HARDENING POLICY

Code: POL-TI-008
Revision: 01
Data: 24/02/23

WWW.DMSLOG.COM

1. PURPOSE

The Hardening Policy is a formal statement by DMS LOGISTICS regarding its commitment to the protection of the information assets owned and/or held by it.

Its main objective is to define the strategic guidelines to maintain the Security of Information and Communications, in order to preserve the confidentiality, integrity, availability and authenticity of the data and information produced, acquired, stored, in transit, discarded, owned or under the control or operation of the DMS LOGISTICS System.

It seeks to prevent threats, internal or external, minimize any risks, reduce exposure to loss or damage from security breaches, and ensure that adequate resources are available.

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. 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.

3. SCOPE

A Hardening 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 computational and active information environments belonging to or held by DMS LOGISTICS, which includes: computers; routers and switches; database.

All employees, interns, young apprentices and employees of any nature of DMS LOGISTICS must understand and follow the guidelines of this policy. Any changes in DMS LOGISTICS' systems and applications must follow the rules.

3.1. Normative References

This document was prepared on the basis of the recommendations proposed by ABNT NBR ISO/IEC 27001, clauses A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5, A.8.7, A.8.8, A.8.15, A.8.17, A.8.18, A.8.19, A.8.24, A.8.25, A.8.27, A.8.29, A.8.30, A.8.31, A.8.32, A.8.33 and ABNT NBR ISO/IEC 27002, clauses 5.8, 5.15, 5.16, 5.17, 5.18, 8. 2, 8.3, 8.4, 8.5, 8.7, 8.8, 8.15, 8.17, 8.18, 8.19, 8.25, 8.26, 8.27, 8.29, 8.30, 8.31, 8.32, 8.33, all recognized worldwide as codes of practice for the management of information security, as well as are in accordance with the Brazilian laws of law.

3.2. Hardening

Hardening is the procedure that aims to improve the infrastructure to face attempted attacks. It involves identifying vulnerabilities, mapping threats, actions to mitigate or minimize risks, and performing corrective activities.

Hardening involves user authentication, access authorization, audit log keeping, clock synchronization, and infrastructure access techniques. In addition to these actions, it also involves the maintenance of records of operations, system characteristics, such as maintenance of updated software and permission to be active only the resources actually used and configuration requirements such as maintenance of backups, for example. The non-implementation of this policy can have a significant effect on the efficient functioning of the organization, and it is therefore the obligation of all its employees, regardless of the hierarchy, to follow the guidelines mentioned in this document.

4. HARDENING PROCEDURES

4.1. Authentication

Authentication is the process that seeks to verify the identity of the user at the time the user requests access. ABNT NBR ISO/IEC 27000 defines authentication as the assurance that a claimed characteristic of an entity is correct.

- In DMS LOGISTICS, the basic procedures for authenticating users involve the following requirements:

- A user must be created for each active operator, disabling old accounts.
- A single standard administration account should not be used by different users;
- Access passwords must be strong;
- Passwords should not be stored in plain text;
- The Two-Factor Authentication (MFA) feature must be utilized.

4.2. Authorisation

It has the function of differentiating the privileges assigned to users who have been authorized to access the systems. It follows the principles of least privilege and need to know.

- All users of the DMS LOGISTICS System must obtain permission to access the equipment according to their work.
- The administrator password should not be provided to all users in order to mitigate accidents, malicious agents or without the necessary training to handle these resources internally.
- External devices, when connected to the DMS LOGISTICS network, must first be authorized by the IS department before being connected.

Users must be classified into a privilege group, functionality that is allowed on multiple systems.

4.3. Audit

The audit procedure is access to information related to users' utilization of infrastructure resources.

As basic procedures, the following are required:

- Keep track of each user with their respective permissions.
- Record user actions on systems.
- Classify the records with criticality level: Informational, Warning and Critical.
- Sort records into types: Documents, Logs, and Configuration Backup.
- Records must have the correct date and time.

