Hosted PowerLender® Security FAQ

Hosted PowerLender Security Overview

This document provides a brief overview of the methods used to secure data within the Hosted PowerLender environment. Hosted PowerLender is a fully functional online version of our PowerLender client/server desktop LOS.

With Hosted PowerLender, we maintain the LOS and the accompanying hardware and computing infrastructure. Hosted PowerLender is accessed from lender laptop and desktop PCs, with the software running on ASC-managed servers in a secure data center. With only minor differences, the user experience is the same as if PowerLender was installed on in-house PCs.

Lending data resides within our secure data center. Hosted PowerLender is designed to accommodate Gramm/Leach/Bliley regulations, which concern the handling and access of private information. Much of the responsibility for compliance is now transferred from the lender to Associated Software Consultants, Inc. (ASC).

How are Site Log In and Loan Data Entry Secured?

Data transfer between the client and the Hosted PowerLender server is secured using a combination of industry-approved security technologies:

- Password-controlled system entry
- Thawte-issued Digital Certificate
- Secure Sockets Layer (SSL) protocol for data encryption, server authentication and message integrity for an Internet connection.

SSL provides a “security handshake” that initiates the connection. This handshake results in the client and server agreeing on the level of security to employ and authenticates the connection. The Hosted PowerLender server uses a minimum of 128-bit encryption and automatically upgrades to 256-bit encryption in browsers that support it. This is the highest level of commercially available security.

Encryption Methods, Certificates and Ciphers Used:

<u>HTTPS:</u>

SHA256 RSA 4096 Bit Server Certificate

TLS 1.2

Ciphers supported:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

<u>SSH:</u>

Key Exchange: curve25519-sha256, diffie-hellman-group-exchange-sha256

Client Authentication: Ed25519 with SHA512, RSA with SHA1 (4096 bit)

Symmetric Ciphers:

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

Message Authentication Codes:

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-ripemd160-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256
- hmac-ripemd160
- umac-128@openssh.com

Log in and Passwords Security

Hosted PowerLender requires that passwords pass minimum "security strength" tests and also requires that passwords be changed every 90 days. Hosted PowerLender automatically locks out any user account after a predetermined number of consecutive failed login attempts. Hosted PowerLender monitors all connections, blocking any internet address that attempts to login with an invalid username too many consecutive times. Hosted PowerLender can also restrict access within specific time periods as determined by the lender. It is still the responsibility of the user to keep usernames and passwords confidential and secure. ASC must be informed immediately when a user is no longer allowed access to the system so that we can inactive their password.

Firewall & Intrusion Detection System (IDS)

Before reaching the Hosted PowerLender server, all logins and data entry to the server are filtered through a hardware firewall, which in turn opens only when necessary to process acceptable data requests. Lenders can also restrict Hosted PowerLender access to only known Internet addresses to further enhance security.

Hosted PowerLender's security architecture responds to network abuse before systems are compromised. ASC's network intrusion detection system (IDS) runs 24 hours a day, 7 days a week. The IDS hardware monitors all traffic on each Hosted PowerLender network segment, looking for attack signatures-evidence of an intrusion or denial-of-service (DOS) attack.

Site Penetration Test

ASC employs authorized third-party companies to perform automated and individual penetration tests of the Hosted PowerLender site to check network security and to safeguard the system from new exploits and vulnerabilities.

Master Host Agreement

The dedicated physical server for Hosted PowerLender is provided and housed by a third-party secure data center, which guarantees appropriate technical and organizational measures to protect your dedicated equipment and data from accidental or unlawful destruction, alteration, unauthorized disclosure or unauthorized access. Both ASC and the data center restrict access to employees who have agreed in writing not to access the equipment or your stored data.

SSAE 18 SOC2 Type II Certification

Successful completion of the SSAE 18 Audit indicates that ASC processes, procedures and controls have been formally evaluated and tested by an independent accounting and auditing firm. The examination includes ASC's controls related to security monitoring, change management, service delivery, support services, backup and environmental controls, logical and physical access as well as the accuracy of the security, availability, integrity, confidentiality and privacy controls for ASC's hosted systems.

A copy of our SSAE 18 SOC2 Type II Report is available upon request.