date	Summary of Changes	Version	Updated By	Changes marked
3/9/23	Added History and Property sections, renamed to Endpoint Protection, removed redundant info found in AUP	1.0	mchatzopoulos	N
2/12/24	Annual review & updated guidance on minor/major policy updates	1.1	dstapleton	N
7/25/24	Updates to policy and procedures content and approval process	1.2	Dstapleton	N
2/4/2025	Annual review and minor edits	1.3	Dstapleton	N
5/21/25	Updated oper resp section	1.4	Dstapleton	N
5/22/25	Re-classified prior to posting to Trust Center	1.5	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 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 Information Security Policy is the parent policy document for all other subordinate and related security policies in place at ProcessUnity, Inc. (ProcessUnity).

1.1. Purpose

ProcessUnity's Information security program is established to ensure the proper level of security throughout the environment. The Information security program is based on business requirements derived from:

- Assessing security risks to the organization.
- Defining the legal, statutory, regulatory, and contractual requirements that ProcessUnity, our business partners, contractors and service providers must satisfy.
- Defining the set of principles, objectives, and requirements for information processing that ProcessUnity has developed to support its operations.

Information security is continually improved by implementing a set of effective controls, which consist of policies, standards, processes, procedures, organizational structures, and hardware or software functions. These controls need to be established to identify and minimize risk and protect information assets that are required by ProcessUnity to meet the operational, financial, and regulatory requirements of its business. Information security is characterized as the preservation of Confidentiality, Integrity, and Availability.

Confidentiality – Prevents unauthorized disclosure of sensitive information.

Integrity – Prevents unauthorized modification of systems and information.

Availability – Prevents disruption of service and productivity.

1.2. Audience

The information security policies outlined herein apply to all employees, consultants, temporary personnel, or others who have access to ProcessUnity information, each of which, have an obligation to protect such information from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional in nature.

1.3. Program Component Definitions

ProcessUnity's Information Security Management System (ISMS) governs the controls that we must implement to ensure we are adequately protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

Policies are high-level directives that are technology neutral. Policies are statements approved and enforced by Executive Management which provide the ground rules for governing the global ProcessUnity environment. These policies will be used as the baseline for all future security related activities for both internal and external entities.

Standards\Matrixes are derived from the policies but deal with specific technologies. A standard describes how to configure a specific technology to be compliant with policies.

Procedures are step-by-step instructions that must be completed to achieve a certain goal.

Guidelines are recommended approaches that are intended to complement Information Security policies, standards, and controls.

Processes are a series of pre-defined operations used to achieve a specific goal.

2. Scope

2.1. Sites and Systems

This policy applies to all ProcessUnity sites and systems as well as to third party solutions utilized by ProcessUnity to process ProcessUnity Information.

2.2. Operational Responsibility

2.2.1. Information Security Executive Sponsor

The Executive Sponsor of ProcessUnity's Information security program shall have ultimate responsibility for the program. Unless otherwise directed by either the Chief Executive Officer or the Board of Directors, the Chief Technical Officer shall be the Executive Sponsor of the Information security program. If the Executive Sponsor, as assigned above, is not available, the executive with acting responsibility for the sponsoring role will be considered the Executive Sponsor. For example, if the Chief Executive Officer is the Executive Sponsor of the Information security program and is unavailable, a member of the Board of Directors would likely be the acting Chief Executive Officer and thus the acting Executive Sponsor of the Information security program. Executive Sponsorship may not be assigned to a role more junior than Vice President.

2.2.2. Executive Management

- Support the implementation, maintenance and improvement of the ISMS.
- Hold membership on the Information Security Committee.
- Provide adequate resources to implement, maintain and improve the ISMS.
- Commit to the fulfillment all ISMS requirements, policies, standards and procedures.

- Responsible for ensuring that employees execute security procedures within their area of responsibility.

2.2.3. Information Security Committee

- Approve ISMS strategies and programs.
- Approve the risk management process including risk assessment methodology, risk acceptance criteria, residual and accepted risks.
- Approve ISMS documentation.
- Approve ISMS policies, processes and procedures.
- Approve the Business Impact Analysis (BIA) and the Business Continuity Plan (BCP).
- Fully review the ISMS at least once a year, or whenever significant changes in the ISMS occur.
- Review results of ISMS audits and reviews and act accordingly to resolve all issues in the most effective way possible.
- Submit the list of projects and requisite funding for approval.

