# LoanPro Data Breach & Incident Response Process & Procedure

**Last Updated March 30, 2023**

## Purpose

LoanPro Software enforces rigid security protocols to prevent data security breach. These controls cover data access by all parties, and data-storage procedures including encryption, rotation of keys, firewalls, and other security measures. The purpose of this document is to outline our policies and procedures in the event that our data security is breached, physical or logical.

Data Breach/Incident types:

- Physical Security Breach
- Information Systems Failure
- Malware Activity
- Denial of Service Attack
- Loss of Data Integrity
- Breach of Confidentiality
- System Exploit
- Unauthorized Logical Access

## Players

**Potential incident reporter —** Any team member in LoanPro that detects any potential security breach, either logical or physical that can compromise the integrity of LoanPro, customer or borrower confidential data.

**Software Support team —** In charge of classifying and resolving any technology related data breach.

**Facilities team —** In charge of classifying and resolving any physical related data breach.

**RCA Manager —** In charge of running the RCA process once the breach has been resolved.

**Security Team —** Ensure a quick, effective and orderly response to address weaknesses, events and security incidents.

## Procedure

# Security Measures

At a minimum, LoanPro Software uses industry-standard practices to protect our customers' information. Sensitive information is protected using the most secure methods that are reasonably available.

**Payment Profile Information —** LoanPro Software integrates with Secure Payments, a sister product, for the storage of payment information and payment processing. Secure Payments is PCI compliant and maintains a PCI-DSS Level 1 Attestation of Compliance (AOC). LoanPro is integrated according to PCI standards and never directly interacts with payment data.

**Data Access —** Data access is restricted by username and password authentication. LoanPro offers a multi-factor authentication option to further protect against unauthorized access.

Our personnel have access to client data only the client authorizes the access by providing a support code. Records are kept for each support transaction, which include information about the authorizing party and the authorized support representative. All data access by LoanPro Software personnel is restricted to within our offices through IP filtering. A record is kept of any changes made inside a client account by LoanPro personnel. Our hiring process includes a full background check for any new employee.

Employees are granted access to information on a need-to-know basis. Employees are regularly trained on our security and privacy practices to avoid security breaches through social engineering. Changes to privacy and security policies are also disseminated immediately through staff meetings and memoranda.

Employees who are authorized to access LoanPro databases must have their IP address whitelisted in order to do so. Access is only permitted through a secure shell (ssh). Permissions to hardware, environments, and data are configured per user, using the principle of least privilege. All servers are housed in Amazon data centers, which use the latest in firewall and other security technology.

Please see our Privacy Policy for more details on security measures.

# Incident Management

LoanPro will take the following steps in the event of a data breach: identify and close vulnerabilities, reinforce, report.

# In the Event of Data Breach

## Identify and Address Attack Points

If a security breach occurs, our first action will be to identify the vulnerability that allowed the breach to occur. Once a point of vulnerability is identified, our team will implement the necessary configuration, code, or controls to limit and/or close it. This includes the reinforcement of security protocols.

We have self-contained and external monitoring that continuously runs on our system. The primary responsibility to identify and address vulnerabilities falls on the on-call personnel in each department of our software division. Once a vulnerability has been identified, our entire software division is responsible for identifying and mitigating vulnerabilities. Departments responsibilities are as follows:

| Responsibility | Department(s) |
|---|---|
| Identify Vulnerability | Software Development, Development Operations, any LoanPro team member |
| Eliminate/Mitigate Vulnerability | Software Development, Development Operations |
| Test Vulnerability Fix | Software Development, Development Operations, Quality Assurance |

## Provide Notice

LoanPro Software will provide timely and appropriate notice to affected parties when there is a reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information from LoanPro Software. If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

1. Written notice will be provided to the affected individuals through the postal service unless the cost is excessive or insufficient contact information exists. The evaluation of cost and the determination that cost is excessive will be the decision of the LoanPro Software CTO and its legal counsel.

2. If written notice to the affected individuals is not reasonably possible, one or both of the following methods will be used to provide notice:
    1. Email
    2. Status Website

## Investigation

Security breach incidents are investigated fully after a fix for these events is put in place. Our internal and external monitoring keeps a detailed log of all events. Access to these logs is also tracked. Access to the logs is given to personnel on a least-privilege basis. The tracking of access to logs serves as the chain of custody documentation for evidence of a breach incident.

If the breach was the result of actions of LoanPro personnel, and the breach was not malicious in nature, a formal reprimand will be included in the individual's personnel file. If the same individual causes three breaches, without malicious intent, the individual’s employment or association with LoanPro will be terminated.

