Security Awareness and Training Policy

Revision History

Revision Date	Summary of Changes	Version	Updated By	Changes marked
1/19/23	Added History and Property sections, updated document after review. Updated Training Schedule, consolidated the ProcU Training Policy		mchatzopoulos	N
1/31/24	Added Slavery and ESG Annual training		mchatzopoulos	N
2/1/24	Annual Review	2.0	Dstapleton	N
9/30/24	Updated content of annual training campaigns	2.1	Dstapleton	N
2/10/2025	Annual review and minor edits	2.2	Dstapleton	N
5/22/2025	Re-classified prior to posting to Trust Center	2.3	Dstapleton	N

Document Properties

Status	Check Sharepoint for Status
Document Owner	VP, Chief Information Security Officer
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 Security Awareness and Training Policy defines the requirements for establishing a security awareness program and additional training that Workers may need or want to take.

1.1. Purpose

To establish a security awareness program that provides timely and periodic security training and awareness materials and classes to ProcessUnity Workers that are both general in nature and tailored to the information handling and operational responsibilities of various worker roles.

The policy emphasizes the importance of maintaining a continuous learning program to develop a core of well-trained individuals whose performance will enhance the company's abilities to perform at a level that is consistent with growth and profitability objectives.

2. Scope

2.1. Operational Responsibility

The Chief Information Security Officer is responsible for maintaining the Security Awareness and Training curriculum.

The Information Technology Department is responsible for tracking participation by ProcessUnity Workers.

2.2. Subordinate Applicability

All ProcessUnity Workers must complete assigned security awareness and training activities in a timely fashion.

This policy applies to all ProcessUnity workers who have direct access to any ProcessUnity sites, systems, or applications.

This policy shall not apply to consultants who have no access to ProcessUnity sites, systems or applications.

3. Policy Statement

ProcessUnity shall provide such information security awareness and training as is necessary to ensure that all ProcessUnity Workers are familiar with ProcessUnity's Information Security Policies, are familiar with their information protection responsibilities, and are familiar with information handling requirements for Privacy Information.

This training and awareness shall, at a minimum, include the following:

Awareness/Training	Curriculum	Applicability	Frequency
Policy & Procedure Acknowledgement	All Policies and Procedures	All ProcessUnity Workers	Hire Date Annually
Refresher Courses	Varied Courses pushed out throughout the year. Phishing, Smishing, Passwords, Data Privacy and Handling, Bribery	All ProcessUnity Workers	Quarterly
Information Security Awareness Training	General Security Awareness Training (including Phishing and Malware), Strong Passwords, Remote Working. Handling Sensitive Information, ISO 27001, GDPR Specific Policies: 1. BYOD 2. Teleworking 3. AUP (includes Ethical Behavior) 4. Code of Business Conduct and Ethics	All ProcessUnity Workers	Hire Date Annually Note: If the New Hire Date is during the annual awareness training, the users are required to complete only one.
Secure Coding Best Practices (including OWASP Top 10)	Data and Password Hygiene Memory Management OWASP Top 10 Protecting Source Code Specific Policies: 1. Secure Coding Guidelines and Standards 2. Secure Software Development Lifecycle Policy 3. Open Source Usage Policy	ProcessUnity Workers who write or modify source code.	Hire Date Annually
ESG and Human Trafficking\Slavery Awareness	Environmental, Social, and Governance Awareness and Human Trafficking and Slavery Awareness.	All ProcessUnity Workers	Annually
Phishing Simulation Campaigns with Additional Phishing training for "Clickers"	Simulated Phishing Emails	All ProcessUnity Workers	Quarterly
Incident Response First Responder Training	Tabletop exercises and review: Incident Response First Responder Training educates administrators on how to identify and escalate potential information security incidents. This training includes: • How to identify a potential incident • How to escalate a potential incident • How to avoid disturbing evidence of an incident	ProcessUnity Workers with facility, network, system, application, or database administration responsibilities.	Annually

Awareness/Training	Curriculum	Applicability	Frequency
Business Continuity Training	Tabletop exercises and review: Business Continuity Plan training educated ProcessUnity Workers on their role during a Disaster Incident as well as on how to use the Business Continuity Plan. This training includes: • Worker safety • How to initiate the Business Continuity Plan • How to use the Business Continuity Plan	All ProcessUnity Workers	Annually

3.1. Other Training

ProcessUnity emphasizes the importance of maintaining a continuous learning program to develop a core of well-trained individuals whose performance will enhance the company's abilities to perform at a level that is consistent with growth and profitability objectives.

Professional Development is identified as training needs which are recognized as a means for an employee to improve their performance, their development as a professional within the organization, or as a means of their retaining and developing key skills and competencies.

ProcessUnity may provide and require other training from time to time as may be necessary to meet the objectives of this policy. Furthermore, training needs may be identified as a result of a corporate and/or policy change; which will affect everyone within the organization, and this will come under the same category

3.1.1. Examples of Additional Training

- New hire training
- Product training
- Role Based Training
- Systems and Security training
- Compliance training (i.e. Sexual Harassment Training provide by HR)
- Leadership training
- Sales training

3.2. General Awareness

The Chief Information Security Officer shall set a company-wide tone of security awareness by providing informal reminders from time-to-time including:

- Presentations to senior management
- Security Awareness messages via e-mail
- Security Awareness posters

3.3. Consultants

Where Contractors are effectively employees with an indirect compensation relationship to ProcessUnity but who report to ProcessUnity Management and Consultants are employees of consulting companies and where the consulting company, not the Consultant, is engaged on a project basis, this requirement can be met for Consultants by contractually obligating the consulting company to provide materially similar information security training and awareness internally within their own organization.

4. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.