2.2.4. Chief Trust Officer

- Accountable for strategic oversight and outcomes from information security and compliance program.
- Report to executive team and board of directors as needed on security and compliance domains.
- Enable internal go-to-market departments and teams on security and compliance topics.
- Key stakeholder in ideation and testing of Product strategy and roadmap features
- Liaison for prospects and customers regarding security, compliance, and emerging technologies.
- Interface with external authorities for all issues regarding information security.
- Deliver public thought leadership on security and compliance topics via media, industry conferences, etc.

2.2.5. Chief Information Security Officer

- Overall implementation, maintenance, and improvement of the ISMS.
- Chair the cross-functional Information Security Committee. They will decide what topics will be communicated but typically those should include, but not limited to, at least:
    - Risk Treatment Plan tasks status (if any).
    - Audit reports and corrective actions.
    - Incidents.
    - Vulnerabilities.

  - New legal, regulatory, or contractual requirements.
  - Metrics.
  - ISMS documentation review.
  - ISMS Project overall Status.
  - Other security topics.
- Interface between the Information Security Committee and all the departments within the scope of the ISMS.
- Fulfill all ISMS requirements, policies, processes, and procedures.
- Establish, maintain, and coordinate risk management processes that appropriately identify, analyze, communicate and mitigate information security related risks.
- Ensure that the ISMS complies with both business and ISO 27001 requirements.
- Develop, maintain, and improve a training and awareness program in accordance with ISO 27001 requirements.
- Act as the central point for all issues concerning information security.
- Responsible for the audit of information systems to ensure security controls in place, adequate and mitigate the risk as defined by the Information Owner.
- Ensures access to audit tools, software and data files is restricted to those persons who are authorized to perform audit functions. All information retrieved from the audit is considered confidential and must be handled according to the Information Classification and Handling Policy.
- Ensure all non-conformities and security incidents are resolved in the most effective and fastest way possible.
- Coordinate the investigation, communication, documentation, and resolution of information security incidents in accordance with published processes and procedures.
- Establish, collect, analyze, and report ISMS metrics requirements in order track program effectiveness.
- Sponsor external information security assessments.

2.2.6. Information Owners

- Take ownership for all information assets that support their business processes.
- Responsible for identifying records required for legal and regulatory purposes and ensure appropriate safeguards are implemented.
- Ensure the ISMS is implemented within their departments.
- Ensure risk assessments on their information security assets and processes are performed and implement the suggested ISMS controls.
- Ensure all non-conformities and incidents related to their operating area are mitigated in the most effective and fastest way possible.
- Promote awareness of information security requirements and good practices within their operating area.

- Fulfill all ISMS requirements, policies, processes and procedures as communicated to them.
- Assist in the collection and reporting of ISMS metrics, records and evidence that support their business processes.
- Provide support for regular reviews of the compliance of their systems with the security practices.

2.2.7. Information Custodians

Information Custodians are the individuals responsible for overseeing and implementing the necessary controls to protect the information assets at the level defined by the Information Owner. This role is usually a system or network administrator that controls access to a computer, network, or a specific application or even a filing cabinet.

2.2.8. Information Users

- Take responsibility for all company assets that are made available to them.
- Promptly communicate any detected information security incidents or anomalies.
- Fulfill and follow all ISMS requirements, policies, processes, and procedures as communicated to them.

2.3. Subordinate Applicability

All activity on ProcessUnity information assets is subject to monitoring, logging and review for any business reason deemed appropriate by ProcessUnity, including compliance with this Information Security Policy. Anomalous behavior, when identified, should be recorded, and investigated.

3. Policy Statement

3.1. Definition of Information Security Program

ProcessUnity's information security program shall consist of effective administrative, technical and physical safeguards, consistent with accepted industry standards and practices, as necessary to protect against reasonably anticipated threats and hazards; to protect against unauthorized access, use, or disclosure; and to ensure the confidentiality, integrity, and availability of ProcessUnity Information assets and ProcessUnity's information processing assets in accordance with the Information Classification and Information Handling Policies, subordinately defined.

Additionally, the information security program shall consist of other safeguards as necessary to ensure compliance with applicable regulations, required industry standards, and applicable contractual obligations.

The information security program is further defined by the subordinate policies and associated program documents listed by reference herein.

3.2. External Information and Forums

ProcessUnity's Chief Information Security Officer, as well as subject matter experts from throughout the organization, will maintain such associations, memberships, subscriptions, and relationships as necessary to ensure that ProcessUnity remains aware of emerging threats, remains aware of trends in information security practices, and maintains relationships with outside parties as may need to be called upon for specific advice or support in emergency situations.

