GO ANYWHERE®
Managed File Transfer

DATASHEET *(Cybersecurity)*

Simplified, Secure and Automated Managed File Transfer Solutions

Simplify file transfers while meeting FISMA compliance requirements

Government agencies face significant regulations and security policies when it comes to protecting sensitive data. An effective Managed File Transfer solution is critical for helping agencies meet these strict security requirements.

HelpSystems' GoAnywhere Managed File Transfer solution helps organizations meet the data security requirements of regulations such as the Federal Information Security Act (FISMA.)

FISMA mandates that every agency must create, document and implement a plan to ensure that the information systems and the data they contain are kept secure. This includes data that is provided or managed by third-party entities such as other government agencies, contractors and trading partners.

GoAnywhere is FIPS 140-2 Certified to Keep Sensitive Data Secure

Government professionals at all levels can manage data transfers more efficiently and securely with these enterprise-level benefits:

- Centralized file transfer processes within the organization;
- Automated workflows with configurable step-by-step wizards;
- Restriction of critical access to files and folders to only authorized users;
- Monitoring for file transfer processes – both across the Internet and within the organization's intranet;
- Detailed audit trails and reporting of every file transfer, identifying the users, the recipients, and the file names transmitted; and
- Integration with pre-existing applications within the organization.

Data is protected using NIST-Certified FIPS 140-2 Validated Cryptography, provided through an embedded RSA security module that includes the popular AES and Triple DES algorithms. Users are authenticated, ensuring only the intended party can access and read the files. Detailed audit trails will track file movement with extensive reporting, all managed through a browser-based centralized dashboard. GoAnywhere has also earned the Certificate of Networthiness (CON) from the U.S. Army.

GSA Advantage!®

NAICS codes:
511210

Cage code:
5GFH6

GSA Contract ID
47QTCA18D0058

Meet FISMA regulations with detailed auditing, strict administrative controls and FIPS 140-2 encryption

The table below shows how the GoAnywhere™ Managed File Transfer solution helps organizations satisfy the compliance requirements for the FIPS 200 and NIST Special Publication 800-53 Information Security Standards and Guidelines. Government entities have the flexibility to apply the baseline security controls so that they align with their business requirements and environments of operation.

NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	Corresponding GoAnywhere Feature
Access Control Prevent unauthorized access from users or software that do not have permissions.	Users and passwords can be authenticated using a variety of techniques including database authentication, LDAP and Active Directory (AD). Accounts can additionally be authenticated using X.509 certificates and SSH keys. Role-based security allows administrative users to access only authorized features. Folders and files can be authorized to user groups or individual users.
Audit and Accountability (AU) Ensure security risks are identified, tracked and reported through audit trails.	Audit trails will document all transactions, making it possible to detect and document any time unauthorized attempts are made to alter or delete documents through GoAnywhere.
Security Assessment and Authorization Meet criteria outlined by an independent review of a Security Assessment Plan, conducted to demonstrate that controls and procedures are in place to ensure the agency's compliance with security requirements.	Integrating GoAnywhere into an organization's Security Assessment Plan is critical because it includes administrative controls that designate which functions are accessible to specific users or groups, as well as detailed auditing that document file transfer activity.
Configuration Management Provide change control to monitor and track for changes in baseline configurations.	Changes made to file transfer configurations are tracked in the audit log.
Contingency Planning Develop a business continuity strategy to provide a contingency plan for information systems.	GoAnywhere is highly scalable with support for clustering and Active-Active failover.
Contingency Planning Ensures each user can be tracked and prevent unauthorized access from users or software that do not have permission to view or access.	Each GoAnywhere user must have a unique user ID and password to log into GoAnywhere. Every user can be restricted to perform specific tasks within GoAnywhere.

Source: NIST Special Publication 800-53, Revision 4; Security and Privacy Controls for Federal Information Systems and Organizations
http://dx.doi.org/10.6028/NIST.SP.800-53r4

In addition to satisfying these government requirements, GoAnywhere also helps government agencies are comply with other regulations such as HIPAA, HITECH, PCS DSS, SOX and GLBA.

GoAnywhere.com | 402.944.4242 | 800.949.4696 | goanywhere.sales@helpsystems.com

helpsystems
www.helpsystems.com

About HelpSystems
Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.