Encryption Key Management Policy

Version number	2.7
Last Approved	Mar 12, 2024
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 .

Purpose

The purpose of this policy is to outline The Company's standards for use of encryption keys so that they are used and managed securely, consistently, and appropriately in order to ensure privacy and protection of Company and customer data.

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.

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

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.

In the event a team member assigned to manage the encryption keys at The Company resigns, the keys should be rotated.

Audit Logging

Audit logs and records shall be reviewed at least annually.

Log retention shall be in line with The Company standard for log data archiving.

Additional Information

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

Document control

ⓘ 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 @Sarah Zwicker (Unlicensed) @John Cole	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 12, 2024
Review cycle	ANNUAL	
Next review date	Mar 12, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 01, 2024	@angelina.kilmer	2.7	Changed Policy classification from Confidential to Public.
Mar 12, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	2.6	Annual Review + link updates
Jul 27, 2023	@John Cole	2.5	Annual review + minor updates
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	2.4	Annual review + logo updated
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	2.3	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	2.2	Title change for VP InfoSec, Annual Review
Aug 10, 2021	@Art Machado & @Sarah Zwicker (Unlicensed)	2.1	Updated policy
Mar 11, 2021	@Sarah Zwicker (Unlicensed)	2.0	Formatting changes, changing references to reflect LTG.
8/27/2020	@Art Machado	1.9	Formatting changes. Completed annual review.