Security

SaveOnFaxes is committed to protecting your sensitive information and keeping it secure is our top priority. SaveOnFaxes product and service resiliency is built on its long history as the world's principal provider of business communication services and the company's commitment to customer care.

System security is comprised of procedural and technical safeguards to protect against unauthorized access to SaveOnFaxes facilities and system data.

- **Physical Security**

To ensure a secure physical environment, SaveOnFaxes limits all facility access and utilization based on business needs in accordance with job responsibilities. Each employee's role is evaluated before access levels are assigned. Specific customer data areas, applications and locations are included in the authorization.

All areas deemed to contain sensitive data, or where sensitive cluster operations occur, are locked. At the New Jersey facility, an assigned card-key is required for access. In addition, the Data Center is staffed 24x7 by SaveOnFaxes professionals who are charged with monitoring the facility. This staff follows established operating guidelines that define procedures for handling expected and problematic conditions, recording environmental issues and other events in logs and turnover journals, and alerting the appropriate people of suspicious activity when necessary.

Non-operational staff may only access the Data Center with an approved escort. Contractors and third-parties may be approved for access to SaveOnFaxes areas/systems for business reasons, limited to the time required to accomplish defined and approved tasks. Upon completion, access to all SaveOnFaxes resources is revoked.

Access is monitored through several levels of auditing and logging, and alert tools keep management aware of violations or exceptions.

All access points at the Virginia facility are controlled with biometric hand readers. The Virginia facility offers the additional security measure of locating servers and networking operations in private or shared caged areas. In shared cage situations, visitors are escorted to their area. Cage access histories are recorded and available for review. In addition, customer equipment racks/cabinets within the cages have self-powered locks with a numbered keypad to restrict access.

All areas of the Virginia facility are monitored by 24-hour security officers and visitors are required to produce a valid government-issued picture ID. The entire facility is covered and recorded by CCTV, which is integrated with the access control and alarm system. All exterior entrances are protected by silent alarm and automatic notification of law officials. The exterior of each facility is fully anonymous with no signage.

- **Security Infrastructure**

SaveOnFaxes maintains multiple layers of hardware and logical access controls to protect environmental integrity and the confidentiality of resident customer data. The security staff has developed a platform that is adaptable to internal and external requirements. Components of the infrastructure include:

Component	Features
Firewalls	Manages Internet access using port and rule-based controls. Clients are further segmented by individual extranets.
Intrusion Detection Systems (IDS)	Used both at the network and system level to monitor and prevent unwanted activity.
ID Management Solution	LDAP /Kerberos-based for authentication to production systems.

Network Vulnerability Scans	Performed twice a year by two different parties. Vulnerabilities are analyzed then remedied.
Anti-Virus	Performed by McAfee.
Log Analytics / Monitoring	Handled by a combination of Micromuse Netcool, HP Openview and an application developed in-house to monitor application performance and availability.
Transaction Security	Uses encryption when needed.
Database Protection	Managed on a customer need basis with AES storage encryption services.

- **Data Security**

SaveOnFaxes employs a robust security infrastructure to maintain the confidence of customers and to address regulatory requirements imposed on SaveOnFaxes as a public entity, as well as those requirements imposed on our customers. The security infrastructure is viewed by SaveOnFaxes as a competitive business asset that delivers value to our customers.

- **Data Access Controls**

SaveOnFaxes employs a formal procedure for granting, modifying and revoking access to all SaveOnFaxes information, systems and networks.

- **Internal Access Control**

Authorization and access to all SaveOnFaxes system utilities is based on business need in accordance with job duties and responsibilities. SaveOnFaxes provides accounts, User IDs, passwords, and encryption characters to approved users.

Contractors and third-parties (e.g., external service providers) may access SaveOnFaxes information systems based on business requirements and subject to SaveOnFaxes management approval. When approved, access to

SaveOnFaxes communication and information systems is granted only for the time required to accomplish defined and approved tasks. Such users must sign a non-disclosure of information statement at the beginning of their contract.

All users are responsible for maintaining the security of their account and password. Access shall be immediately revoked whenever a user changes his/her job function or ends their relationship with SaveOnFaxes.
Access privileges and account activity is regularly reviewed for unusual account behavior. SaveOnFaxes explicitly prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of its information and information resources. All users granted access must abide by SaveOnFaxes information security policies and procedures.

- **External Access Control**

Remote access to SaveOnFaxes internal network by authorized users (e.g., staff working remotely, customers) also requires User IDs and passwords. Access is granted through a centrally managed virtual private network (VPN) that provides encryption and secure authentication. Systems that contain strictly confidential company and client data is available remotely only after an explicit request is made and approved by the data owner or originator, and is subject to the provisions outlined in SaveOnFaxes data classification policy. Remote access privileges are always subject to review and may be revoked.

