Business Continuity Policy

Purpose

The purpose of this policy is to establish requirements and plans to recover <Company Name> operations following a disruption due to causes such as natural disaster, loss of access to premises, pandemic, or malicious activity from external or internal sources.

Scope

This policy applies to all <Company Name> systems determined to be of critical importance to the business, as described in the Impact Analysis

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

<Company Name> employs continuity planning and disaster recovery to enable the continuous operation of its product(s) without unacceptable interruptions or data loss. <Company Name> establishes plans and technical measures that are commensurate with the complexity and risk of each component, taking into account its function and data.

Business Continuity

Impact Analysis

As part of its continuity planning, <Company Name> performs analysis of its systems and assets classified according to the Data Classification Policy, and determines the criticality of each component to the business. This analysis is performed annually, or upon significant architectural changes or additions of new key vendors.

Critical systems are systems that store Customer Confidential data, as well as those that are deemed business-critical by the team. For each critical system, <Company Name> determines impact and risk, and plans contingencies accordingly.

Business location

<Company Name>'s operations do not require access to a physical office. Company employees are fully equipped and empowered to work from home and perform all business critical functions, including developing and operating its products, and communicating with each other as well as with customers. Further information on home office security is available in the Physical Security Policy, and Authentication and Password Policy.

Data Backups

<Company Name> data backups are stored, retained and tested as described in the Backup Policy and all related backup controls.

Data Centers

<Company Name> uses established Infrastructure-as-a-Service cloud providers to procure the necessary infrastructure required to meet its business objectives. These cloud vendors provide and manage best-in-class data centers that offer asset management, redundant power and networks, and physical security. The company employs security controls to govern its obligations as part of the shared responsibility model required by each cloud provider.

Contingency Planning

<Company Name>'s operating infrastructure consists of 3 main parts:

- Cloud environment hosting <Company Name>'s product
- Physical office(s)
- Critical third-party vendors

Cloud environment

As mentioned in the "Data Centers provided by Cloud Providers"

Disaster Recovery Plan

The company maintains a Business Continuity Policy which outlines a plan to recovery from prolonged disruptions in operations.
[POLICY OWNER]
is responsible for managing any disaster recovery efforts by following the plan outlined herein.

The Disaster Recovery plan outlines the main stages that<Company Name> follows to bring its systems back online following a major disruption. The exact actions performed in each phase will differ depending on the type of the disruption, but following this plan will facilitate consistency, clear communication, and minimization of impact.

Phase 1: Declaration and notification

A disaster is declared when it becomes clear that an ongoing disruption or outage will significantly exceed the standard time required to resolve an incident. Since exact definitions

are hard to formalize, the incident manager and their team of subject-matter experts (SMEs) must determine on a case-by-case basis whether to move into the Recovery phase of the plan, or whether to wait for the issue to be resolved following <Company Name>'s standard resolution strategy.

[POLICY OWNER]
 is responsible for leading disaster recovery efforts, involving any necessary SMEs, and communicating to business stakeholders.

Phase 2: Recovery

The Recovery phase consists of the steps required to create a new production environment and divert traffic to it.

If the original cloud region is experiencing degraded performance or is otherwise unavailable, the new environment may be created in a different region.

In order to prepare for this phase, <Company Name> maintains:

- Infrastructure scripts and code for creating a new production environment, including the creation and configuration of networks, accounts, databases, and any computing clusters
- Access to sufficient backup copies to satisfy the required Recovery Time Objective
- An ability to update DNS records to point to a new environment

Explicit procedures to recover and validate individual components belong with the component's internal documentation, and are not outlined in this policy.

After all components are restored, testing is performed to ensure that the new environment is fully functional, before making it accessible for customers. As a final step, the team communicates resolution to all affected customers using the appropriate channels.

Phase 3: Retrospective

The Retrospective phase establishes a blame-free environment that allows all parties to gain a clear understanding of the incident and its resolution. A retrospective meeting should occur within 1 week of a disaster recovery event.

Retrospective meetings must definitively outline the root case and response timeline, along with any lessons, as well as action items for improving tooling, process, and software. Following the meeting, a retrospective report outlining key items should be created and shared with all participants and relevant stakeholders. Depending on customer impact, a customer-facing version of the report may be created and shared with customers as required by legal obligations and customer agreements.

Disaster Recovery Testing

A disaster recovery test with predefined RTO goals is performed annually, assuming a full outage of our primary cloud region.

A disaster recovery test with predefined Recovery Time Objective (RTO) goals is performed annually, assuming a full outage of the primary cloud region.

Disaster recovery testing is essential for ensuring <Company Name>'s readiness to stay within its RTO and RPO goals, and for confirming <Company Name>'s ability to both act and communicate quickly both internally and externally.

The main DR capability of <Company Name> is the ability to create a new production environment from scratch, potentially in a separate cloud region, and seeding it with a restore of previously backed up production data.

This capability has two requirements:

- Data backups are sufficiently isolated from the regular production infrastructure boundary. If backups are stored along with the data, then the attacker or an accident can affect both. Sufficient isolation requires that the backups are stored in a separate physical region, under a separate cloud account with a different set of account credentials.
- Infrastructure setup is maintained as code or equivalent procedural documentation exists, to ensure a speedy recovery in an automated or scripted fashion.

This capability addresses disaster scenarios such as:

- Ransomware and cyberattacks
- Unintentionally erased databases, files or folders/buckets
- Prolonged datacenter outage

Due to its distributed workforce, <Company Name>'s operations are well protected against pandemics, because all employees are equipped to securely work from home.