SigningOrder

powered by NotaryLoop

Security Report

February 16, 2022

SigningOrder uses strong security across all levels of the SigningOrder.com platform. Security protocols are detailed at every level in this report.

Registrar

SigningOrder.com is registered at GoDaddy.com. We make full use of DNSSEC security to protect users from forged DNS data, which would result in a user being sent to a malicious site. DNSSEC provides a layer of trust on top of the DNS "phonebook" of the internet, allowing a user's browser to cryptographically verify the results of the DNS lookup.

DNS

SigningOrder uses Cloudflare as our DNS provider. Cloudflare provides real time threat detection and presents users with a challenge page when using a non-standard browser or is sending suspicious traffic. Less than .001% of traffic to our system is detected as a threat by Cloudflare, a very low number. Cloudflare also provides SigningOrder.com with a reverse proxy CDN giving faster site performance and increased security to users.

HTTPS

When traffic leaves the browser it is encrypted using HTTPS security. HTTPS is the standard for sites that need their site's data encrypted between the user and the servers. Our HTTPS scheme is configured to be as secure as possible, but will gracefully degrade to the level of security the user's browser can support. In order of priority, our system will deliver security certificate information in the following order.

1) SHA256 ECDSA (most secure, modern browsers)
2) SHA256 (very secure, most browsers)
3) SHA1 RSA (secure, legacy browsers)

HTTPS protects user data in motion between the browser and our platform, making it impossible for any unknown third party to see the data en route. Once a user's data reaches our system, is it decrypted for interpretation by SigningOrder.com.

Data Center Security

Our servers are hosted on enterprise grade infrastructure provided by AWS in a secure environment. Physical access to the servers is restricted to only authorized engineers and protected by biometric authentication and round-the-clock surveillance.

Server Access

Server access is restricted using SSH private/public key pair authentication, and the only people authorized to access it are four of SigningOrder's engineers.

File Security

All uploaded files, including all order-related documents, W9, and E&O documents are stored in an encrypted format in a secure AWS S3 buckets. Before a file is stored in AWS S3, the uploaded files are encrypted using AES-128 bit CBC encryption. This assures the files are protected against any unauthorized access from independent AWS techs, or others.

User Access

All access to the SigningOrder.com platform is protected by username and password authentication. Multi-Factor Authentication is available to be turned on and is required for all Administrators. Passwords are stored in a secure one-way "salted and peppered" hashed format. If a password is lost, it must be reset, as there is no way to recover it. Twelve administrators have access to "impersonate" a user to assist with supporting users through any problems they may have.

Database Security

The SigningOrder.com database is protected from external access by anyone. Only SigningOrder.com can connect to the database directly. The database servers exist in the same data center as the web servers, and traffic between them is secured internally.

Backup Policy

SigningOrder maintains a complete backup of the system daily for the past 14 days. After 14 days the backup is removed and replaced with the most recent backup. All backups are stored in a secure location in an encrypted format. Backups of file uploads are maintained by AWS.

Email Security

Emails are protected by a published SPF, DKIM, and DMARC policy. SPF and DKIM ensure emails users receive from SigningOrder.com are ACTUALLY FROM SigningOrder.com. DMARC provides a policy for how email recipients should handle unauthorized senders pretending to be SigningOrder.com. DMARC also provides a weekly report of potentially malicious emails. SigningOrder reviews the report and takes action to mitigate any malicious senders.

Note: this does not apply when sending emails through your own email SMTP service.

Transparency

SigningOrder will notify all affected users of any attack, breach of security, or loss of data detected within our system immediately. As of February 16, 2022, SigningOrder or its parent companies have never received a National Security Letter, an order under the Foreign Intelligence Surveillance Act, or any other classified request for user information. If we ever receive such a request, we would seek to let the public know it existed.

Updates

SigningOrder will update this security report yearly, unless a significant change or event happens that requires this document to be updated. We will not issue an updated version of this document more than once per quarter.

Revisions:

2022-02-16

- File Storage moved from Rackspace to AWS.
- Three engineers added to signing order development team.

2020-12-06

- Server moved from Rackspace to AWS.
- Three engineers added to signing order development team.
- Database moved from Rackspace to AWS and no longer a cluster.

2020-12-06

- Server moved from Rackspace to AWS.
- Three engineers added to signing order development team.
- Database moved from Rackspace to AWS and no longer a cluster.

2018-12-02

- Two more individuals have been given increased administrator privileges within the SigningOrder platform, allowing them to impersonate users.
- One engineer with server access has been removed, and two new engineers have been added.

2017-10-05

- One additional engineer has access to SigningOrder’s servers.
- Files are now stored on Rackspace CloudFiles instead of being distributed between web nodes.
    - Files are encrypted individually before being uploaded to Rackspace CloudFiles.
- The Database has been migrated to an HA Cluster.
- Added Transparency Section
- Added Update Policy

2016-10-05

- Original Document Published.