There is no direct access to SaveOnFaxes core systems by external users. External controls include our Firewall Demilitarized Zone (DMZ) to limit the sources and types of traffic permitted. The DMZ utilizes monitored network-based IDS as an alert mechanism. Restricted external access is allowed via customized access gateways for data transmission using Verisign web-based SSL public-key encryption or customer-requested hardware VPN's over data-acquisition/distribution.

Customers accessing SaveOnFaxes network are limited through the application to view only their data. Within the customer IDs, they are allowed to further segment rights for their own employees. There are some application-to-application integrations that allow queries and updates to SaveOnFaxes systems. These applications are authenticated through a combination of ID and SFTP authorization.

Security Audits

Penetration Audits

Periodically, SaveOnFaxes contracts third-party auditors to test SaveOnFaxes remotely accessible paths to its external network to identify possible exposures. The results are reported back to management and SaveOnFaxes closes any new or evolving threats, enabling us to continue meeting our commitment to trustworthy services.

SaveOnFaxes has contracted Ernst & Young, TrustWave, and Greenwich Technology Partners Inc. (GTP), all leading network infrastructure-consulting firms, to perform such audits. Industry accepted network testing tools and manual penetration techniques are used to assess the protection surrounding SaveOnFaxes Internet facing resources. These tests try to discover unnecessary exposures by challenging deployed controls with probes common in today's inter-connected world. Results of these tests have given SaveOnFaxes medium-to-low threat ratings on a risk exposure scale. Such a rating puts SaveOnFaxes on par with peer service providers. SaveOnFaxes has followed up on the audit results by resolving virtually every minor issue reported.

User Audits

All SaveOnFaxes system users are authenticated and identified prior to access, and a record of user activity is maintained so that users can be held accountable for their actions. This log of activity, or "audit trail," records system and application processes as well as user activity of systems and applications.
Additional logs are kept of key system activities, such as User ID creation or deletion, and suspicious or anomalous activity which might be an indication of unauthorized usage.

System Audits

SaveOnFaxes systems are audited on a regular basis. At a minimum, the audit process includes consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures.

Audits also include the regular use of vulnerability analysis software. Audits are performed by technical personnel other than those responsible for the administration of the systems.

Specific types of transactions, such as financial, require additional data security measures that should be assessed by a professional organization. In 2004, SaveOnFaxes contracted with TrustWave to perform a TrustKeeper Payment Industry Compliance (TPIC) assessment to determine if their facilities comply with the major Card Associations' published security guidelines and requirements. The TPIC assessment focused solely on the security of Cardholder data, whether SaveOnFaxes has implemented information security policies and processes, and if the security measures are adequate to comply with the various card industry requirements to protect Cardholder data.

The initial review, performed in 2nd quarter 2004, identified specific 'Required for Compliance' areas for improvement. By the beginning of the 3rd quarter, each of these categories had been clarified and, where necessary, improved. SaveOnFaxes is now certified as compliant with the TPIC and Cardholder Information Security Program (CISP).

- **Employee Confidentiality**

Trustworthy employees are critical to the security of a successful operation. SaveOnFaxes has instituted the following procedures to mitigate risk created by employees who have access to confidential customer data:

- Upon hiring, all SaveOnFaxes employees are subjected to a background check to uncover possible vulnerabilities or past acts that are unacceptable.

- All SaveOnFaxes employees receive employee handbooks which include details on their handling of all sensitive information. The booklet instructs associates to avoid misusing or disclosing any customer data. Our employees are required to sign an acceptance statement and honor that standard as a condition of continued employment. This message is periodically reissued to promote awareness among staff, consultants and other necessary third-parties.

- Internal processes are in place to ensure that proper data handling methods are observed. Sanctions include reprimands and dismissal.

Consistent compliance of all policies is essential to successful implementation. All SaveOnFaxes employees and affiliated third-parties are expected to conform. Non-compliance of employees with any of the provisions set forth, either willfully or through neglect, could be categorized as misconduct and subject to disciplinary actions.

Non-compliance by consultants or third-parties will result in removal of access by the external service provider to SaveOnFaxes computer and communication systems, and may also result in termination of any existing contracts.

Risk Management

SaveOnFaxes constantly evaluates various risk scenarios that could impact the system infrastructure, impeding operations and standards compliance. Management actively promotes programs for ongoing risk assessment and reduction, and supports the development and maintenance of necessary procedures and product standards needed to keep current with evolving issues. Reasonably foreseeable events are vetted by a series of design review forums, security evaluations and scans. All change management processes are reviewed by the Security Manager to ensure that security and contingency considerations are addressed. Resulting action items are implemented through internal / external access controls and security infrastructure.