Encryption Management Policy

Overview

This document is for exclusive use by MSLA.

Version	Description [or description of changes]	Author	Creation date	Approved by	Date approval
1.5	Updated version	MSLA IT Department	10/21/2022	Luis Rios	10/25/2022

TABLE OF CONTENTS

Purpose

The purpose of the MSLA International Encryption Management Policy is to establish the rules for acceptable use of encryption technologies relating to MSLA Information Resources.

Audience

The MSLA International Encryption Management Policy applies to individuals responsible for the set up or maintenance of MSLA encryption technology.

Policy

- All encryption technologies and techniques used by MSLA International must be approved by MSLA International IT Management.
- MSLA International IT Management is responsible for the distribution and management of all encryption keys, other than those managed by MSLA International customers.
- All use of encryption technology should be managed in a manner that permits properly designated MSLA International personnel to promptly access all data, including for purposes of investigation and business continuity.
- Only encryption technologies that are approved, managed, and distributed by MSLA International IT may be used in connection with MSLA International **Information Resources**, other than those managed by MSLA International customers.
- MSLA International IT Management will create and publish the MSLA International Encryption Standards, which must include, at a minimum:
    - The type, strength, and quality of the encryption algorithm required for various levels of protection.
    - Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
- All MSLA International information classified as **confidential** must be encrypted when:
    - Transferred electronically over public networks.
    - Stored on mobile storage devices.
    - Stored on laptops or other mobile computing devices.
    - At rest.
- The use of proprietary encryption algorithms is not permitted, unless approved by MSLA International IT Management
- The use of encryption for any data transferred outside of the United States must be formally approved by MSLA International IT Management prior to transfer.

Waivers

Waivers from certain policy provisions may be sought following the MSLA International Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.