ProcessUnity shall maintain appropriate contacts with relevant authorities. For the purposes of this policy, relationships maintained by ProcessUnity Corporate Counsel are sufficient to meet this requirement.

3.3. Security Training

All personnel who have access to Confidential Information are required to successfully complete initial security awareness training, including affirmative acknowledgement of their security and privacy responsibilities, and annual refresher training thereafter. Please See ProcessUnity Security Awareness and Training Policy.

The Information Security office must have advanced security training to be unaware of their roles and responsibilities in relation to current security threats which can reduce the risk of security incidents and help detect and mitigate risks. Maintaining security certification like Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) meets this need.

Information security training shall be provided by the IT-Security Department on a regular basis to make staff aware of information security policies, procedures, and responsibilities. All staff shall be trained in the security requirements and processes associated with their job duties, services provided, appropriate business controls, and the correct use of IT systems and facilities.

3.4. Subordinate Policies, Standards, and Procedures

All other ProcessUnity information security policies are subordinate to this Information Security Policy. While each may be modified, reviewed, and approved independently, each is an official extension of this policy document. Together they constitute the ProcessUnity Information Security Program.

3.5. Document Reviews

All information security policies and standards contained herein are subject to review at least once per year. The purpose of the annual review is to ensure that policies and

standards are maintained with respect to the current information assets, technology changes, potential threats, the changing business environment, and other changes that impact information security.

3.5.1. Modification

Policy and procedures changes may be initiated by any stakeholder. It is expected that most changes to the Information Security Policies will be initiated by the Chief Information Security Officer. When policies or procedures are updated their version number should be incremented in accordance with this guidance:

- Minor changes add .1 (e.g. 2.2 to 2.3) until the tenth minor change after which a full step is needed (e.g. 2.9 to 3.0)
- Major changes add a full version number/step (e.g. from 2.2 to 3.0)

Minor changes are those that have limited impact on the primary meaning or intent of the document. Updating the title of a stakeholder or adding an additional approval step in a request process are examples of minor changes. Major changes have a material impact on the meaning or intent of the document. Removing or replacing whole policy sections or adding requirements to address a new regulation are examples of major changes.

Any specific technologies named in policies are subject to change at any time, with necessary leadership approval. The IT-Sec team should monitor for those changes and update the associated policy documents without undo delay.

3.5.1.1. Policy and Procedure Approval

Policy changes will not take effect until the policy has been reviewed and approved by the Information Security Executive Sponsor.

Once the policy has been approved, the approval information shall be added to the Policy's Document History.

Policy changes will not take effect until the policy has been reviewed and approved by the Chief Technology Officer.

3.5.1.2. Exclusions from Approval Process

The following edits may be made without formal review or approval:

- Modification of the Cross References section
- Spelling, punctuation, and grammar corrections that do not alter the content or meaning
- Additions to the Document History section that describe edits made under this Exclusions clause
- The addition of formal approval information to the Document History

3.5.1.3. Distribution and Acknowledgement

- The Information Security policies are documented and available to employees by accessing the IT-Security SharePoint Site, shown below. These documents are considered proprietary and confidential and are intended for use within ProcessUnity only. These documents may not be shared with external parties unless authorization has been granted by the Information Security Office.
- IT-Sec - ProcessUnity Information Security Policies - All Documents (sharepoint.com) ProcessUnity Workers will be informed of any policy changes and will be required to acknowledge, read, and agree to abide by each applicable policy associated to their role:
    - Upon hire
    - Annually
- Information security responsibilities are to be followed by all staff who have access to ProcessUnity's information resources. All Staff must acknowledge in writing that they have read the appropriate Confidentiality Agreement.

