ENCRYPTION POLICY

Code: POL-TI-003
Revision: 01
Data: 28/02/2023

WWW.DMSLOG.COM

1. PURPOSE

The purpose of the rules on Information Security of DMS LOGISTICS. is to ensure the protection of its information assets against threats, internal or external, minimize any risks to information security, reduce exposure to loss or damage arising from security breaches and ensure that adequate resources are available, maintaining an effective security program and making its Employees aware of it.

Information is an asset and access to it must be managed appropriately to ensure that confidentiality, integrity and availability are maintained. Encryption of information and devices helps mitigate the risk of unauthorized interception, disclosure, and access.

DMS LOGISTICS uses encryption to protect data and information while stored, processed, and handled, protect user credentials, and enable secure communications.

This policy sets out DMS LOGISTICS' approach to cryptographic controls and management , and provides the requirements and responsibilities to ensure that information security and data governance objectives are achieved.

Encryption allows data to be secure so that it cannot be read by those who do not have the keys to decrypt it, providing confidentiality. Encryption allows levels of integrity and authentication to be achieved that ensure the security of data and information.

The General Data Protection Law (LGPD) requires companies to implement appropriate technical measures to protect the data in their possession, including data at rest and in transit. Encryption is a method that fulfills this function. It can serve to provide integrity to data that can be freely and publicly read, but must be transmitted and stored securely.

DMS LOGISTICS works to establish and continuously improve a corporate culture in Information Security, compatible with the acceptable use of information and the assets that support it, in order to minimize risks and create a safe environment for the performance of the Company's activities.

It must therefore be followed by all its Employees, regardless of the hierarchical level or function in the institution, as well as employment relationship or provision of services.

2. SCOPE

This Policy applies to:

All physical environments, including headquarters, branches, regional units, development units, processing centers and any others belonging to the heritage or custody of DMS LOGISTICS.

All computer environments and information activities owned or guarded by DMS LOGISTICS.

All employees, trainees, young apprentices and collaborators of any legal nature of DMS LOGISTICS.

All information processing systems used by DMS LOGISTICS that use encryption or that have to protect data must comply with the provisions of this policy.

3. PRINCIPLES

The basic principles of this Policy are:

The preservation of the image of the company and its employees;

The creation, development and maintenance of information and communications security culture;

That the level, complexity and costs of Information and Communications Security actions are appropriate and appropriate to the value of DMS LOGISTICS' assets, considering the impacts and the probability of occurrence of incidents.

The preservation of joint and several liability for data of other companies that travel in the assets of DMS LOGISTICS.

4. OBJECTIVES

4.1. THIS POLICY HAS THE FOLLOWING OBJECTIVES:

- Reduce information-related risks to appropriate and acceptable levels;
- Protect the confidentiality, integrity and availability of DMS LOGISTICS' assets, services and digital data;
- Ensure that company information is properly protected from theft or accidental loss of the device where it is stored;
- Ensure that company information is adequately protected when it is transferred from system to system;
- Observe the key themes of cyber resilience, which are: Identify, Protect, Detect, Respond and Recover;
- Establish minimum standards and responsibilities for the encryption of digital assets;
- Ensure that encryption is managed consistently and appropriately;
- Provide security to the owners of the information from which their information is protected.

5. POLICY

All encryption technologies and techniques used by DMS LOGISTICS must be approved by the company's Information Security Team. This Team is responsible for the distribution and management of all encryption keys.

All use of encryption technology must be managed in a manner that allows employees designated by DMS LOGISTICS to have prompt access to all data, including for the company's investigation and business continuity purposes.

DMS LOGISTICS' Information Security Equ will create and publish the encryption standards, which should include minimally:

● The type, strength, and quality of the encryption algorithm required for various levels of protection;

- Key lifecycle management, including key generation, storage, retrieval, distribution, end of utilization and destruction.

All DMS LOGISTICS information classified as confidential must be encrypted when it is transferred electronically or over public networks; stored on mobile storage devices; stored on laptops or other mobile computing devices;and when at rest.

DMS LOGISTICS' encryption policy provides for the adoption of measures for data in transit and at rest for its servers and systems.

Measures for data protection at rest may include:

- Full disk encryption;
- Full file encryption;
- Full application encryption;
- Full database encryption.

All systems use HTTPS certificates since authentication.

Encryption must be implemented using approved methods and technologies. Standards, algorithms, protocols, and encryption keys must meet acceptable standards. Ciphers, protocols, and algorithms that are not supported should be disabled where possible.

