Disaster Recovery
Process & Procedure

Last Updated October 4, 2023

Purpose

It is our top priority to make our clients' data available when and where they need it, in the cleanest, most organized way feasible. The purpose of this Disaster Recovery & Business Continuity Plan is to outline how we will fulfill this purpose, even if a disaster were to affect our operations.

Disaster

A disaster is any event or circumstance that restricts our ability to deliver our software to our customers for more than 24 consecutive hours, or that prevents us from operating out of our current facilities for more than 1 week.

Order of Recovery

In the event of a disaster, the following would be the priority for recovery of our operations:

1. Continuous Delivery of Software
2. Software Development Operations
3. Support
4. Onboarding
5. Software Development
6. Business Administration
7. Sales
8. Product
9. BI, Compliance & Project Management
10. Marketing

Procedure

Company & Software

We have architected our applications to facilitate automatic scaling or adjustment (fail-over). This keeps our applications running as seamlessly as possible, and limits downtime and recovery time, in the event of a disaster. We have also taken steps to ensure adequate data backup (See Data Backup Policy), rapid data recovery, and geographically diverse systems and personnel.

Responsibilities & Roles

LoanPro Software has well-defined roles for our team members, in the event of a disaster, to ensure efficient recovery of the application. These roles and responsibilities are in force even outside times of disaster. They cover the following areas: Preparation, Testing, Identification, Assessment, Containment, Eradication, Recovery, Post Mortem.

Customer Notification

In the event of a disaster that has an impact on the LoanPro Software application, our organization will provide updates on the third-party provided Status page.

Software Application

Our software operates inside of the AWS (Amazon Web Services) Cloud platform. This provides us with significant disaster recovery options. We operate with a “hot standby” database which continuously mirrors data from the primary database and a “pilot light” system to enable more server power on the fly when needed for queued job processing and web traffic. AWS servers and databases are available in various geographically-diverse zones to insure against a localized disaster. This can all be managed remotely through an AWS dashboard allowing for quick deployment and automated scalability as needed. On the EC2 platform, the current AWS service commitment is to provide 99.9% monthly uptime.

We utilize Amazon’s world-class data centers, which are highly secure data centers equipped with state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. Data centers located across multiple geographic regions (Availability Zones) allow for the effective mitigation and management of disasters. In the worst-case scenario, we have architected system deployment which includes the streamlined ability to deploy the application to a new AWS region if necessary in a matter of hours.

Support & Phone System

We utilize VoIP phone systems with a fallback to landlines (or cell) in case of power or internet outages. In addition, at all of our support centers we operate with multiple internet providers and onsite backup generators in case of power outages. If a disaster were to disable our office for an extended period of time, we have the ability for support staff members to work remotely until the disaster is resolved. This allows us to continue to serve our clients throughout the disaster.

Geographic Diversification

We have diversified operations in multiple locations, including our headquarters in Farmington, Utah, USA. In addition to our headquarters and various locations in México. This diversification ensures that a local disaster will not affect our entire team. We also utilize servers across two continents that are backed up in geographically separate locations. This will ensure that at least part of our team has Internet access to be able to continue providing assistance and support to our clients. Our headquarters operates with redundant internet providers to ensure constant connectivity to provide service to our Clients.

Non-Time-Critical Recovery

LoanPro has insurance to cover our building, furniture, computers, etc. at our offices. Because of well-designed software architecture in the AWS Cloud, recovery time for impacted items to our clients should be very limited, in the event of a disaster our physical office is not required in order to have the application fully functional.

Specific Scenario

LoanPro has implemented measures to mitigate the threat of disaster.

Database Failure — In the event that one or more of our primary databases fails, we employ a synchronized backup database, in a separate geographic location, that will take over. Should every primary database and corresponding hot standby fail, we keep 30 days worth of daily server backups, which are stored on Amazon's S3. Every 30 days, these data backups are stored in a magnetic format that can be put into service in 24-hours if all other backups fail. See Data Backup Policy for more details.

Server Failure — LoanPro has spent significant time structuring our code to make it possible to add new server instances on the fly. If any server fails, we can automatically create a new server and bring it into service. In addition, we employ a dynamic load balancer to route traffic automatically which will result in limited/no impact to our clients in the event of a server failure.

Security Breach — LoanPro employs the latest security measures and testing to keep unauthorized users out of our software. Customer databases are separated to keep users from unauthorized data access. LoanPro stores personally identifiable information with a minimum of 256-bit encryption, making data that was illegally accessed very difficult, if not impossible, to

use. Please review our data security breach policy for more details on how such an event would be handled.

Significant Loss of Personnel — LoanPro employs personnel in multiple countries across many geographic areas. While a reasonable number of them work at our main office, many of them, including a portion of our key personnel, work in satellite offices of sufficient distance that they would not all be affected by a localized disaster. Our company has policies and procedures in place that allow us to conduct normal business even if we suffer a significant loss in personnel.

The inability of 40% or more of LoanPro personnel to work for a duration of 5 or more consecutive days is a disaster for us. When this happens, we implement policies to shore up our customer support with key personnel, and suspend software releases until the percentage of employees who can't work drops below 30%. We also have a succession plan that specifies a trained backup for all key responsibilities.

Loss of Key Personnel — In the event that LoanPro loses a significant number of key personnel, there is an established hierarchy in place that dictates seniority among existing officers. LoanPro has worked hard to document its policies, procedures, relationships, codebase and succession plans to enable new and existing employees to carry on company operations if key personnel are lost. We have implemented a company knowledge base that includes documentation on every area of the business in an attempt to decentralize information and eliminate "islands of knowledge".

System Monitoring — We have both automatic 24x7 system monitoring as well as a rotating on-call Development Operations team monitoring the software application at all times. This business policy results in very short response times to address any disasters that may occur.