Business Continuity Planning and Disaster Recovery Policy

Version number	3.2
Last Approved	Apr 22, 2025
Classification	PUBLIC

Overview

The Business Continuity Planning (BCP) and Disaster Recovery (DR) Policy defines the processes by which the Company maintains and tests risk-based resiliency plans for its business and systems.

Disaster Recovery (DR) addresses customer-facing continuity in its hosted systems and is inclusive of customer data.

This policy ensures that the Company will perform regularly scheduled BCP / DR testing to align the Company's capabilities with its risk posture and Client commitments.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview.

Purpose

This policy establishes principles and requirements to ensure that the risk of interruption to its business operations and SaaS services is maintained within tolerable levels that also align with its legal, regulatory, and contractual commitments.

Scope

BCP and DR encompass the comprehensive set of processes responsible for ensuring protection and continued availability of Company assets and applications at all times. This policy covers subsequent remediation plans for risks such as (but not limited to):

- Cyberattack;
- Pandemic Natural Disasters (Floods, Hurricanes, Tornadoes, Earthquakes);

- Civil unrest;
- Acts of Terrorism;
- Fire;
- Health & Safety Issues;
- Senior Management Succession;
- IT/Business tool unavailability.

Business Continuity Planning

The Company shall complete the following components of the Business Continuity Planning effort on an annual basis:

Business Impact Analysis

The Business Impact Analysis may include any of the following, as deemed appropriate:

Elements	Guidance
Business Process Inventory	• Captures general information about the process as well as the dependencies on which the process relies, including not only IT systems but also physical, environmental, human or other dependencies • Indicates criticality of each process
Dependency Inventory	• Captures dependencies on which business processes rely • Captures estimated or actual recovery time objectives for each dependency
Impact Assessment	Captures management's assessment of the impact to The Company in the event of a critical process outage.
Risks	Describes known risks to business process continuity
Recovery Plans	Describes existing recovery plans that have been developed for the department's operations

Subcontractors & Suppliers	Lists (and describes the functions performed by) any subcontractors or suppliers that are critical to the continuity of business processes
Other comments	Documents any additional concerns that may be relevant to a given process

Business Continuity Plan

The Business Continuity Plan builds on the Business Impact Analysis as necessary to elaborate processes and/or measures necessary to ensure resiliency levels aligned with objectives.

Among these processes, the most critical is Disaster Recovery Planning.

Facilities Dependencies

Due to The Company’s fully remote-capable workforce, traditional considerations related to facilities dependencies are not applicable; for example, internal call trees and stakeholder communication plans for in-scope facility locations. Residual facility dependencies are Third Party and therefore, stakeholder contacts and communication plans are maintained via vendor management process.

Plan Improvements, Testing & Risk Acceptance

Improvements to the Business Continuity Plan and acceptance of residual risk to Business Continuity shall be performed by the Executive Security Steering Committee for Business Continuity Planning efforts.

On an annual basis, the Company will perform a thorough test of the Business Continuity Plan to evaluate its comprehensiveness and effectiveness relative to the Company’s Business Continuity objectives and commitments.

Any critical deficiencies identified during Business Continuity or Disaster Recovery testing will either be addressed in alignment with the Company’s Vulnerability Remediation SLAs (30 days for Critical/High; 90 days for Medium) or contemplated in the subsequent Executive Security Steering Committee to determine appropriate risk management measures. Ownership of follow-up and remediation responsibilities for all critical findings are assigned promptly upon completion of annual testing (not to exceed 30 days).

Disaster Recovery

Disaster Recover ensures that the Company has well-defined and tested capabilities for restoring in-scope system availability and data that meets defined **Recover Time** and **Point Objectives** (RTO and RPO). The Company will maintain updated documentation of DR procedures. On at least an annual basis, the Company will thoroughly test its DR capabilities by conducting disaster recovery tests across its systems. The results of DR testing will be measured against the recovery objectives and remediation plans identified and implemented for any gaps.

SOC 2: A1.3

> *The entity tests recovery plan procedures supporting system recovery to meet its objectives.*

Data Center Distance Criteria: Each data center (primary and secondary) shall be no closer than 60 miles or 100 km from its proposed regional counterpart.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Apr 23, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Apr 22, 2025	@Art Machado @Paul Gordon @angelina.kilmer	3.2	Removed Risk Management Policy references from BCP/DR Policy
Apr 9, 2025	@Paul Gordon	3.1	References made to ISO 42001
Feb 25, 2025	@Paul Gordon @Art Machado @angelina.kilmer	3.0	Annual review
Nov 01, 2024	@angelina.kilmer	2.12	Changed Policy classification from Confidential to Public
Jun 26, 2024	@Art Machado & @angelina.kilmer	2.11	Updated Plan Improvements, Testing, and Risk Acceptance section with regards to critical deficiencies ownership and remediation. Updated Medium and Low risk ratings.
Mar 12, 2024	@Art Machado , @Sarah Zwicker (Unlicensed) , @Paul Gordon	2.10	Annual review, approver change.

May 16, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	2.9	Remediation timeline alignment to Vulnerability Management policy. Considerations for facilities.
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	2.8	Annual Review, logo change, update to Risk Assessment section
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	2.7	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	2.6	Title change for VP InfoSec, Annual Review
Jun 22, 2021	@Sarah Zwicker (Unlicensed) & @Art Machado	2.5	Updated policy to reflect changes in the Risk Assessment section.
Mar 10, 2021	@Sarah Zwicker (Unlicensed)	2.4	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.3	Reformatting, policies linked
Jan 26, 2021	@John Cole	2.2	Annual review, role title change

Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.1	Changed owner. Added sections to refer to LTG policies and organizational change.