Security Policy

Physical Security

Facilities

Screenfluence service providers physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

On-site Security

Screenfluence utilizes ISO 27001 and FISMA certified data centers managed by Amazon. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection.

Screenfluence access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Location

Screenfluence service providers data centers are located in the United States.

Network Security

Protection

All firewalls infrastructure and management is provided by our service providers: Amazon AWS.

Network Security (Contd.)

Protection

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to the ports and protocols required for a system's specific function in order to mitigate risk. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

Vulenrability Scanning

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Our service provider utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Encryption

Encryption In Transit

Communications between you and Screenfluence servers are encrypted via industry best-practices (HTTPS).

Application Security

QA

Our QA department reviews and tests our code base. Dedicated application engineers on staff identify, test, and triage security vulnerabilities in code.

Separate Environments

Testing and staging environments are separated from the production environment. No actual customer data is used in the development environment.

Security Policy

Secure Development

Secure Credential Storage

Screenfluence follows secure credential storage best practices by never storing passwords in human readable format.

Additional Product Security Features

Access Privileges and Roles

Access to data within your Screenfluence is governed by access rights, and can be configured to define access privileges. Screenfluence has various permission levels for organization and users.

Transmission Security

All communications with Screenfluence service provider servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Screenfluence is secure during transit.