fileinvite

DOCUMENT COLLECTION ON AUTOPILOT

Security & Privacy

20th October 2019

Commercial and in Confidence

Table of Contents

1. **Introduction** **3**

2. **Infrastructure & Encryption** **4**

SECURE ARCHITECTURE 4

SERVER HARDENING 4

DATA CENTRES 4

ENCRYPTION IN TRANSIT 4

ENCRYPTION AT REST 4

DOCUMENT STORAGE 5

3. **Operational Security** **5**

CODING AND TESTING METHODS 5

SECURE CODING PRACTICES 5

WORKSTATION SECURITY 5

PASSWORD MANAGEMENT 5

4. **Access Control** **6**

ACCESSIBILITY 6

AUTHENTICATION 6

LOGGING, AND ALERTING 6

DISASTER RECOVERY 6

5. **External Validation** **6**

SECURITY COMPLIANCE AUDITS 6

PENETRATION TESTING 6

MONITORING AND SYSTEM ALERTS 7

6. **Data & Privacy** **7**

TREATMENT OF INFORMATION 7

DISCLOSURE 7

OWNERSHIP OF DATA 7

DATA RETENTION AND DISPOSAL 7

SUPPLIER MANAGEMENT 8

RESPONDING TO INCIDENTS 8

7. **More Information** **8**

AUDITS BY CUSTOMERS 8

QUESTIONS 8

8. **Company Details** **9**

1. Introduction

Keeping it under wraps

The lengths we go to keep client data secure

FileInvite is a cloud-based, automated platform for collecting information, files and signed documents from your customers.

Document collection is all about using online tools to help manage client information. These alternatives to email and local data storage streamline the way you collect, store and share documents. They reduce handling errors, keep your data safe and compliant, and improve your overall productivity.

And in this world, security is paramount.

Did you know?

91% of cyber attacks start via a phishing email. Your company email is undoubtedly one of the weak points in cyber security, and having sensitive documents contained in your employee's email inboxes is a huge risk and potential for data breach. FileInvite moves your document collection out of the inbox to an independent safe and secure platform that protects your data and keeps your reputation intact.

Our product security team works hard to help ensure that the FileInvite portal remains a safe and reliable place for client data. Multiple types of security practices and technologies are deployed to help ensure consistency and integrity of the platform.

2. Infrastructure & Encryption

SECURE ARCHITECTURE

FileInvite at its core was designed with security in mind. The architecture is based on best practice development principles separating file and associated meta data, and keeping environment data separate and encrypted in transit and at rest.

SERVER HARDENING

FileInvite divides its systems into separate environments to better protect sensitive data. Systems supporting testing and development activities are hosted in a separate environment from systems supporting our production infrastructure. All servers within our production fleet are hardened (e.g. disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment.

Network access to our production environment from open, public networks (the Internet) is restricted, with only a small number of production servers accessible from the Internet. Only those network protocols essential for delivery of FileInvite's service to its users are open at our perimeter. Additionally, for host-based intrusion detection and prevention activities, FileInvite logs, monitors, and audits system calls and has alerting in place for system calls that indicate a potential intrusion.

DATA CENTRES

FileInvite is deployed on the Amazon AWS global backbone infrastructure. We utilise data centres which are at the forefront of technology, using innovative architectural and engineering approaches, and the latest in cloud technologies and infrastructure design.

Physical access is strictly controlled both on the perimeter and the construction of entry points by professional security staff using video surveillance, intrusion detection systems, biometric analysis, and other electronic means.

ENCRYPTION IN TRANSIT

Our in-transit encryption ensures that messaging, data, and file transfers are all secured while in transit to the latest global standards with similar technology as used in many banking platforms.

All http calls are encrypted with HTTPS SSL at transport layer, and API data can also be optionally be encrypted at message layer by using our inbuilt MLS encryption of API payload.

FileInvite supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols at a minimum, AES256 encryption, and one way SHA2 where possible.

ENCRYPTION AT REST

Stored data such as relational databases, file stores and database backups are encrypted using multiple types of encryption. FileInvite employs both container and object encryption for both files and database entries.

Each customer’s data is hosted in our shared infrastructure and logically separated from other customers’ data. We use a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested.

DOCUMENT STORAGE

FileInvite stores the documents that you request in the Amazon S3 facility. The original files and the customer data are split, isolated and placed in different locations and encrypted at rest in addition to a complex management by encryption keys.

Access to these files is only via authenticated calls through the FileInvite file proxy, and using time expiry signed URLs.

3. Operational Security

CODING AND TESTING METHODS

We leverage best practice programming techniques applicable to the software industry wherever possible. All our products and solutions follow a quality assurance path through our software development lifecycle, and our teams follow OWASP guidelines, code reviews, and regular security awareness training so that our application meets stringent safety and security standards.

SECURE CODING PRACTICES

The security of our solution is evaluated by the development team through a combination of secure coding practices, peer code reviews, and automated tools such as code sniffers. Vulnerability tests follow OWASP principles and include the use of commonly known web application security tool kits and scanners to identify application vulnerabilities before they are released into production. The development team has regular sessions for security awareness training to improve coding security and standards.

WORKSTATION SECURITY

All workstations issued to FileInvite personnel are configured to our standards for security. These standards require all workstations to be properly configured, updated, and be tracked and monitored by FileInvite’s endpoint management solutions. The default configuration sets up workstations to encrypt stored data, have strong passwords, and lock when idle. Workstations run up-to-date monitoring software to report potential malware, unauthorized software, and mobile storage devices.

