



SEND WORD NOW SECURITY CONTROLS

At Send Word Now, we're completely dedicated to protecting all of our customers' sensitive data. We take this responsibility seriously, and we treat it in the same manner as our promise to always deliver critical services in times of great need. And so in that regard, we've taken all possible measures to ensure the highest degree of security within our service, infrastructure, and data centers, to deliver the highest quality of service to you, our valued customer.

How are Customer Passwords Protected?

All communication with the Send Word Now service occurs over 128-bit encrypted (SSL) connections. Globally unique usernames and passwords are used to protect user accounts, customer administrator accounts, Send Word Now administrator accounts, as well as the network elements, servers, and applications that comprise the Send Word Now Service.

Customer administrator accounts and passwords are established by a Send Word Now Customer Support Manager (CSM), and they can be modified by customer administrators and Send Word Now Customer Support. Administrator passwords are case sensitive, and must conform to policies (complexity, reuse, expiration) established by the customer administrator. And because these passwords are not validated client-side, they are not at risk for client-side eavesdropping or cracking.

How is each Session Protected?

After a user is authenticated, a unique session is created to keep track of his or her ID, IP address, and activity. Each request must consistently return the session value and correct user information, and so if the session/IP address combination changes, the session is terminated.

Whenever a user makes a request, the appropriate SP checks whether the request is valid according to the user's role, the user's entitlements, and the user's rights to any pertinent data in the database. In certain cases, an SP may be invoked from the application without intervening middleware; in other cases, the middleware may pass information that is ultimately arbitrated by an SP. At the database level, the rights and associations between the user and key data elements are typically enforced in a three-table, two-column format. So, for instance, if there is a "Member" table describing a user's properties in detail, and a "Group" table describing a group's properties in detail, there is also a "Member-Group" table that pairs the unique identifier for the member with the unique identifier for the group. If there is no association, the member cannot see, retrieve, or modify any information associated with that group. If there is an association, the request is validated and the system responds with the pertinent information, enabling the user's next action(s) as applicable.



How are Administrator Authentications Different?

After successful authentication, an encrypted session token containing the username, IP address, and user activity is generated and an account's feature authorizations are confirmed in the database. Send Word Now offers a "Features by Account" model in which each account can have separate feature authorizations, which customizes the account user interface to the customer's preferences.

Assuming the authenticating user is an account administrator, he or she will typically have full entitlement within the account. In unusual business cases, it is possible to reduce administrator entitlements for role-based administration, but administrators will have full privileges within an account by default.



If the user is not an administrator, there are a series of configurable entitlements, some assigned by the administrator in real time, and some that may be executed by Send Word Now Customer Support, for limited-privilege users. Such configurable entitlements may include sending alerts, seeing and editing recipient contact information, seeing specific alerting groups, seeing groups and recipients from multiple accounts, and running reports.

How does Send Word Now Safeguard its Service Complexes?

At Send Word Now's data centers, redundant Cisco firewalls block all but the necessary categories of traffic entering a service complex (HTTP, HTTPS, VPN, etc.). These firewalls limit the traffic between servers within the complex. For instance, traffic to and from the databases located on the database servers is limited to that originating from (and terminating on) the application servers. The firewalls and intrusion detection devices also reduce vulnerabilities to denial of service attacks.

Send Word Now data centers provide extensive state-of-the-art physical security, and we've taken many steps to ensure customer information is always protected:

- On-site security guards are present 24/7, supplementing both indoor and outdoor security monitoring.
- Access to a facility requires a valid photo ID as well as inclusion on the list of authorized personnel for that facility.
- Biometric hand scans are required for entry to a facility, as they limit hosting customers from moving from one co-location area to another within the facility.
- Closed circuit cameras monitor and record every area within the facilities.
- Customer equipment within the hosting facilities is either in a locked cage or a locked cabinet. The hosting provider keeps all keys to cages and cabinets; customers do not have copies of the keys. As a result, only Send Word Now personnel have either physical or logical access to Send Word Now resources.
- Application data is backed up and secured using near real-time log shipping between Send Word Now service complexes. There are also weekly backups.
- Customer data is never transferred onto portable media. This data is backed up from secure site to secure site, and remains resident behind the firewalls, DMZ, etc. (Code backups do go to media and are taken physically offsite from operational centers.)

What Other Security and Privacy Controls Does Send Word Now Have in Place?

All Web applications within the Send Word Now service are hardened in order to eliminate known classes of vulnerabilities to malicious attacks, and all servers are protected with anti-virus software. Virus definitions are updated automatically and regularly. SNORT is used for network intrusion protection and detection.

At Send Word Now, we always require entry-point sensitivity determinations when hiring new members of our personnel. Sensitivity levels for Send Word Now are set at an absolute level to obtain employment, and further articulated according to an employee's role within the organization.

Send Word Now provides role-based access to sensitive resources as needed to appropriate employees. Additionally, we observe the privacy principles of Notice, Choice/Fair Processing, Access, Security/Integrity, Onward Transfer and Enforcement/Compliance in processing personal information, and we also comply with EU-U.S. Safe Harbor privacy principles published by the U.S. Department of Commerce.