Business Continuity Policy

Revision History

Revision Date	Summary of Changes	Version	Updated By	Changes marked
1/19/23	Added History and Property sections	2.0	mchatzopoulos	N
2/2/24	Annual review	2.1	Dstapleton	N
2/5/25	Updated history and property, update BIA	2.2	mchatzopoulos	Y
2/12/2025	Annual review	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	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 Business Continuity Policy defines the requirements for maintaining and testing a Business Continuity Plan.

1.1. Purpose

The purpose of this Business Continuity Policy is to define the high-level requirements for a business continuity program including the maintenance and testing of a Business Continuity Plan.

2. Scope

2.1. Sites and Systems

This policy applies to all ProcessUnity sites and systems.

2.2. Operational Responsibility

The Chief Information Security Officer is responsible for maintaining the Business Continuity Plan.

All ProcessUnity department heads are responsible for ensuring the Business Continuity Plan meets the needs of their department.

2.3. Subordinate Applicability

This policy applies to all ProcessUnity Workers.

3. Policy Statement

ProcessUnity shall have a business continuity program which maintains a Business Continuity Plan and a Disaster Recovery infrastructure necessary to ensure that continuity of the business in the event of a natural or man-made disaster. These include - but are not limited to – the following:

Natural Disasters	Man-Made Disasters
• Damaging Winds • Drought & Water Shortage • Earthquakes • Pandemics • Extreme Heat • Floods • Hail • Hurricanes & Tropical Storms • Landslides & Debris Flow • Snow & Ice Storms • Thunderstorms and Lighting • Tornadoes • Tsunamis • Wildfire • Pandemics	• Chemical or Biological Emergency • Civil Unrest • Cyber Attack • Explosion • Hazardous Materials Containment Incident • Nuclear or Radiological Emergency • Power Disruption or Blackout

3.1. Priority

The safety of ProcessUnity Workers shall be the top priority in the event of any disaster.

3.2. Business Impact Analysis

ProcessUnity shall conduct and document an annual Business Impact Analysis (BIA) per department. The BIA will:

- Identify a representative of the departments that are critical during a disaster
- Detail the non-financial impacts of the department not being able to perform their roles
- Understand the minimum staff required to support their roles and critical business processes
- Identify critical business processes they perform
- List the software and third parties required to support the business. For each of these:
    - The importance
    - RTO
    - RPO
    - Financial Impact

- Scope of the service

3.3. Disaster Recovery Solution

ProcessUnity shall design, build, and maintain a disaster recovery solution including the alternate sites and systems necessary to meet the business continuity requirements documented in the Business Impact Analysis.

The location of alternate sites shall be sufficiently dispersed to ensure that incidents impacting a site are unlikely to impact its backup site. The suitability of a particular distance between sites should be determined during the Business Impact Analysis.

3.4. Business Continuity Plan

ProcessUnity shall develop and document one or more Business Continuity Plans that articulates the following:

- Process for declaration of a disaster.
- Procedures for contacting all ProcessUnity Workers.
- Procedures for each ProcessUnity Worker to follow during a disaster.
- Procedures for activating the Disaster Recovery Solution.
- Procedures for resumption of business as usual activities.

If more than one plan is developed, they shall use a common framework.

3.5. Business Continuity Training

ProcessUnity shall conduct annual Business Continuity Training to ensure that all ProcessUnity Workers understand their responsibilities during a declared disaster and to ensure that all ProcessUnity Workers are familiar with the Business Continuity Plan and where to find business continuity program materials during a disaster.

3.6. Business Continuity Test

ProcessUnity shall conduct an annual Business Continuity Test to validate that the Business Continuity Plan works and that all ProcessUnity Workers have been appropriately trained.

If a failure is noted during the test, a root-cause analysis shall be performed and the Disaster Recovery Solution and/or the Business Continuity Plan shall be updated to ensure success. ProcessUnity Workers will be re-trained on the new solution and plan. If the nature of the test failure was material in scope, ProcessUnity shall re-perform the test.

3.6.1. Security Tests of Disaster Recovery Solution

Separate from the Business Continuity Tests, any Disaster Recovery solution deployed in compliance with *Section 3.3 Disaster Recovery Solution* must be included in any Information Security Testing conducted according to the Information Security Policy, the Risk Assessment Policy, or the Vulnerability Management Policy.

3.7. Applicability of Information Security Policies

The Business Continuity Plan does not supersede, suppress, or obviate ProcessUnity's information security policies. ProcessUnity's information security policies are to be considered in full effect and force during recovery from an incident.

As with all information security program policies, exceptions to this policy may be defined and approved as defined by the Information Security Policy.

4. Enforcement

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