### Report to Authorities

Any attempt to circumvent data security is a violation of the SaaS Agreement. All attacks on LoanPro Software IT resources are infractions constituting misuse, vandalism or other criminal behavior. If the perpetrator of a security breach incident is identified, their information will be reported to law enforcement. When an incident is identified, it is the duty of any LoanPro employee or contractor to report the incident to his or her direct supervisor.

If a LoanPro client or affiliated party suspects or can confirm an information security breach, the breach should be reported to LoanPro Software, either via email to security@loanpro.io
or by calling (800) 559-4PRO. LoanPro Software will investigate each report. Once the incident is dealt with, the reporting party will be notified of its conclusion.

## Private Information

If the data in question is defined as personally identifiable and was not in an encrypted format, a public notification may be warranted. For the purposes of this policy data is defined as personally identifiable if it includes a name (first and last name or first initial and last name) in combination with any of the following: Social Security Number, Bank Account Number, Credit, or Debit Card Account number with security access, or password that would permit access to the account. Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address, are not considered private information for the purposes of this policy.

# Incident Types

## Unauthorized Physical Access

### Identification

Unauthorized Physical access incidents should be reported, as and when they occur or as early as possible, through appropriate management channels by . Any visitor who has access to more than our reception area is also required to wear a visitor's badge and provide identification. Even if unauthorized access is gained, LoanPro adheres to a clean-desk policy, which requires all sensitive information on paper, whiteboards, etc. to be destroyed before the end of each day.

Passwords are required for all LoanPro computers. System access and access to sensitive data also require authentication through passwords. On top of this, no customer data is stored directly on computers located on our premises but are housed in the cloud.

Additionally, our office entrances are monitored by cameras 24 hours a day. These cameras continuously record everyone entering the office. If motion is detected after hours, an alert is sent to key personnel informing them of what is happening. The cameras provide the option of a live stream that can be viewed remotely by our personnel. Recordings from these cameras are kept for 30 days.

### Recovery & Remediation

If unauthorized physical access is discovered, the Facilities Manager should escort unauthorized persons. Facilities Manager should perform an assessment of what data or hardware may have been removed from the premises. If hardware has been removed, law enforcement should be notified.

If hardware containing sensitive data has been removed, the data should be wiped remotely, if possible. The proper authorities will be notified and provided footage from our in-office cameras. An assessment will be made to determine if anything was stolen, or if information could otherwise have been taken.

Passwords for our software applications, company GSuite accounts, Monday.com, and Zendesk will be administratively reset to ensure they aren't used to gain unauthorized access to sensitive data.

### Notification

Because unauthorized physical access does not guarantee unauthorized access to information, notification about a physical breach will occur when unauthorized access to information has occurred or seems reasonably likely.

LoanPro Software will provide timely and appropriate notice to affected parties when there is a reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information from LoanPro Software. If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

1. Written notice will be provided to the affected individuals through the postal service, unless the cost is excessive or insufficient contact information exists. The evaluation of cost and the determination that cost is excessive will be the decision of the LoanPro Software CIO and its legal counsel.

2. If written notice to the affected individuals is not reasonably possible, one or both of the following methods will be used to provide notice:
    1. Email
    2. Status Website

## Information System Failure

### Identification

We employ Pingdom, NewRelic and SumoLogic to continuously monitor our system and check for system failure. Our systems continuously monitor available disk space, CPU, RAM and Network load. For more information on system monitoring, see Operating Procedures.

### Recovery & Remediation

When the system fails, our on-call developers are our method of first response. On-call programmers are available 24x7x365. Our on-call development staff is responsible to make adjustments or fixes as per the on-call process, where needed in order to bring the system back online with the support of other teams as needed.

If the hardware that serves our software to clients stops functioning, the CTO and the Software Support and Operations Manager should work with personnel from the Software Department to restore hardware or deploy new hardware to take its place.

Remediation and recovery may also require help from our business personnel to make sure the customer data is updated in a timely manner. Updates to customer data will always occur, but if there is a system outage, it can help if our system updates loans in a specific order.

### Notification

If customers will be affected by a system outage, they are always notified via email as soon as possible. This notification may occur in the middle of the night, which is why email is the preferred method of notification. These notifications usually contain information about the outage, what is being done to fix it, and what the customer can or should do, if anything, to help the situation. In addition or instead of this a message in the status page is added informing all customers according to LoanPro Status Page Process.

## Malware Activity

### Identification

Anti-virus scans are performed on a weekly basis on  workstations that connect to AWS instance. Anti-virus software is updated continuously to ensure that all the latest known malware is scanned for. The system also logs information on the following:

- Web Application Firewall
- IDS/IPS
- File Integrity Monitoring (FIM)
- Application Exceptions
- Web Server
- Database Server

These logs are reviewed daily through Sumo Logic.