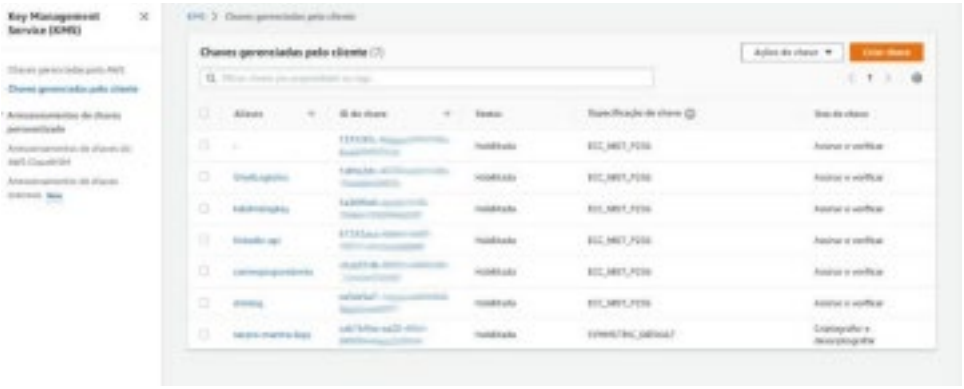
Encryption algorithms and specific implementations of algorithms may contain vulnerabilities. The use of algorithmic and encryption software must be monitored and managed through the Vulnerability Management Policy.

Systems, infrastructures, and applications and services should be configured to accept only connections that meet these requirements.

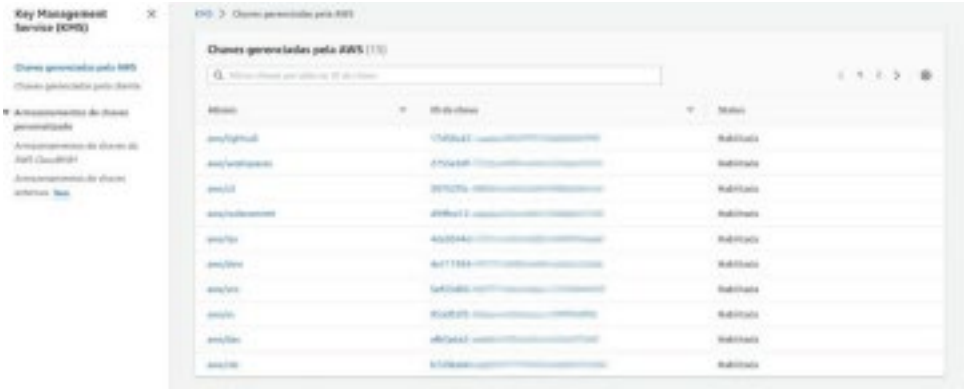
Cryptographic keys must be generated, stored, and managed in a manner that prevents loss, theft, or compromise. Access to cryptographic keys must be transmitted through reliable and secure methods to maintain confidentiality and integrity. Separate communication channels should be used for the transfer of keys and data. Under no circumstances should encrypted keys and data be transferred together by the same means.

Procedures and controls for revoking keys and certificates should be followed when they are compromised or expired.

By using the AWS cloud there is no computational delay or overhead in the implemented measures. Evidence of encryptions.
Evidence 1:



Evidence 2:



Monitoring encryption is done with the AWS tool, CloudWatch.

For developers there is the freedom to use the operating system that suits them, however it is mandatory that the HD's of desktops and laptops are encrypted.

6. KEYS

DMS LOGISTICS' encryption policy defines that thevid-a cycle of encryption keys passes in four general phases: pre-operational, operational, post-operational, and destruction.

In the pre-operational phase, the cryptographic material is not yet available for use, but is in the process of being created or activated.

In the operational phase the cryptographic material is available for normal use.

In the post-operational phase the cryptographic material is no longer available for normal use, but access to it is still possible in certain circumstances.

Finally, the fa. of destruction where the keys are destroyed, as well as all the records of their existence.

The management of encryption keys in the AWS environment is done by the AWS Key Management Service (KMS) solution, thus ensuring the integrity and reliability of the data. In a local environment, the keys are stored in a separate repository (dedicated email) and managed by the IT Director.

7. USERS

DMS LOGISTICS' encryption policy verifies a user's identity. Only after authentication can you use the authenticated user information on the system to set this user's authorizations.

The use of cryptographic keys is only allowed after the user has been identified.

Thus, for the proper management of the keys, the system must provide authentication and authorization mechanisms or allow the use of the keys in the existing systems.

8. EXCEPTIONS

Any exception to the requirements defined in this document must be justified, with risks being evaluated, documented and approved by the Information Security Team, in contact with the owner of the data.

9. IMPLEMENTATION AND UPDATE

The Encryption Policy – N2 of the DMS LOGISTICS system be updated whenever necessary or in an interval not exceeding 01 (one) year.

10. REVISION HISTORY

Revision	Data	Description
00	08/02/2023	Document creation.
01	28/02/2023	Document review and standardization

11. APPROVAL AND CLASSIFICATION OF INFORMATION

Prepared by:	CyberSecurity Team	
Reviewed by:	Leonardo Sabbadim	
Approved by:	Victor Gonzaga	
Level of confidentiality:	**X**	**Public Information**
		Internal Information
		Confidential Information
		Confidential Information

WE NEVER PUT QUALITY OR ETHICS AT RISK IN BUSINESS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM