SECURITY & COMPLIANCE OVERVIEW

For FaxFinder Cloud, security is a top-priority. The FaxFinder Cloud service operates in Equinix datacenters which are SOC 2 compliant and provide customers with a HIPAA and PCI compliant fax solution. In addition to HTTPS connections, we leverage multiple defense-in-depth strategies provided by patented etherFAX technology including two-factor authentication, end-to-end encryption, and in-network routing to guarantee that faxes remain protected.

FaxFinder's core business is providing reliable and cost effective fax server solutions than span from on-premise deployments and hybrid fax servers to a fully cloud based service. FaxFinder servers are critical to the financial, insurance and healthcare industries and we have been doing this for more than 15 years.

PHYSICAL SECURITY

All Equinix data centers are the 'gold standard' for security and reliability. Their qualifications earn them all of the required certifications for a world class datacenter. For more information visit https://www.equinix.com/services/data-centers-colocation/standards-compliance/#/

The data centers are staffed with 24-hour security officers. Visitors are screened upon entry to verify identity and escorted to appropriate locations. Access history is recorded for audit. Only authorized and essential personnel have access to the FaxFinder Cloud servers and are the only ones who can manage the equipment.

All personnel are subjected to criminal background checks prior to employment and are performed at the unspecified intervals at the discretion of management.

NETWORK SECURITY

Network security protects data from both intentional and unintentional breaches that could occur and since FaxFinder Cloud handles sensitive data daily, the network is designed to protect that information.

- Current and up-to-date firewalls
- DMZs or logical components
- Intrusion Detection and Logging
- PCI-compliant levels of SSL and TLS security (AES 256 bit encryption)
- SSL encryption for internal communication between servers / data centers
- Frequent vulnerability assessments performed on internal and production cloud networks
- Frequent security scans performed on internal and cloud fax networks
- Frequent penetration tests performed on internal and cloud fax networks
- Ongoing process of updating and patching the cloud ax network
- Documented procedures describing the control processes over network security and administration processes
- Network and host intrusion detection and prevention (IDS / IPS)
- Systematic auditing and review of logged data including, but not limited to:
    - Invalid access attempts
    - Access to identification, authentication and authorization mechanisms
    - Access attempts to the database
    - Account changes
    - All successful and unsuccessful logins
- Formal alerting and response process used in the event the Intrusion Detection System detects a suspicious event or exceeds normal thresholds or our environment.

HIPAA COMPLIANCE

While there is no federal agency that can "certify" a solution as such, FaxFinder adheres to the following published HIPAA guidelines:

ADMINISTRATIVE SAFEGUARDS

Policies and procedures to comply with HIPAA by maintaining security measures to protect electronic information and manage the conduct of covered entity's employees.

- Third party vendors must comply with HIPAA requirements, typically through contracts stating vendor will meet the same data protection requirements that apply to the covered entity (Business Associate Agreement — BAA)

PHYSICAL SAFEGUARDS

Controlling physical access to protect against inappropriate access to protected data.

TECHNICAL SAFEGUARDS

Controlling access to computer systems and protecting communications containing PHI transmitted electronically over open networks from being intercepted by anyone other the intended recipient.

PCI DSS COMPLIANCE

FaxFinder Cloud meets the following PCI security requirements (from the PCI Security Standards Council):

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Identify and authenticate access to system components

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security for all personnel

APPLICATION SECURITY

As data breaches and cybercrime become increasingly common, organizations are in need of a way to send and store documents in a secure method now more than ever. Malicious attacks on sensitive information aren't the only threat to data, however. Often times, important information is saved on physical devices that are lost, stolen or handled inappropriately, resulting in compromised data.

FaxFinder Cloud uses the same underlying security technology used by online banking. Built on the Microsoft.net platform and leveraging Microsoft SQL server, FaxFinder uses AES 256 encryption on all faxes at rest within the server. FaxFinder takes care to ensure any info in the system is properly secured at all times.

- All faxes are encrypted in-transit (within FaxFinder's network and in the communication with etherFAX) and is also encrypted while at-rest.
- Utilization of Secure Socket Layer (SSL) encryption for all web traffic (SSL v2/v8 are disabled or security best practices) and Transport Layer Security (TLS 1.2) for all email communication (opportunistic or enforced).
- AES 256-bit encryption support.
- Strictly controlled users and administrator authentication on platform.
- Enforced minimum password standards or length, complexity, and characters.
- Controls in place to protect the authenticity to communications sessions.
- Multiple options or customers to specify the duration of fax document storage.

REDUNDANCY & DISASTER RECOVERY

Redundant infrastructure and Enterprise Class Servers provides for 99.99% uptime. Significant investments in Enterprises Class servers that deliver exceptional performance. High speed hardware maximizes output, production and reliability. Dual power supplies prevent system downtime in the event of any power component failure. With out-of-band management via IPMI our technicians can respond immediately.

The FaxFinder software, running in multiple datacenters, has no single point of failure. The 'mothership' of the application is the Microsoft SQL server, which runs on multiple hardware instances and is mirrored. FaxFinder processes are also installed on redundant hardware instances, which eliminates any single point of failure and ensures no single 'bottle-neck' for critical processes.

Equinix datacenters have redundant Internet connections, power and generators, along with other measures to insure no single point of failure that could take the datacenter down. During the Hurricane Sandy superstorm, the Equinix facilities that were in the path of the storm never experienced an outage.

TRANSPORT SECURITY

FaxFinder Cloud leverages etherFAX for transport of all inbound and out faxes generated by the server. Security is a clear differentiator when comparing other outsourced fax services to etherFAX. etherFAX incorporate a multi-level encryption/security system known as a "defense-in-depth" approach. It is a layering tactic, conceived by the National Security Agency (NSA), as a comprehensive approach to information and electronic security.

etherFAX starts with a secure communication channel over HTTPS that secures the "pipe" between the etherFAX client/customer and the back-end services hosted by etherFAX. Once a secure channel has been established, each customer is authenticated using his or her account, user name, and password. Lastly, the etherFAX web service model further encrypts and protects the communication on a "message level" even though the HTTPS channel is already arguably secure.

FAXFINDER WRITTEN INFORMATION SECURITY PROGRAM

1.0 Policy Statement

The FaxFinder Written Information Security Program ("WISP") is intended as a set of comprehensive guidelines and policies designed to safeguard all confidential and restricted data maintained within FaxFinder's various hosted fax servers, and to comply with applicable laws and regulations on the protection of data on our subscribers, fax images stored on the FaxFinder server and details on fax transmissions.

2.0 Overview & Purpose

The WISP was implemented to comply with regulations and policies related to the Payment Card Industry (PCI) and HIPAA. FaxFinder is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who use the FaxFinder software for sending and receiving faxes.

The purposes of this document are to:

- Establish a comprehensive information security program for FaxFinder staff, with policies designed to safeguard sensitive data that is maintained on the FaxFinder servers in the cloud.
- Establish employee responsibilities in safeguarding sensitive data; and
- Establish administrative, technical and physical safeguards to ensure the security of sensitive data.

3.0 Scope

This Program applies to all FaxFinder employees, hired consultants and interns. The data covered by this Program includes any faxes stored and accessed on our cloud servers.

3.1 Definitions

For the purposes of this document, data refers to transactional information about fax transmissions, fax images, User accounts, including subscriber's email addresses.

4.0 Polices for Safeguarding Sensitive Data

To protect sensitive data the following policies and procedures have been developed that relate to access, retention and purging of fax records and images.

Access & Storage

- Only those employees or authorized third parties requiring access to sensitive data in the regular course of their duties are granted access to servers containing this data.
- All electronic records are maintained in an encrypted SQL database. All fax images on the FaxFinder server are encrypted with a 256 AES symmetric algorithm.
- The hosted FaxFinder servers are located in Equinix datacenters that provide 7x24 monitoring and are Type 2 - SOC 1 and SOC 2 SSAE 18 certified.
- Upon termination of employment or relationship with FaxFinder, electronic and physical access to documents, systems or other network resources containing sensitive data is immediately terminated.

4.1 Policies for Safeguarding Sensitive Data

- Access to the FaxFinder cloud servers is restricted to staff who have a legitimate business need for access to servers.

4.2 Password Requirements

In order to protect sensitive data, all employees must use unique passwords following these guidelines:

- Has at least 8 characters
- Contains a combination of at least three of the four character types: uppercase and lowercase letters, numbers, and special characters (e.g., @ $ # !)
- Does not contain repeated characters or a sequence of keyboard letters (e.g., qwerty, 12345, or yyy99)
- Does not contain any part of the user's name, username, birthday, or social security or those of friends and family (e.g., Jill1030)

FAXFINDER WISP (CONTINUED)

4.3 Computer System Safeguards

FaxFinder support staff monitor and assess safeguards on an ongoing basis to determine when patches and updates are required. FaxFinder has implemented the following to combat external risk and secure the network and systems containing sensitive data:

- Secure user authentication protocols:
    - Unique passwords are required for all user accounts; each employee receives an individual user account.
    - Server accounts are locked after multiple unsuccessful password attempts.
    - Computer access passwords are disabled upon an employee's termination.
    - User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures:
    - Access to specific files or databases containing sensitive data is limited to those employees who require such access in the normal course of their duties.
- FaxFinder support staff perform regular internal network security audits to all server and computer system logs to discover to the extent reasonably feasible possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of data.
- Operating system patches and security updates are installed to all servers on a regular basis.
- Antivirus and anti-malware software is installed and kept updated on all workstations.

4.4 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of sensitive data, or of a breach or attempted breach of the information safeguards adopted under this Program, is reported immediately to the CEO. The Incident Team will document all breaches and subsequent responsive actions taken.

5.0 Enforcement

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential or Restricted data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

6.0 Effective Date

This Written Information Security Program was implemented January 1, 2019.