Encryption Key Management Policy

Version number	4.0
Last Approved	Feb 13, 2026
Classification	PUBLIC

Overview

The Encryption Key Management Policy defines the requirements used to control public and private encryption keys and defines their lifecycle, inclusive of creation, usage, storage, and deletion.

Applicability

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

Scope

This policy applies to all key-pair encryption performed within Company-hosted Client-facing systems and systems containing sensitive Company assets.

Encryption Key Management Policy

Encryption Key Lifecycle

An encryption key lifecycle includes all the phases associated with an encryption key between the time it is generated and it is destroyed. These include: key generation, key storage, key distribution and key destruction.

Encryption keys shall be stored inside a secure key store or automated Key Management System (KMS) throughout the lifecycle. The key store should:

- Store a key in encrypted format
- Associate a key to an owner
- Log access of key pair

Key Generation

Algorithms and key sizes to be used shall be compliant with industry accepted standards.

An encryption key shall not be used until a copy has been stored into a key store.

Key Rotation

Keys should have a stated life and should be changed on or before the stated expiry date.

The standard key rotation interval should be quarterly unless explicit justification for a longer interval is approved.

In the event of key compromise or the termination of personnel with key access, keys should be rotated.

Key storage

All encryption keys shall be stored in an secure key store. Keys should not be stored in plaintext format on operational storage (e.g. the hard disk of a server which uses the key for encryption/decryption), except for asymmetric public keys.

Keys must not be stored on the same media as the encrypted information.

All encryption keys must be regularly backed up so the Company could recover in the event of a corruption.

Key Distribution

Except for asymmetric public keys, all encryption keys shall be encrypted prior to distribution. Secrets and public/private keys must be distributed separately, e.g. no complete set of information using the same medium.

Key Destruction

Expired, decommissioned and compromised keys should be archived and retrieval restricted to a limited population.

Audit Logging

Key Management Audit Logs will be secured and retained in alignment with the requirements for other security logs and reviewed as appropriate to monitor compliance with this policy.

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 13, 2026`
Review cycle	`ANNUAL`	
Next review date	`Feb 13, 2027`	

Version History

Date	Author(s)	Version	Changes
`Feb 13, 2026`	Angelina Kilmer Paul Gordon	4.0	Annual review

May 16, 2025	Angelina Kilmer Art Machado	3.2	Clarified purpose & scope, as well as key rotation
Mar 3, 2025	Art Machado	3.1	Update to key rotation
Feb 25, 2025	Art Machado Angelina Kilmer Paul Gordon	3.0	Annual review
Nov 01, 2024	Angelina Kilmer	2.7	Changed Policy classification from Confidential to Public.
Mar 12, 2024	Art Machado, Sarah Zwicker, Paul Gordon	2.6	Annual Review + link updates
Jul 27, 2023	John Cole	2.5	Annual review + minor updates
Feb 23, 2023	Sarah Zwicker & Art Machado	2.4	Annual review + logo updated
Mar 24, 2022	Sarah Zwicker	2.3	Added Privacy considerations and components
Mar 16, 2022	Sarah Zwicker & Art Machado	2.2	Title change for VP InfoSec, Annual Review
Aug 10, 2021	Art Machado & Sarah Zwicker	2.1	Updated policy
Mar 11, 2021	Sarah Zwicker	2.0	Formatting changes, changing references to reflect LTG.
8/27/2020	Art Machado	1.9	Formatting changes. Completed annual review.