

DATA SECURITY

Goldleaf Partners is continuously evaluating and deploying the latest cybersecurity technologies to ensure the integrity, confidentiality, and availability of information.



Goldleaf uses a unique and comprehensive strategy to protect the integrity of our network, programs, and data from cyberthreats, damage, or unauthorized access. Our security measures involve the deployment of the latest technology to safeguard your data from malware, ransomware, phishing, and application attacks. We also employ hardware-based measures, such as data encryption and offsite backup storage, to ensure that data is safe from malicious attacks by viruses and hackers. Our security measures defend against the full spectrum of threats.

SECURE EMAIL AND FILE TRANSFER

Many cyber threats infiltrate networks through malicious email. Goldleaf utilizes ZixGateway for transferring protected electronic data with clients and partners. Using proven policy filters, emails and attachments are scanned automatically for privileged or proprietary information. If emails contain sensitive data, they can be encrypted or quarantined.

To prevent malware, ransomware, and other advanced threats from compromising our email and network, Goldleaf has employed ZixProtect to analyze multiple characteristics of email, starting with IP addresses and URLs. ZixProtect examines email content for targeted phrases, campaign patterns, and both known and zero-hour malware attacks. We also employ additional email security with multi-factor authentication through Microsoft Office 365.

For the transfer of very large files, or bulk file transfers, Goldleaf utilizes ExaVault's S/FTP platform to keep data secure. The ExaVault infrastructure employs data centers throughout the United States with best-in-class computer and network security policies to protect data from online attackers. Their SOC 2 Type 1 and 2 facilities require four-factor biometric authentication to physically access equipment.

SECURE NETWORK

Goldleaf has implemented RSA's SecurID® to provide identity and access assurance through our VPN. RSA SecurID® software tokens use a highly secure provisioning protocol, the Cryptographic Token Key Initialization Protocol (CT-KIP), to support two-factor authentication. This ensures our remote employees are working through a secure connection.

Goldleaf uses Varonis' DatAdvantage to employ machine learning and bi-directional cluster analysis to identify and safeguard PII (Personally Identifiable Information), PHI (Protected Health Information), and PCI (Payment Card Industry) data. This ensures that sensitive data will not be overexposed and will be protected from internal and external threats.

**sensitive data will
not be overexposed
and will be protected
from threats**

Additionally, Goldleaf uses Varonis' user behavior analytics to detect cyber threats by analyzing data, account activity, and user behavior. This technology monitors, identifies, and flags suspicious activity so that we can investigate potential security issues before it's too late.

SECURE HARDWARE

Goldleaf backs up all data and encrypting before replicating to an offsite location that is SAS70 (SSAE16) certified. When we must maintain necessary data from partners, we utilize our secure network document management system protected with firewalls to access structured data.

SECURE OFFICE

In addition to employing the latest software and hardware technology to protect our electronic data, Goldleaf has adopted company policies to reduce and protect the amount of sensitive unstructured data on our desks, computers, and network. These policies include:

- Clean Desk Policy to eliminate exposed conditional and sensitive information whether it be on paper, a storage device, or a hardware device.
- Password Policy, which requires all users to have strong network passwords which must be renewed frequently.
- Multi-factor Authentication Policy for Office 365 applications.

All Goldleaf employees are required to use the password manager LastPass to store, secure, and manage passwords. LastPass uses AES-256bit encryption with PBKDF2 SHA-256 and salted hashes to provide Goldleaf employees with complete password security in the cloud.

In the event of cybercrime, Goldleaf Partners is prepared with cybercrime insurance. Coverage includes security and privacy liability, regulatory action sublimit of liability, network interruption, cyber extortion, media content, and event management.

