goanywhere
by HelpSystems

GUIDE *(Cybersecurity)*

Our View on Security and Compliance

GoAnywhere works within compliance frameworks, regulations, and standards to help you make the best decisions for your data security. GoAnywhere is ready to help you in your quest for compliance and assist you in processing your data in a secure manner. Whether you use GoAnywhere on-premises or in the cloud, you get to choose how to manage, monitor, and audit the controls surrounding your data.

The GoAnywhere Philosophy

We care deeply about security and compliance.

As a software solution dedicated to protecting your sensitive data in motion and at rest, GoAnywhere MFT takes all aspects of data security seriously. We actively improve security and compliance in GoAnywhere and maintain a roadmap to keep us moving forward. You will always be in the driver seat on your data security, and we'll be here to help you build a better IT.

Enabling Data Security Compliance

GoAnywhere MFT addresses many controls in popular and widely-used security frameworks, standards, and regulations, including:

- PCI DSS
- The GDPR
- HIPAA & HITECH
- FISMA & NIST
- Australia's CDR
- PIPEDA
- California Consumer Privacy Act
- Singapore's PDPA

See how GoAnywhere addresses your industry's standards ›

Security Features in GoAnywhere

Auditing & Reporting

- Generate full audit trails of all user events and file activity with reporting
- Feed audit log messages to a central SYSLOG server

Authentication & Encryption

- Use Domains to virtually segment a GoAnywhere installation into multiple security zones
- Filter connections with IP blacklists and whitelists (Global and User level)
- Block Brute-Force and Denial of Service (DoS) attacks with an automatic IP blacklist
- Authenticate SFTP connections with passwords and/or SSH keys
- Utilize only FIPS 140-2 certified encryption algorithms to meet U.S. Government (NIST) standards
- Authenticate FTPS and HTTPS connections with passwords and/or SSL certificates
- Automatically encrypt files on disk using AES256 encryption
- Ability to accept or reject files with certain extensions
- Run services under non-standard port numbers
- Create and manage SSL certificates, SSH keys, and Open PGP keys through integrated screens

User Access & Controls

- Authenticate users against LDAP, Active Directory (AD), IBM i profiles, RADIUS, RSA SecurID, Google Authenticator, Duo Security, and other IAM (Identity and Access Management) solutions
- Define administrator user permissions for separation of duties
- SAML support for single sign-on and dual factor authentication
- Restrict users to specific home directories and subfolders
- Specify folder level permissions (upload, download, delete, rename, etc.) by user and group
- Restrict user logins to certain days-of-week or times-of-day
- Set password policies and expiration intervals
- Authorize selected services (e.g. FTP, SFTP, FTPS, HTTPS and AS2) to certain users and groups
- Disable user accounts after maximum login attempts
- Disable user accounts automatically after a period of inactivity
- Receive instant notifications on login failures
- Disable anonymous login
- View the active sessions for logged-in users with the ability to terminate (kick) sessions

Encryption

There's no doubt that encrypting sensitive files at rest and in motion is essential to guard against cyberthreats and for compliance with local, national, or industry-standard requirements. Encryption is one method of encoding information so that it's unusable until decrypted – giving only authorized parties the keys to read or access that data. Encrypting files helps to prevent unauthorized access or tampering while data is in transit or at rest, depending on the method used.

Each encryption standard helps to protect the privacy and integrity of your organization's data slightly differently (Open PGP, GPG, SFTP). Overall, file encryption encodes your data either in motion or at rest, or both, and requires a key to decrypt the data. This keeps the contents of your files secure.

Interoperability

GoAnywhere MFT interfaces with partners and external users via multiple protocols and advanced workflows. GoAnywhere is tested for interoperability with enterprise-level operating systems, popular web browsers, and to ensure it meets commercial and federal compliance regulations.

Organizations have used GoAnywhere to:

- Create multi-state interoperable systems with 24/7 functionality
- Meet Drummond requirements for AS2
- Provide technical safeguards for file transfers between organizations
- And more!

There are many ways to connect your GoAnywhere instance with servers, tools, and popular cloud and web apps. Learn about GoAnywhere's connectivity features, our Cloud Connectors, ways to integrate GoAnywhere MFT with applications you use every day, or our Secure ICAP Gateway, which introduces deep content inspection engine, adaptive data redaction, and flexible policy settings to GoAnywhere's file transfer capabilities.

GoAnywhere MFT: A Closer Look

Learn how organizations use GoAnywhere MFT

Have a Feature Question? Ask an Expert

GoAnywhere Solutions

goanywhere by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.