TransferHub

Security FAQ

Regulatory Compliance and Independent Validation

Do you conduct independent audits for reviewing the efficiency and effectiveness of implemented security controls to ensure compliance obligations?

Yes. TransferHub maintains a full-time compliance program to meet its SLA and regulatory requirements. TransferHub complies with the AICPA SOC 2 Trust Services Criteria for Security, Availability and Confidentiality. An independent CPA firm conducts audits annually.

Do you conduct independent audits for reviewing the efficiency and effectiveness of implemented security controls to ensure compliance obligations?

Yes. TransferHub maintains a full-time compliance program to meet its SLA and regulatory requirements.

TransferHub complies with the AICPA SOC 2 Trust Services Criteria for Security, Availability and Confidentiality.

Do you have the capability to continuously monitor and report on the compliance of your infrastructure against your information security baselines?

Yes. TransferHub performs internal audits and continuous monitoring throughout the year to maintain compliance.

Do you make third-party audit or certification reports available?

Yes. By request only.

Do you conduct penetration tests of your cloud infrastructure?

Yes. We partner with an independent third-party to conduct both network and application penetration tests of the TransferHub cloud service infrastructure at least annually.

Do you conduct any third-party reviews of your platform or services?

Yes. TransferHub partners with Amazon Web Services, to provide a reliable and secure service. This includes periodically performing an AWS Well-Architected Framework review to ensure we are following best practices and leveraging the infrastructure's security offerings to their fullest.

Risk Management

Does TransferHub maintain a Risk Management program?

Yes. Risk assessments of TransferHub and its service providers are performed to identify and categorize risks, understand their cause and potential impact, and outline mitigation steps that reduce their impact or severity.

How frequently does TransferHub conduct risk assessment?

Assessments are conducted annually, as well as before any major change to the service, and are reviewed by senior management to ensure risks are both understood and accepted.

Personnel & Operations

Are TransferHub employees subject to background checks?

Yes. TransferHub employees undergo reference and background checks before being granted access to any customer information or the Production Environment.

Are TransferHub employees subject to employment agreements and mandatory training?

Yes. All employees are subject to a perpetual Non-Disclosure Agreement to ensure confidentiality.

TransferHub employees receive mandatory information security and privacy training upon hire and at least once per year thereafter. The content includes (but is not limited to) company and policy requirements, security risks, and user responsibilities.

Availability & Infrastructure

Where is the TransferHub service hosted?

Production systems for processing and storing customer data are hosted on Amazon Web Services (AWS).

Does your organization have a plan or framework for business continuity management or disaster recovery management?

Yes. TransferHub maintains a framework for business continuity. This includes plans for both Disaster Recovery and Incident Management.

How does TransferHub manage backups?

TransferHub performs geo-redundant encrypted backups daily. Backup verification and restoration are included in the automated process. Customer data backups are securely maintained for thirty days.

Does TransferHub support a High Availability solution?

If you require a highly available data center, please contact TransferHub regarding Amazon availability zones.

What is TransferHub's commitment to service uptime?

TransferHub maintains a 99.9% target for uptime and service availability. Our SLA commitments including RTO and RPO may be accessed via the customer portal.

Incident Management

How do I contact TransferHub regarding a security related issue?

If you believe you have detected a security event or potential vulnerability, please let us know by emailing us at security@TransferHub.io.

Does TransferHub maintain an Incident Response Team?

Yes. TransferHub maintains a team to monitor security and availability issues and, if needed, implement our incident response plan.

What is TransferHub's policy regarding breach notification?

TransferHub complies with the General Data Protection Regulation (GDPR).

Data Protection

Does TransferHub ever share my data?

No. TransferHub does not share customer data with any third party.

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Yes. Replication or use of production data in a non-production environment is strictly prohibited. Access to Production Systems is restricted to the TransferHub Operations team and the principles of least privilege and need to know are implemented and regularly reviewed.

Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?

Yes. All production data is segmented and only accessible to authenticated users who are authorized to access the data.

Do you encrypt my data at rest (on disk/storage) within your environment?

Yes. We leverage AWS KMS and encrypt production data at rest using AES-256, including files, databases and backups.

Do you encrypt my data in transit?

Yes. Data is encrypted in transit over HTTPS using TLS 1.2 or greater.

Identity and Access Management

Do I have granular control over who may access my data?

Yes. As an organization, you have control over whom you invite to access your data and to what degree. Production databases use Row Level Security (RLS) to allow you to specify and enforce granular per-object access controls within the TransferHub service.

How does TransferHub enforce identity controls within the service?

By default, production systems require strong/complex passwords and Multi-factor Authentication (MFA).

Can I use my own Identity Provider?

Yes. TransferHub supports integration with a customer specified IdP.

Platform and Network Security

Does TransferHub support Three Tier Architecture?

Yes. Production database servers are protected and isolated on a Virtual Private Cloud, separate from the web and Internet accessible servers.

Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?

Production systems are protected by network firewall controls to restrict access as well as Web Application Firewall (WAF) controls to protect against common web exploits.

Are production servers hardened to provide only necessary ports, protocols, and services to meet business needs?

Yes. Production servers are built from a standard template as a baseline, with non-essential accounts and applications removed or disabled.

Are production servers scanned for vulnerabilities?

Yes. Vulnerability scanning of production systems occurs daily. Security patches for the applications and system OS versions are included in our baseline image build framework and are kept up to date at all times.

Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

Yes. Servers are deployed from a master image, which includes file integrity monitoring and whitelisting controls.

What security tools are implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?

Anti-malware and Intrusion Detection technologies are applied both on the network and production servers.

Production systems are monitored in real-time and generate alerts for both security and availability related events.

Are audit logs centrally stored and retained?

Yes. Internal audit logs are centrally stored and retained for 12 months for forensic purposes.

Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, etc.)?

Yes. Access to Production Systems and infrastructure is restricted to the TransferHub Operations team and is audited. The principles of least privilege and need to know are implemented and regularly reviewed.

Secure Development

Are TransferHub services built and deployed in accordance with leading industry standards?

Yes. TransferHub is committed to following a Secure SDLC to develop, implement, and comply with industry-standard secure coding best practices.

All changes to the TransferHub service, included but not limited to software updates, network or system configuration changes, and security controls go through a formal change control procedure.

Process phases include design, development, functional, integration and regression testing as well as risk assessment. Prior to release to production the source code and application services are scanned and tested for vulnerabilities.

We follow OWASP security by design principles and all changes to the service require peer review and approval by senior management before being released to production.

Zero-downtime deployments allow us to make changes without waiting for a change window and allow us to return the application to a previous state easily.

Are production services isolated from the development process?

Yes. Test and staging environments are separate from the production environment. Customer data is never used or stored in non-production environments or as test data.

Other questions? Please contact us at security@transferhub.io