3.6. Personnel Security

- Asset protection plays an important role in ensuring information confidentiality, availability, and integrity. Protection measures are introduced at the recruitment or vendor procurement phase, included in the Employee Code of Conduct and Business Ethics, vendor contracts, and monitored during an individual's employment or use of third-party service providers.
- All staff must protect both tangible and intangible corporate assets. Staff are responsible for reporting to the appropriate manager any real or suspected threats to corporate assets.
- Specific information security responsibilities must be incorporated into all contracts with staff who have access to ProcessUnity assets.
- Prior to hire, all employees must pass a background check that includes examination of criminal conviction records, credit bureau records, and verification of previous employment.
- All ProcessUnity employees must be trained to recognize conflicts of interest and the appearance of conflicts of interest during their first week of employment and annually thereafter. All staff must identify and submit to their immediate supervisor any conflicts of interest. All conflict-of-interest statements must be reviewed by the Chief Information Security Officer (CISO). If the CISO identifies a significant conflict of interest, the conflicts must be discussed with the staff member's immediate supervisor to determine the appropriate course of action.
- The CISO will implement a system for security incident reporting, response, tracking, and resolution. All staff are responsible for reporting to the appropriate ProcessUnity manager any violations of this Policy.

- The Human Resources Department is responsible for ensuring that background checks are performed on ProcessUnity employees. Background screening helps determine whether a particular individual is suitable for a given position. Generally, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening alone to reduce the risk to ProcessUnity. Pursuant to local laws, regulations, ethics, and contractual constraints all employment candidates, contractors and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk.
- Executive management shall ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Department Heads are responsible for enforcing compliance with this policy.

3.6.1. Performance Evaluations

Employee performance is consistently being monitored during their tenure at ProcessUnity. Formal performance evaluations are completed by managers on an annual basis.

3.7. Governance

Information Technology (IT) - Security (IT-Sec) governance is a part of the organization's corporate governance. IT-Sec governance is focused on Information Resources and their performance and risk management. IT-Sec governance helps ensure that the organization properly manages its projects, service delivery, and compliance requirements.

ProcessUnity's IT-Sec governance and management framework exist to:

- Align the organization's IT and Security requirements with the organization's business goals and objectives.
- Enable high-quality enterprise IT-Sec planning and management.
- Define the roles and responsibilities necessary to create and sustain a comprehensive governance, planning and management framework.
- Enable new strategic capabilities that allow ProcessUnity to operate efficiently and effectively.
- Identify and manage risk and protect ProcessUnity's Information Resources.

The IT-Sec Department provides the central point of accountability, leadership, vision and coordination for the enterprise. The IT-Sec Department is responsible for:

- Design - design and implement processes necessary to govern, plan, manage, oversee, evaluate, and implement business planning, technical architecture, standards, information and telecommunications resource management planning, budgeting, funding, quality assurance, asset inventory and management, procurement, security, and performance standards and measurements.

- Governance - provide governance for enterprise IT-Sec coordination, planning, decision-making, and policy development.
- Tracking - coordinate, facilitate, track and report to executive management, the status of IT-Sec projects.
- Communications - develop and implement IT-Sec communications and management support infrastructure including enterprise focused information sharing.
- Policy - create the policies, standards, and practices necessary to carry out the directives of ProcessUnity management as they pertain to IT-Sec.
- Initiatives - act as the sponsor for IT-Sec initiatives including research, identification and development of opportunities, proof-of-concept, etc.
- Assessment - establish and maintain a technical assessment capability through which to evaluate information and telecommunications technologies and management practices.

Policies and procedures shall require management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.

3.8. Policy Exceptions & Risk Acceptance

All exceptions to the Information Security Policies must be approved by one of the following:

- An officer of the company
- The Chief Information Security Officer in conjunction with a Vice President (or above) where the approving Vice President is neither a manager of the requestor nor themselves the requestor of the policy exception.

All exceptions and their approvals will be documented.

The Chief Information Security Officer will review all open exceptions on a semi-annual basis to confirm that the resultant risk remains acceptable, and, where practical, create and manage projects to eliminate the need for each exception.

This Policy Exception Process is strongly recommended but not required for exceptions to Associated Program Documents, as listed above.

3.9. Policy Compliance

The Chief Information Security Officer and the Executive Sponsor are responsible for ensuring that this policy is enforced. Informally, the CISO will monitor company-wide conformance with this policy on an ad-hoc basis throughout the year. Formally, the Executive Sponsor will monitor company-wide conformance with this policy on an approximately annual basis by performing, or causing to be performed, an audit or an

assessment or series of audits and assessments of the Information Security Program that, in their judgment, test the overall effectiveness of the program and the overall conformance of the program to the combined Information Security Policies.

Any findings identified by these monitoring activities that expose the organization to undue risk shall be remediated in a timely fashion.

4. Enforcement

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

Violations of any policies covered by this policy are subject to discretional disciplinary action up to and including termination. Specific disciplinary action for violations is determined once forensic activities are completed as part of standard incident response procedures.