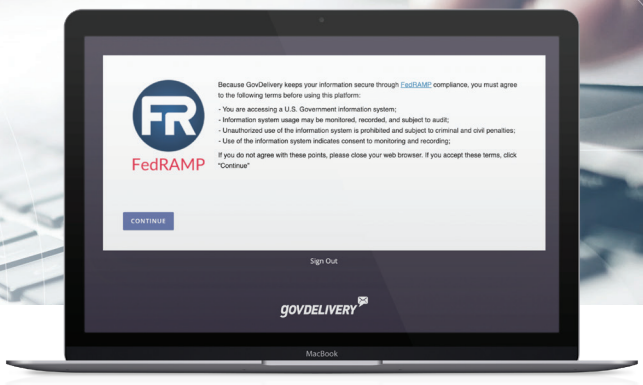
govDelivery

FedRAMP

Federal-grade Security for govDelivery



DID YOU KNOW

66%

of organizations attacked by hackers were not confident they could recover?

FedRAMP Security Highlights

- Enhanced FedRAMP security features for govDelivery – including complex password management, IP restrictions, and multi-factor authentication.
- Encryption utilizing FIPS 140-2 validated encryption modules for all connections.
- Security reporting for logging and monitoring administrative activity.
- On-going communication and subscriber data protection.
- Hands-on security guidance and training.

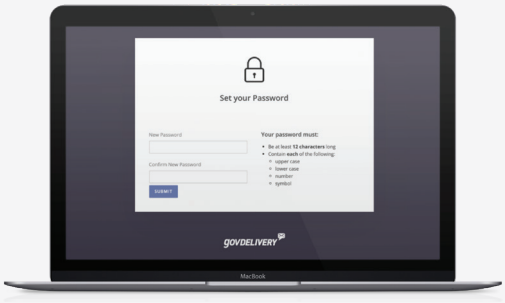
Simple Steps to A More Secure Future

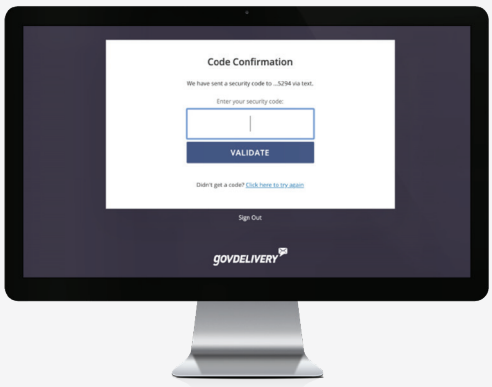
Protect agency communications and subscriber data with enhanced, FedRAMP-authorized security for govDelivery. By enabling Federal-grade, best-in-class security controls, organizations can be confident that hundreds of process, environment, and technology requirements for FedRAMP security standards are consistently met and updated as necessary without placing the burden on their teams.

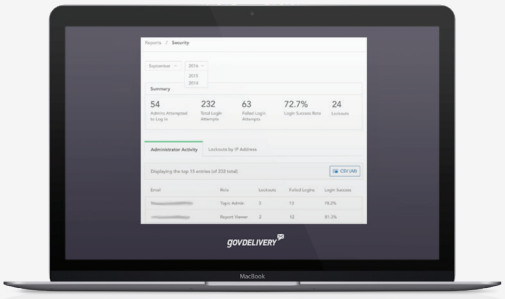
What If You Could...

- ✔ **Quickly adhere to best-in-class security practices** with FedRAMP's required compliance measures, like password complexity requirements and session logout controls?
- ✔ **Proactively combat unauthorized access** by limiting access to only trusted IP addresses and enabling multi-factor authentication?
- ✔ **Establish security monitoring and reporting** to ensure only authorized users continue to have account access?
- ✔ **Gain security guidance and training** to help internal teams easily adapt to new security approaches?
- ✔ **Leverage Granicus experts** to provide recommendations when pursing your agency's Authority-to-Operate (ATO)?

govDelivery







With FedRAMP Security You Can...

Strengthen govDelivery administrator controls

- Require administrators within your organization to change their password at a more secure interval.
- Enforce complex passwords management that complies with FedRAMP requirements.
- Set administrative controls to automatically log out due to govDelivery session inactivity.

Shield unauthorized govDelivery account access

- Activate multi-factor authentication by means of either SMS, voice, or via PIV card tied to OMB MAX.
- Ability to limit account access to only IP addresses in a trusted list identified by your agency.
- Option to temporarily lockout of govDelivery after a predetermined number of failed login attempts.

Monitor security levels with govDelivery reporting

- Summary of login attempts and lockouts across your agency's govDelivery account.
- View an administrator activity section for a breakdown of login attempts or lockouts by administrator.
- See a display of where and when a lockout happened, as well as login attempts made from IP addresses outside your trusted list.

Shared Security Commitment

Granicus shares security responsibilities through a list of controls for your agency to easily meet FedRAMP compliance requirements. Once your agency issues an ATO with FedRAMP, access is given to our complete system security plan (SSP) and monthly continuous monitoring results to show security-related POA&M items are addressed in a timely manner. During initial implementation and training, your team is also advised of security options and best practices to support on-going security protection.

Trusted Partner for Federal Agencies

About Granicus: More than 4,200 government agencies use Granicus to modernize their online services, web presence, and communications strategies. We offer seamless digital solutions that help government actively reach, inform, and engage citizens on the first unified civic engagement platform for government.

GRANICUS

For more information, visit granicus.com/solution/govdelivery or email us at info@granicus.com.