Business Continuity and Disaster Recovery Policy

Last Updated **May 14, 2025**

Purpose

It is LoanPro's top priority to make 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 LoanPro fulfills this purpose, even if a disaster were to affect its operations.

Disaster

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

Order of Recovery

In the event of a disaster, the following is the priority for recovery of LoanPro's operations:

1. Continuous Delivery of Software
2. Software Development Support/Operations
3. Customer Support
4. Onboarding
5. Software Development

6. Business Administration
7. Sales
8. Product
9. Compliance & Project Management
10. Marketing

Procedure

Company & Software

Loanpro has architected its applications to facilitate automatic scaling or adjustment (fail-over). This keeps its applications running as seamlessly as possible, and limits downtime and recovery time, in the event of a disaster. LoanPro has 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 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, the organization provides updates on the third-party provided Status page as per the Status Page Process.

Software Application

LoanProsoftware operates inside of the AWS (Amazon Web Services) Cloud platform. This provides significant disaster recovery options. LoanPro operates 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 is an elastic infrastructure and can be expanded instantly. Some cases include auto expansion using a warm pool for EC2 instances based on percentage of load on each EC2 instance. AWS servers and databases are available in various geographically-diverse zones to insure against a localized disaster. This is 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 99.90% monthly uptime.

LoanPro utilizes 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, LoanPro has 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

LoanPro utilizes VoIP phone systems with a fallback to landlines (or cell) in case of internet outages. In addition, all of the support centers operate with multiple internet providers. If a disaster were to disable the office for an extended period of time, there is the ability for support staff members to work remotely until the disaster is resolved. This allows them to continue to serve clients throughout the disaster.

Geographic Diversification

LoanPro has diversified operations in multiple locations, including headquarters in Farmington, Utah, USA. In addition to the headquarters, it has employees in various locations in the United States, México and other countries in the continent. This diversification ensures that a local disaster doesn't affect the entire team. LoanProalso utilizes 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 its clients should be very limited, in the event of a disaster the 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, LoanPro employs a synchronized backup database, in a separate geographic location, that takes over. Should every primary database and corresponding hot standby fail, LoanPro keeps 30 days

worth of daily server backups, which are stored on Amazon's S3. See Data Backup Policy for more details.

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

Security Breach — LoanPro employs the latest security measures and testing to keep unauthorized users out of the software. Customer databases are separated to keep users from unauthorized data access. LoanPro stores main 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 the 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. If 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.

Ransomware Attack — We utilize advanced technologies for ransomware protection, including MFA, backup services, anti-malware software, intrusion detection and prevention systems and encryption tools. These technologies can detect and prevent ransomware attacks before they cause significant damage.