TransferHub

Data Integrity Policies

Data security is TransferHub's highest priority. We strive to assure that data is protected from unauthorized access and that it is available when needed. These are the policies we use to protect your data.

TransferHub Production Systems & Services

- Production Systems that create, receive, transmit, or store the customer's data are hosted on Amazon Web Services (AWS).
- TransferHub follows the AWS "Well-Architected Framework" in implementing and reviewing "Best Practices" for building secure, high-performing, resilient, and efficient infrastructure for their applications.
- Customers may choose to have their data and backups physically stored in the United States or within the European Union to meet regional compliance and data residency requirements.
- The General Data Protection Regulation (GDPR) is supported.
- TransferHub does not share customer data with any third party.
- All Production Systems are only to be used for TransferHub business needs.

Infrastructure Protection

- All Production Systems disable or remove non-essential user accounts, applications and services that are not required to achieve the business purpose or function of the system.
- Production web servers are protected by network firewall controls, which restrict access to network protocols required to achieve business needs. This is analogous to placing an on-premises web server on a DMZ behind a firewall.
- Production web servers are protected by a web application firewall (WAF) to scan for malicious content and protect against common web exploits.
- Production web servers validate data requests and access the database servers via a private secure API.
- Unfiltered data or commands are never sent directly to the Production database servers.

- Production database servers are protected by network firewall controls, which only allow database traffic between the web services and database servers.
- Production database servers are isolated on a Virtual Private Cloud (VPC) and located on a protected network segment, separate from the web and other internet-accessible servers. This is analogous to placing an on-premise database server on an internal network behind a firewall.

Data Protection

- Production Systems enforce Identity Controls, requiring strong passwords, Multi-factor Authentication (MFA) and/or Single Sign-on (SSO).
- Customer configurable access controls enforce user permissions and restrictions over reading or modifying customer data on a per document basis.
- All Production Data is segmented and only accessible to authenticated users who are authorized to access the data.
- All Production Data is stored encrypted at rest.
- All Production Data is encrypted in transit. Customers may access the Production web servers via HTTPS.
- All Production Data is periodically and cryptographically archived on a separate Production Database instance.
- Customers may securely download a copy of their data store and documents via a RESTful API call.
- Databases use Row Level Security (RLS) policies to allow ACL enforcement at the lowest level.

Detective Controls

- All access to Production Systems must be logged. This includes network connections as well as attempted logins.
- All access to Production Data must be logged. This includes the creation, modification, reading, importing, or exporting of documents.
- All Production Systems are monitored using IDS technology and scanned for malware. Suspicious activity is logged, and alerts are generated. Detected malware is evaluated and removed.

Operations and Maintenance

- TransferHub access to Production Systems is controlled using centralized tools and authentication. Access is limited to Production System administrators in the TransferHub Operations Group and logged for auditing.
- Up to date system lists and architectural diagrams are kept for all Production environments.
- Amazon Inspector is used to perform configuration assessments for known bugs or vulnerabilities.
- Production System administrators leverage and actively monitor external threat feeds and vulnerability resources (e.g., US-CERT, CVE, OWASP, etc.) to help secure Production Systems.
- Patches, applications, and system OS versions are always kept up to date. New versions are tested before deployment and software rollback is supported.
- Vulnerability scanning of Production Systems must occur on a predetermined and regular basis. Scans are reviewed, with defined steps for risk mitigation.
- External third-party Penetration Tests occur on a regular basis, no less than annually.
- Disaster Recovery and Availability policy requires storing encrypted backups off site and in a different region.