LoanPro
Modern Credit Platform

Information Security Policy

Last Updated May 7th, 2024

Table of Contents

Purpose **5**

Security Policy Ownership and Responsibilities **6**

Management Roles and Responsibilities **6**

Assignment of Management Roles and Responsibilities for Security 6

Table 1 - Management Security Responsibilities 6

Policy **7**

Build and Maintain a Secure Network and Systems **7**

1 Install and Maintain a Firewall Configuration to Protect System Data 7

1.1 Establish and Implement Firewall/Router Configuration Documentation 7

1.2 Restrict Connections between Untrusted Network Segments and the Protected Data Environment 8

1.3 Prohibit Direct Public Access between the Internet and any System Component in the Protected Data Environment 8

1.4 Personal Firewall Required on Mobile Computers 9

1.5 Security Policies and Operational Procedures Documentation 9

2 Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters 9

2.1 Change Vendor Supplied Defaults 9

2.2 System Hardening and Standard Configuration of Devices 9

2.3 Use Secure Protocols for Non-Console Access 10

2.4 System Inventory 10

2.5 Security Policies and Operational Procedures Documentation 10
2.6 Shared Hosting Providers 10
Protect Stored Sensitive Data 10
3 Protect Stored Data 11
3.1 Retention and Disposal of Sensitive Credit Card Account Data 11
3.2 Store Sensitive Data in an Unreadable Format 11
3.3 Protection of Cryptographic Keys 11
3.4 Cryptographic Key Management Policies 12
3.5 Security Policies and Operational Procedures Documentation 12
4 Encrypt Transmission of Sensitive Data across Open, Public Networks 13
4.1 Transmission of Sensitive Data over Public Networks 13
4.2 Transmission of Sensitive Data via End User Messaging Technologies 13
4.3 Security Policies and Operational Procedures Documentation 13
Maintain a Vulnerability Management Program 13
5 Protect All Systems against Malware and Regularly Update Anti-virus Software or Programs 13
5.1 Deploy anti-virus software to protect systems 14
5.2 Ensure that all anti-virus mechanisms are current 14
5.3 Ensure that all anti-virus mechanisms are actively running 14
5.4 Security Policies and Operational Procedures Documentation 14
6 Develop and Maintain Secure Systems and Applications 14
6.1 Vulnerability risk ranking process 14
6.2 Regularly update systems and software 15
6.3 Secure Software Development 15
6.4 Change Control Procedures 15
6.5 Application Development 16
6.6 Protect Exposed Web Applications 16
6.7 Security Policies and Operational Procedures Documentation 17
7 Restrict Access to Sensitive Data by Business Need to Know 17
7.1 Restrict Access to Sensitive Data and Systems in the Protected Data Environment 17
7.2 Access Control Systems 17
7.3 Security Policies and Operational Procedures Documentation 18
8 Identify and Authenticate Access to System Components 18
8.1 Require Unique User IDs 18
8.2 User Authentication Methods 18
8.3 Multi-factor Authentication 19
8.4 Password Policy 19
8.5 Group or Shared Accounts and Passwords 19
8.6 Other Authentication Mechanisms 19
8.7 Access to Database with Sensitive data 19

8.8 Security Policies and Operational Procedures Documentation 19
9 Restrict Physical Access to Sensitive Data 19
9.2 Employees and Visitor Identification 20
9.3 Physical Access Control 20
9.4 Identify and Authorize Visitors 20
9.5 Physically Secure All Media 20
9.6 Media Distribution 21
9.7 Media Storage and Accessibility 21
9.8 Media Destruction Policies and Procedures 21
9.9 Security Policies and Operational Procedures Documentation 21
Regularly Monitor and Test Networks 21
10 Track and Monitor All Access to Network Resources and Sensitive Data 21
10.1 Monitor System Components within the Protected Data Network 22
10.2 Generation of Audit Trails 22
10.3 Audit Trail Entries 22
10.4 Network and System Time Sync 22
10.5 Audit Trail Security 22
10.6 Log Review 23
10.7 Audit Trail History 23
10.8 Internal Auditing of Security Controls 23
10.9 Security Policies and Operational Procedures Documentation 23
11 Regularly Test Security Systems and Processes 23
11.1 Rogue Wireless Network Detection 24
11.2 Vulnerability Assessment Scans 24
11.3 Penetration Testing 24
11.4 Intrusion Detection/Prevention 25
11.5 Change Detection 25
11.6 Security Policies and Operational Procedures Documentation 25
Maintain an Information Security Policy 25
12 Maintain a Security Policy that Addresses Information Security for All Personnel 26
12.1 Publish, Distribute, and Update the Information Security Policy 26
12.2 Implement a Risk-Assessment Process 26
12.3 Critical Technology Usage Policies 26
12.4 Assign Information Security Responsibilities 27
12.5 Assign Information Security Management 27
12.6 Security Awareness Program 27
12.7 Background Checks 27
12.8 Policies for Sharing Data with Service Providers 28
12.9 Additional Requirements for Service Providers 28
12.10 Incident Response Plan Policies 28

12.11 Internal Auditing of Critical Processes 29

Linked Documents and Templates 30

Table 2 – Security Process and Standards Documents Referenced by Policy 30

Compliance and Regulations 31

Version History 31

Purpose

This document contains the LoanPro Software information security policies. Detailed standards and processes that support this policy are described in associated standards and procedures documentation. This document is for internal use only and is not to be distributed.

To safeguard LoanPro Software‘s information technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Security Policy reflects LoanPro Software‘s commitment to comply with required standards governing the security of sensitive and confidential information.

LoanPro Software can minimize inappropriate exposures of confidential or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as Payment Card Industry Data Security Standard, SOC 1, SOC 2 and others), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses LoanPro Software‘s information technology resources. It is the responsibility of employees, contractors, business partners, and agents of LoanPro Software. Each should become familiar with this policy's provisions and the importance of adhering to it when using LoanPro Software‘s computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the Security department.

The primary purpose of this security policy is to establish rules to ensure the protection of confidential or sensitive information and to ensure protection of LoanPro Software‘s information technology resources. The policy assigns responsibility and provides guidelines to protect LoanPro Software‘s systems and data against misuse or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to LoanPro Software‘s data network. It may apply to users of information services operated or administered by LoanPro Software (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with LoanPro Software are subject to these same definitions and rules when they are using LoanPro Software‘s information technology resources.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks or data.

All cardholder data as defined by the PCI DSS guidelines are stored & tokenized outside of LoanPro Software by Secure Payments who holds a PCI DSS Level 1 AOC, thereby reducing the scope of LoanPro to fall outside of PCI guidelines.

This Information Security Policy complies with ISO 27001 requirements and is aligned to the security objectives described in the Information Security Management System (ISMS), these objectives are:

Please contact us to get the full version of the document.