Data Encryption Policy

Version number	4.0
Last Approved	Feb 25, 2025
Classification	PUBLIC

Overview 🔗

The Data Encryption Policy defines requirements for the use of various encryption technologies to protect client data and privacy and to ensure that encryption regulations are followed. The policy defines types of encryption to address *Data in Transit* and *Data at Rest* requirements.

Applicability 🔗

The applicability of this statement falls under purview of the 🔲 Security Documentation Overview .

Purpose 🔗

The purpose of this policy is to ensure that Personnel properly use encryption to secure confidential data that is:

- processed on, stored on, or transmitted through Company computers and network systems (including portable devices and removable media);
- under the custodial control of The Company.

Scope 🔗

The scope of this policy encompasses client data and confidential Company data. It defines all of the appropriate mechanisms and requirements for encryption.

Data in Transit 🔗

This section outlines the acceptable methods and key sizes for secure data transmission. Application or vendor requirements shall not result in the use of key sizes less than the minimum requirements stated in this policy.

Systems are not permitted to operate with expired encryption certificates or keys. Where encryption methods are used, the security requirements of the most sensitive data classification level shall prevail.

Transport Layer Security (TLS) 🔗

Servers must be configured to accept TLS v1.2 or higher. Exceptions require management approval and must be tracked.

The Company requires that all RSA and DSA keys for use with TLS be 2048 bits in length.

X.509 Certificate Generation 🔗

External Certificates 🔗

TLS/SSL utilizes X.509 certificates (colloquially known as SSL certificates) signed by a trusted Certificate Authority (CA).

X.509 CSRs must:

- Use a DSA/RSA encryption key of at least 2048 bits.
- Web certificates have a maximum expiration date of one year, other certificates have a maximum expiration date of 5 years.

Internally & Self-Signed Certificates 🔗

In some non-customer facing circumstances, we may use internally or self-signed certificates. Certificates for use on internal websites may be signed by the LTG Hosting Production CA.

These certificates must comply with the following requirements:

- Use a DSA/RSA encryption key of at least 2048 bits.
- Web certificates have a maximum expiration date of one year

> ❌ Internally signed certificates are prohibited for use in customer-facing environments.

Email 🔗

The nature of emailing carries with it the disadvantage that the sender loses all control of the sent data. Therefore, there are only limited situations in which emailing sensitive or confidential data is appropriate. If sensitive data must be emailed, steps must be taken to safeguard it.

Transport Layer Security (TLS) and email 🔗

Company email servers are configured for "opportunistic" encryption sessions for all email transmissions. This allows email messages to and from Company servers to be encrypted (if the receiving and sending email server is capable of TLS).

Transfer Protocols 🔗

Transfer of data must always utilize secure protocols such as the SSH protocol family.

No new clients can be configured to use an unsecure protocol and existing clients still utilizing an unsecure protocol must migrate to a secure protocol as soon as possible.

Secure Shell (SSH) Protocol Family 🔗

When utilized, SSH protocols must use version 2 or higher. Our policy prefers the use of public/private key pairs over credentials.

Key Management 🔗

Key management is the crucial element for ensuring the security of any encryption system. The Company's Encryption Key Management Policy is defined here.

Data at Rest 🔗

All storage used in the hosting of customer systems requires data at rest encryption with AES-256 or better.

Encryption of Back Up Media 🔗

Portable drives 🔗

Customers who require data transfers via physical media must provide encrypted media of the appropriate type, capacity, and form factor for the application.

Additional Information 🔗

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the ⊟ Security Documentation Overview .

Document control 🔗

> ℹ This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @angelina.kilmer @Paul Gordon	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History 🔗

Date	Author(s)	Version	Changes
Feb 25, 2025	@Art Machado @Paul Gordon @angelina.kilmer	4.0	Annual review
Nov 01, 2024	@angelina.kilmer	3.2	Changed Policy classification from Confidential to Public
Mar 13, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	3.1	Annual review
Jul 27, 2023	@John Cole	3.0	Annual review
Feb 23, 2023	@Sarah Zwicker (Unlicensed) , @Art Machado	2.9	Annual review + logo updated

Mar 24, 2022	@Sarah Zwicker (Unlicensed)	2.8	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) , @Art Machado	2.7	Title change for VP InfoSec, Annual Review (no major changes noted)
Mar 10, 2021	@Sarah Zwicker (Unlicensed)	2.6	Ownership change, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.5	Reformatting, policies linked
Jan 26, 2021	@John Cole	2.4	Annual Review, role title change
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.3	Ownership change