PASSWORD MANAGEMENT

FileInvite requires personnel to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks. Password complexity and reuse is monitored through centralised password control systems.

4. Access Control

ACCESSIBILITY

To minimize the risk of data exposure, FileInvite adheres to the principles of least privilege and role-based permissions when providing access. Staff are authorized to access only the data that they reasonably must handle in order to carry out their roles. All production access is reviewed at least quarterly.

AUTHENTICATION

To further reduce the risk of unauthorized access to data, FileInvite employs multi-factor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data. Where possible and appropriate, FileInvite uses private keys for authentication, in addition to the previously mentioned multi-factor authentication on a separate device.

LOGGING, AND ALERTING

FileInvite monitors servers, workstations and endpoints to retain and analyse a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on servers in our production network are logged and retained. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel.

DISASTER RECOVERY

FileInvite utilizes services deployed by its hosting provider to distribute production operations across multiple separate physical locations and availability zones. Enterprise customers optionally may select a specific geographic data region where their data is stored from the available server locations.

FileInvite has thorough and externally audited plans for both Business Continuity and Disaster Recovery processes. Our BCDR plan includes full support for disaster management and full backup and recovery procedure to ensure a minimum of disruption and continued service in the event of a full system failure event. BCDR plans are tested at least 6 monthly to ensure RTO and RPO times are achieved at a minimum.

5. External Validation

SECURITY COMPLIANCE AUDITS

FileInvite is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and our internal risk and compliance team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner through a structured risk management procedure.

PENETRATION TESTING

In addition to our compliance audits, FileInvite engages independent 3rd party entities to conduct application-level and infrastructure-level penetration tests at least 6 monthly, and on major code releases. Testing is done through a mixture of grey box methodology and with source code analysis, in conjunction with both automated and manual detection tools.

Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner. Customers may receive assurance statements of these activities containing high level detail by requesting them from their account executive.

MONITORING AND SYSTEM ALERTS

Our production application and underlying infrastructure components are monitored 24/7 by dedicated monitoring systems. Any critical alerts generated by these systems are sent to our technical team for quick resolution. We target 99.9% online accessibility for customers on our enterprise cloud plans. All our systems are mirrored on duplicate servers for failsafe and maintenance purposes.

6. Data & Privacy

TREATMENT OF INFORMATION

All information submitted to FileInvite is deemed as private and treated as such with the same measures and standards of security whether it was public or non-public. We have security measures at both software and operational level meaning that processes and policies are in place both electronically within the platform, and at operational staff level with regards to the handling of customer information. FileInvite is governed by the principles of the New Zealand Privacy Act 1993.

DISCLOSURE

Private information will never be voluntarily disclosed to 3rd parties unless required to do so by law, or as outlined under our standard Terms of service and Privacy Policy. FileInvite treatment of private information is done in accordance with the terms of our Privacy Policy and our General Terms which can both be found at

PRIVACY POLICY:	https://www.fileinvite.com/privacy
GENERAL TERMS:	https://www.fileinvite.com/terms

OWNERSHIP OF DATA

Personal information, data, and files uploaded to FileInvite using our services remains the property of the original owner. FileInvite will not use this data for our own purposes.

DATA RETENTION AND DISPOSAL

Customer data is removed upon deletion by the end user or upon expiration of data retention as configured by the customer administrator. FileInvite hard deletes information from production system backups which are destroyed after 7 days rotation.

Our hosting providers are responsible for ensuring removal of data from disks is performed in a responsible manner before they are repurposed.

SUPPLIER MANAGEMENT

FileInvite outsources some of its services. Where those organizations may impact the security of FileInvite's production environment, we take appropriate steps to ensure our security posture is maintained. We do this by ensuring service organizations selected protect customer confidentiality through established and maintained certifications against one or more international standard such as SOC Type II, ISO 27001, and PCI as a minimum.

RESPONDING TO INCIDENTS

FileInvite has established policies and procedures for responding to potential security incidents. All security incident procedure is managed under the protocol set out by our internal Security Incident Policy and handled by our incident response team which classifies them based on severity. In the event of an incident, affected customers will be informed as necessary under an established incident communication plan, typically through email communications. Based on incident classification and severity under the plan, any required notifications will be given within 72 hours following confirmation of a notifiable data breach. Incident response procedures are tested and updated at least annually.

7. More Information

AUDITS BY CUSTOMERS

Our customers are welcome to perform either security controls assessments or penetration testing on FileInvite's environment subject to written permission by FileInvite prior to any testing. Please contact FileInvite to learn about options for scheduling either of these activities.

QUESTIONS

Every organization deserves and expects their data to be secure and confidential. Safeguarding this data is a fundamental responsibility, and we continue to work hard to maintain your trust. Please contact FileInvite if you have any questions or concerns.

8. Company Details

Trading Name: **FileInvite**

Company Name: FileInvite Limited

NZNBN: 9429030240827

CEO: James Sampson

Chairman: Garth Hinton

Directors:
Garth Hinton
James Sampson
Jiwa Nadan

Physical Address:
669 Great South Road
Penrose
Auckland
New Zealand

Postal Address:
PO Box 12018
Penrose
Auckland 1642
New Zealand

Business Hours:
9am – 5:30pm
Mon – Fri NZST

Website: www.fileinvite.com

Email: info@fileinvite.com

Phone Numbers:

United States:	+1 (628) 201-0083	San Francisco
Canada:	+1 (647) 495-8901	Toronto
Australia:	+61 (2) 9042-2679	Sydney
New Zealand:	+64 (9) 972-3040	Auckland