



SECURITY MATTERS: EVERY LAYER OF PROTECTION COUNTS

SEND WORD NOW'S UNWAVERING COMMITMENT TO SECURITY

At Send Word Now, we take security very seriously, and we approach all aspects of our infrastructure and services with this in mind. Whether it concerns the location of our equipment, the method of firewall changes, or our process management, we manage every detail in order to properly safeguard our customers' data on a platform that is secure, reliable, and resilient. Our goal is to provide the most secure notification platform in the industry and offer our customers a system that they can trust.

We know that notification systems are often reserved for crises, and that they are often used when all other communications systems fail. That's why we believe that the most effective ENS is the one that's always the best secured against attacks, system crashes, and data loss. No matter what happens during a crisis, Send Word Now's robust security features will always be there to provide you the highest threshold of protection. You can always count on us to protect your employee contact data, to deliver your messages on time, and to keep your notification system running whenever you need it.

The Send Word Now Platform - Putting Safety and Security First

At Send Word Now, we strive to always be the most secure notification provider in the industry, offering the highest levels of security and data protection, along with the most customer-facing, customizable security options. Because security is not a product. It's about building layers of protections around a platform and testing those processes rigorously and regularly. And the most reliable provider is the one that ensures proactively that your account is secured against attacks, system failures, and loss.

Our infrastructure is based on a strong foundation, which is maintained through systematic updates, monitoring, auditing, and reporting. The security of our system is based on a defense-in-depth approach, and provides comprehensive protection against attacks.

Network and System Security

In order to protect the system, we have secured all equipment in hardened parts of the network that are not externally accessible, and use both carrier-grade Session Border Controllers (SBCs) and firewalls. Send Word Now's SBCs are configured to only accept traffic from white-listed IPs, while all other traffic is ignored so as to not incur any overhead to the gateway.

Information Security

We are committed to providing the highest levels of information security for all aspects of our platform and we adhere to data privacy best practices at all times. We offer our clients secure and encrypted data transfer, along with role-based access controls and permissions, detailed logging and reporting, and the reassurance of a comprehensive audit trail. Additionally, we comply with the EU Safe Harbor framework.





Redundancy

Send Word Now has active-active data centers. This means that we are up and running in top-tier data centers in multiple, geographically distributed locations at once, ensuring instant failover should an issue arise at one data center. Our fail-over is seamless, and it will never affect your service. Additionally, we provide all of our customers with a 100% uptime guarantee, which is built into our standard service level agreement.

Third-Party Validation

PEN Testing: Send Word Now conducts third party penetration testing to simulate attacks (known as ethical hacks) on an annual basis. We turn to non-biased auditors to conduct detailed PEN tests from both the inside and outside of our system. To provide you added peace of mind, we allow all of our customers to hire their own third party auditors as well. We consider our platform to be an extension of your security environment, and we will allow you to test it according to your standards.

SAS 70 Type II Audits: A clean SAS 70 Type II audit opinion confirms that a notification provider's operations are secure and reliable, and that it is able to deliver customer messages whenever necessary. By illustrating that internal controls within the organization are in place and working as they were meant to, a clean SAS 70 Type II opinion can reassure you that the security of your communication platform is not at risk.

DIACAP compliance: DIACAP (the DoD Information Assurance Certification and Accreditation Process) is a process developed by the Department of Defense to ensure that information systems apply proper risk management standards. By choosing an emergency notification provider that's DIACAP compliant, DoD-affiliated organizations will know for sure that their communications platform will be held to a formal and U.S. government-sanctioned set of security requirements.

Customer-Facing Security Features Provide Added Security and Confidence in Your Alerts

The Send Word Now platform has been designed to meet the highest industry standards, but we haven't stopped there. We recognize that customers in various industries might require additional security controls, and we've created a broad range of features by account to address those needs. You can build and customize your own security controls on top of our platform, picking only the features that support your organization the best.

Additional Features for your Send Word Now Account Include:

Password Security: When you create an account, Send Word Now will send you an initial password, but will also require that you update it immediately to protect your privacy. Using Send Word Now's platform, you can add additional levels of security by specifying your organization's requirements for creating and using passwords. We recommend that you set a minimum length for passwords for your users and adjust complexity levels to require upper case, lower case, and symbols. Set password expiration timeframes, prevent the re-use of a password for a specific number of iterations, and enable auto-lockout after a specific number of invalid login attempts. By doing this, you'll significantly lower the risk of your users' passwords being discovered.

Customizable Session Time-Out and Access Roles: Sometimes, the security of your data and your alerts can be compromised by unwanted users gaining access to your controls. Through Send Word Now's service, you can set a customized session time-out to ensure that no unwanted customers, employees, or passers-by can gain access to your console when you walk away from your computer. Additionally, you can set customized administrator access roles to make sure that different employees at different management levels only see what's appropriate for their position.



Two-Factor Authentication: One of our favorite security features is called Two Factor Authentication. With this feature enabled, users are required to authenticate themselves in two ways in order to login to the service. Along with the standard username and password, users will be required to input a random number that is refreshed every few seconds by a unique hardware token. For customers in industries that protect sensitive data, we recommend this feature for additional security and peace of mind.

PIN Codes for Outbound Voice Messages: While many features ensure the security of the user login, it's also important that you maintain proper security controls on the recipient end of your alerts. To make sure that your messages don't end up in the wrong hands, you can assign PIN codes for access to incoming voice calls so that contacts without assigned PIN codes are not able to listen to phone alerts.

Digital Signatures: In today's public Internet age, security is everything. You don't want the wrong information to get into the wrong hands, especially when dealing with emergency situations. With digital signatures, the recipients of your alerts can know for sure that you are the sender of any given message. This additional layer of security is ideal for any type of sensitive information that is distributed within your organization.

Single Sign-On: Using single log-in, a user can log in with a given set of credentials to only one account at a time from any given browser. Additionally, that user can log in with those credentials from only one browser at a time. This means that credentials cannot be used by multiple users or across multiple sessions. You can also customize your session-time out to prevent unwanted users from accessing your system while you're not using it.

Secure Encryption SSL: Send your data to Send Word Now via our secure encryption SSL. Take advantage of this optional feature to protect the privacy of your data, sending it directly to your account via a secure and encrypted line.

The Bottom Line

Security is not a feature by account. And it's not something that should be tacked on to a platform as a second thought. Security is a threshold, and at Send Word Now, we do our utmost to exceed that threshold by maintaining features that surpass industry standards and by developing the most secure services for our customers.

In choosing your notification system, you should ask any provider for detailed information on security programs before digging deeper into their offerings. And when other providers can't provide the features listed here, think twice before considering their services. We love bells and whistles, and we're always working to develop state of the art features and add-ons to our platform, but without our security measures in place, they wouldn't mean anything. Security is the cornerstone to our service, and we plan on keeping it that way.