Information Security and Privacy

Information Security and Privacy Statement

Protecting the personal information of our clients is something we take very seriously at Ascensus. This statement shares how we protect your personal information. This applies to current and former customer information.

- All client databases, files and other information provided by a client for use with Ascensus services remain the confidential property of the client. All information is retained, and subsequently securely destroyed, in accordance with Ascensus' data retention policy. Client files are not shared with third parties except to facilitate client requested transaction processing or as required by law.
- Ascensus only maintains information required to provide our services.
- Ascensus maintains and monitors appropriate security policies, procedures and practices to protect client files from risks of loss, misuse, alteration, or unauthorized access.
- Ascensus requires its Associates having access to client files to keep this information confidential by using the same care and discretion that Ascensus uses with respect to its own confidential information.
- Ascensus clients assume, and are responsible for, the risk of loss, misuse, alteration, or unauthorized access to client files while client files are in transit to and from Ascensus.
- Ascensus reserves the right to change policies and procedures from time to time to improve security and privacy controls.
- It is Ascensus' policy to require its vendors and business partners having access to client files to keep this information confidential.

Below is a summary of controls Ascensus maintains to protect client information:

Logical Access Controls

Ascensus uses various mechanisms to restrict Associates access to operating systems, data files, databases, and programs in production and development environments. Access to computer resources is based upon an individual's job duties. An electronic sign-on request form must be completed and approved by the Associate's manager before granting system access.

Firewall Protection

Ascensus maintains both network and application firewalls to protect our systems from unauthorized network, application and database activity. These firewalls are layered to provide the highest level of perimeter security and are configured to allow only network traffic that is recognizable as safe. Also, redundancy has been built-in to this architecture in the event there is a failure.

Intrusion Detection & Prevention System

In addition to the firewall technology described above, Ascensus has implemented network Intrusion Detection Systems (IDS) that provide a sophisticated real-time detection mechanism, accomplished by monitoring network in and out of Ascensus. Our solution also blocks malicious activity in some situations as an Intrusion Prevention System (IPS).

Encryption

We use encryption technologies in selected telecommunications channels. Ascensus policy prohibits clear-text transmissions of customer data over the Internet. Ascensus deploys and supports common encryption methods, including, but not limited to: PGP, (S)FTP, SSL/TLS and VPN.

Penetration Tests, Web Application Assessments and Network Vulnerability Scans

Ascensus contracts with leading security firms to perform an annual penetration tests, including focused web application testing and vulnerability scans. The results are tracked to remediation through our Security Team. Additionally, we perform our own monthly vulnerability scans to help identify interim concerns.

Physical Security Controls

Electronic card-access security control is provided throughout Ascensus facilities. A receptionist is on duty in the main lobby of each center during office hours to check visitor's IDs, issue temporary badges and administer the sign-in log. Entry doors are locked outside of business hours. A list of individuals who have access cards is monitored. Physical access to our data centers is highly restricted to only those that require access with motion activated CCTV recordings on entry doors.

Programming and Change Control Management

Formal programming standards and change control procedures are in place. Changes to existing applications and new applications being developed must be authorized, tested, approved, properly implemented, and documented. This structure enables us to integrate security mechanisms to protect changes that effect sensitive information.

Dual Controls and Separation of Duties

The application development and support functions are separate from production functions. Within the production environment, the functions of generating, authorizing, processing, and maintaining custody of assets are separate.

Secure Destruction of Client Data

Ascensus maintains robust destruction methods to insure we securely dispose of hardcopy or electronic equipment that may have client data. We contract with bonded vendors that dispose of our hardcopy documents that reside in locked shred bins. Our vendor that destroys hard drives and other electronic media is also bonded and meets or exceeds all government security requirements for secure disposal – and is 100% recyclable.

Incident Response Program

Ascensus has developed incident response and escalation procedures to isolate, analyze, recover, and report unauthorized access. Recovery involves technical procedures as well as client notification.

Security & Privacy Training

Ascensus requires all Associates to complete annual security & privacy training. Additionally, Associates are reminded of their duty to protect confidential information through emails, internal publications and office postings.

Associate Background Checks

Ascensus Associates must pass credit, criminal, employment and education background checks before hiring.

External Audits (SSAE16)

Ascensus has successfully completed SSAE16 audits (used to be known as SAS70s) conducted by leading audit firms to test controls around our services. Many of the controls summarized in this document are tested by the SSAE16 and help to protect sensitive information.

Ascensus Website Privacy

Ascensus maintains a privacy statement that is accessible on all our websites that describes how we collect, use, and protect the information gathered. Links to this statement are typically accessible at the bottom of our web pages.

Information Security, Organization and Oversight

Ascensus maintains an Information Security function with dedicated resources as well as other supporting functions, such as an Information Security Council that meets monthly to involve cross functional teams into the security effort and strategies. Also, an Ascensus Governance, Risk Management and Compliance function integrates with Security to insure we effectively address information security throughout the organization with appropriate oversight and meet compliance requirements.