deverus

Business Continuity Plan

1.Overview

We plan to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and property, making a quick operational assessment, protecting corporate resources and data, and allowing our customers to transact business. In short, our business continuity plan is designed to permit us to resume operations as quickly as possible, taking into account the scope and severity of the business disruption.

2.Scope

Our business continuity plan addresses: data backup and recovery, mission critical systems, operational assessments, and timely communications with customers and employees.

3.History

Version	Description	From	To	Author
1.0	Initial version	2/1/2018		Terry Greenlaw

4.Team

The CEO and COO are the primary members of the business continuity team. They are the only two employees allowed to incur costs related to business continuity without prior authorization.

During a significant business disruption, they will assemble additional teams as necessary to generate a business impact analysis, and to address any immediate continuity concerns.

5.Facilities

5.1.Office Locations

Our office is located at 1708 West 6th Street, Austin TX 78703. Its main telephone number is 888.690.9297. We engage in operations, software development, and user support at this location. No production or development equipment or data are housed at this location.

deverus

6. Alternative Physical Location(s) of Employees

In the event our primary office location is unavailable, our employees will work from home utilizing secure VPN access to access our production, development, and stage environments from our virtual private clouds in AWS. Employees use corporate laptops to access our systems, so our desktop hardening, appropriate use, and antivirus policies are maintained.

7. Data Backup and Recovery

7.1. Physical Backups

We do not depend on physical backups for any services we deliver to our customers or employees.

7.2. Electronic Backups

All electronic backups are distributed across multiple datacenters within the AWS infrastructure. We maintain multiple copies of our application code distributed across GitHub, our servers distributed across multiple datacenters in AWS, and on our developer's computers.

Our databases are fully backed up nightly, with incremental log backups occurring throughout the day.

Additional details regarding data backup and restoration are contained in our backup policy documentation.

8. Communications

In the event of a significant business disruption, we will determine the best methods for us to communicate with our customers, employees, and critical business partners, and then will make our best efforts to inform all affected parties customers regarding the business disruption within 4 hours.

9. Mission Critical Systems

Our company's "mission critical systems" are those that ensure prompt and accurate processing of transactions, including order taking, data entry, submitting orders to researchers, the maintenance of customer accounts, access to customer accounts and the delivery of information to the end consumer. These systems include our application servers, databases, web application firewalls, load balancers, and task servers. For other infrastructure components like DNS and network firewalls, we rely on the highly available and distributed AWS services.

For business continuity purposes, all servers, databases, and web application firewalls are configured in an “active/active” high availability mode, and are distributed across multiple datacenters in the AWS US East 1 region.

We have a primary responsibility to establish and maintain our business relationships with our customers, and have sole responsibility for our mission critical functions of order capture, order routing and return of results.

10.Recovery Time/Resumption Time Objectives

Recovery time objectives provide concrete goals to plan for and test against. They should not, however, be considered hard and fast deadlines that must be met in every emergency situation. Various external factors surrounding a disruption, such as time of day, scope of disruption, and status of other critical infrastructure components can affect actual recovery times. Recovery time refers to the restoration of basic functionality after a wide-scale disruption; resumption time refers to the capacity to accept and process standard volumes of business transactions after a wide-scale disruption. We have the following significant business disruption recovery time and resumption objectives: recovery time period of 12 hours, and resumption time of 36 hours.

11.Researchers and Other Third-Party Dependencies

Our research partners and data providers may also experience significant business disruptions, which could impact our ability to perform certain types of transactions. When this occurs, we will make every effort to communicate the disruption via website message, email, or alternate communication method to our customers in a timely manner. However, due to the manual nature of some research transactions, we may not immediately be aware of the disruption. Per the Communications section of this document, we will make every effort to communicate third-party disruptions within 4 hours of us being notified of the disruption.

12.Training and Testing

We are continuously testing application deployment and database recovery as part of managing our high availability architecture. Because of this, we do not currently schedule disruption recovery scenarios or document their outcomes.

13.Updates and Annual Review

We will update this plan whenever we have a material change to our operations, structure, business or location. In addition, we will review this plan annually, to ensure it remains in alignment with our business goals and the needs of our customers.