### Recovery & Remediation

All LoanPro products employ backups of both the code base and customer data. If Malware is found on any of the workstations, the typical procedure is to eradicate the malicious software, assess the impacts, and recover the data or roll back the code if necessary.

If malware is discovered, its operation should be stopped. This may be done by removing the malware, stopping a process or Lambda function, or removing infected hardware from the server cluster.

The CTO will make decisions on how to address the immediate threat.

### Notification

If customer data is affected, or if the system will be down for any period of time, a post will be made to our status page and an email sent to the administrative user for affected customers according to LoanPro Status Page Process.

## Denial of Service

### Identification

We employ Pingdom, NewRelic and SumoLogic to continuously monitor our system and check for system failure. Our systems continuously monitor available disk space, CPU, RAM and Network load. For more information on system monitoring, see Operating Procedures.

### Recovery & Remediation

If the source of the denial of service is internal, the procedure is to fix the issue within our own system. If it’s an external attack, we will employ additional servers, where needed, while the source of the attack is identified and dealt with.

If the point of attack is easily identifiable, features or hardware may be taken offline to restore access to our software. If the point of attack is not immediately identifiable, new hardware may be deployed to restore service.

The CTO and the Software Support and Operations Manager will make decisions on how to address the immediate threat.

### Notification

Denial of service notifications will be made through our status page according to LoanPro Status Page Process.

## Incomplete or Inaccurate Data (Loss of Data Integrity)

### Identification

Our systems monitor file integrity and notify us of any issues. Logs of this monitoring can be queried to investigate any issues.

Identification of incomplete or inaccurate data may also be detected by our technical support staff or quality-assurance team, in the course of their daily duties.

### Recovery & Remediation

Depending on the root cause, data may be restored or corrected within the database. If the cause of missing or inaccurate data is not a code or database problem, accounts can be updated using data imports or our ETL system.

If the data in our database is corrupted and no longer correct, we may switch to a redundant database, or restore the data to the database from one of our saved backups.

The CTO and the Software Support and Operations Manager will make decisions on how to address the immediate threat.

### Notification

If we discover data problems, notification will be made to affected customers after the root cause of the loss of data integrity is discovered. Notification will most often occur via email.

## Breach of Confidentiality

### Identification

Our systems are continuously monitored for potential unauthorized access. If confidentiality has been breached and a LoanPro employee has allowed access to our systems by an outside party, suspicious activity will be detected based on the accessing IP address.

### Recovery & Remediation

If access to the user interface has been obtained by an unauthorized party, their activity in the software will be stamped with their user information. This makes it possible to identify and undo the changes they have made in the software.

If access has been gained to our codebase or databases, our logs will show the activity taken by unauthorized parties. This activity can then be undone using our data backups or code base backups.

If a LoanPro employee uses access to LoanPro software to breach the confidentiality of our clients or client’s customers, employee access credentials should be immediately changed. The CTO and the Software Support and Operations Manager will work with or other members of the software department to make sure this happens.

### Notification

If customer data has been stolen as a part of the breach, our customers will be notified with as much information as is available about what was taken.

## System Exploit

### Identification

System exploits are identified through weekly penetration testing. We run OWASP ZAP tests and document test results.

We also perform monthly testing to identify new vulnerabilities. If these vulnerabilities are introduced by a third party library, plugin, or application, they are thoroughly researched in order to understand and mitigate their effects.

Finally, we perform yearly internal penetration testing to identify vulnerabilities in our own system security.

### Recovery & Remediation

When a system exploit is found, the vulnerability is patched by our development and/or development operations team.

If an exploit is found in LoanPro software that may grant unauthorized software access, a patch should be deployed as soon as possible. The CTO and the Software Support and Operations Manager will be responsible to assess the vulnerability to see if anything more immediate can be done to mitigate the exploit.

### Notification

If a system exploit allowed possible access to customer data or affected customers in other ways, customers will be notified of the breach via email. The email should include a description of the exploit and measure that the customer can take to guard against its effects if any.

## Unauthorized Logical Access

### Identification

We perform a weekly review of user access and activity in the AWS Console and servers.

### Recovery & Remediation

If access has been gained to our codebase or databases, our logs will show the activity taken by unauthorized parties. If the activity was destructive, it can be undone using our data backups and code base backups. If sensitive information was taken, a report of the information will be made to the proper authorities.

Accounts and access are reviewed quarterly to ensure that access is not being granted where it shouldn’t and that inactive accounts are deleted.

If unauthorized access to LoanPro’s AWS hardware is obtained, affected access keys should be deleted, and all keys should be rotated. The CTO and the Software Support and Operations Manager will be responsible to make sure this happens.

### Notification

All potentially-affected customers will be notified of unauthorized access and its potential effects via email. The email will be sent to the administrative user for each LoanPro account.