

Your privacy and confidentiality is our #1 priority.

TitanFile is an ISO 27001 certified and SOC-2 compliant solution helps organizations of all sizes maintain the privacy, security, and compliance around the confidential information they share.



State-of-the-art Security and Privacy Features



Encryption

Encryption in Transit

All communication between client and server is performed over a 256-bit TLS connection. This is the strongest, most secure form of encryption that is generally available in internet browsers on the market today.

Encryption at Rest

All files uploaded and shared through TitanFile are encrypted before being stored in our secure cloud environment. The file encryption uses algorithms and schemes that have been approved for encrypting and storing classified information up to the Top Secret level by all US government departments and agencies.

End-to-end Encryption

End-to-end encryption is a mechanism to encrypt files on the user's computer before they are sent to a service provider using encryption keys that are owned by the user. With end-to-end encryption, TitanFile does not have access to encryption keys and therefore is unable to decrypt client data.



Data Storage

Certified Data Centers

For data protection, continuity, and retention, TitanFile uses certified Microsoft Azure and Amazon AWS data centers. Our secure cloud infrastructure includes extensive security measures such as physical security, access control, 24x7 security monitoring and alerting. The infrastructure security has been certified by independent parties to meet compliance standards such as SOC 2 Type II and ISO 27001, and PCI DSS.

Custom Data Residency

TitanFile clients can choose where they want their data stored. We currently offer data residency in Canada, the United States, Europe, or on premise using the client's infrastructure.

Custom Data Retention

TitanFile clients can set their own data retention policy for files uploaded to TitanFile. When files have reached their expiry date, they will be automatically deleted from our servers.



Authentication

Single Sign-On (SSO) Integration

TitanFile allows single sign-on integration with ADFS, cloud providers such as Azure Active Directory and AWS Directory Service, and any third party provider that supports SAML2 or OATH. Enterprise users can use their corporate credentials to authenticate into the platform.

Two-factor Authentication (2FA)

TitanFile uses Two-step verification to add an additional layer of protection to confidentiality. 2FA can be enabled for both users and their recipients. It can be used to protect your account from a compromised password or to verify the identity of your recipients.



Governance & Compliance

ISO 27001:2013 Certified | SOC 2 Type II Compliant

To protect the confidentiality, integrity, and availability of information being managed, TitanFile follows guidelines recommended by the ISO 27001 and SOC 2 Type II standards.

Access Control

TitanFile gives users complete control over who has access to their information with the ability to add recipients to file sharing streams, and add and remove files at their own convenience.

Audit Logs

Comprehensive audit trails capture who did what, when, and where. User can export the audit trails for analysis and compliance.

Email Delivery Reports

TitanFile captures the response code from the recipient's email server, creating a reliable record that an email notification was in fact delivered to its destination. The delivery reports can be exported as a PDF document and used as a proof of delivery when needed.

Compliance

TitanFile and its infrastructure complies with:



ISO 27001:2013

International Organization for Standardization (ISO)



SOC 2 Type II

Service Organization Control



HIPAA

Health Insurance Portability and Accountability Act



PIPEDA

Personal Information Protection and Electronic Documents Act



PHIPA

Personal Health Information Protection Act



GDPR

General Data Protection Regulation



PCI DSS

Payment Card Industry Data Security Standard



WCAG 2.1

Web Content Accessibility Guidelines