4.4. Access

Access to network equipment must be done securely by following the following basic procedures:

- All equipment will be encrypted;
- All equipment has the Endpoint Protection solution;
- All equipment has a deadtime lockdown rule;
- Access to computational resources is through the AWS Identity and Access Management (AWS IAM) solution;
- Access is released according to the permitting policies defined in the AWS IAM platform;
- Permissions vary according to the role of the contributor;
- All activity performed within the platform is recorded and managed through AWS IAM, AWS CloudWatch, and AWS CloudTrail solutions;

4.5. Records

All logs obtained from network operation and configuration must follow the following basic procedures:

- The records will be configured with different levels of criticality;
- The logs will be stored securely within the AWS CloudTrail solution;
- Logs will have their integrity verified by the file integrity monitoring (FIM) feature built into the AWS CloudTrail solution;
- Date and time of the records are synchronized with the NTP.br.

4.6. Time Management of Servers

The DMS LOGISTICS system adopts Amazon Time Sync Service, a time synchronization service provided by the Network Time Protocol (NTP), which uses a fleet of redundant atomic and satellite-connected clocks in each region to provide a highly accurate reference clock. This service is available in all public AWS Regions for all instances running in a VPC.

We understand that time synchronization is critical because all aspects of managing, protecting, planning,and debugging a network involve determining when events occur. Time also provides a single frame of reference between all devices on the network. Without synchronized time, it is difficult, even impossible, to accurately

correlate log files between these devices. In addition:

Tracking security breaches, network usage, or issues that affect a large number of components can be nearly impossible if the timestamps in the logs are inaccurate. Time is usually the critical factor that allows an event on one node of the network to be mapped to a corresponding event on another.

To reduce confusion in shared file systems, it is important that modification times are consistent, regardless of the machine on which the file systems are located.

The Sarbanes-Oxley, BACEN and CVM security rules require precise date and time stamping, for such aspects the management of server schedules and services of the DMS LOGISTICS system is always verified and tested.

4.7. Patching

Operating systems have their own programs/software that may contain security flaws. To prevent this, operating systems and many software applications have periodic security patches, released by the vendor, that need to be applied.

This is because one of these flaws can allow a hacker to compromise a computer and, consequently, threaten the integrity of the DMS LOGISTICS network and all computers connected to it.

DMS LOGISTICS uses Microsoft Windows, Linux and IOS operating systems.

Patches related to them, whether security or critical in nature, should be installed as soon as possible.

Appendix B of this document is a description of the requirements to keep systems and software up to date in all IT systems managed and maintained by DMS LOGISTICS.

4.8. System

All new systems should follow the following recommendations:

- Do the installation following the recommendations of the supplier;
- Disable unused interfaces;
- Disable unused, insecure, recursive DNS, and NTP Server services.
- Remove or disable unused extra function packages;
- Disable neighborhood discovery protocols such as CDP, MNDP, and LLDP;
- Maintain the system always updated in the latest and stable version (LTS).

- Apply all security patches as per test validation and CVE verification.
- Scan for vulnerabilities. The vulnerabilities found should be fixed.

4.9. Container System

DMS LOGISTICS' protection process is ongoing. It is integrated into the development process and is automated to reduce human intervention.

Container security is an additional security measure that aims to protect DMS LOGISTICS processes. It aims to implement security tools and policies to ensure that everything in the DMS LOGISTICS container is working as intended, including infrastructure protection, software supply chain, runtime, etc.

For more details of this regulation, see Annex A - Container security.

4.10. Multi-Tenancy

DMS LOGISTICS uses a multi-tenancy architecture in its application to support multiple tenants at the same time.

DMS LOGISTICS adopts multi-tenancy to reduce the complexity of the software management process for its multiple customers. It increases security because, in case of an update, there is no risk of any customer not upgrading, because the instance of the software is unique.

The Multi-tenancy architecture provides separation between clients (tenants), where a shared instance of a software application installed on a server can serve multiple clients. Therefore, DMS LOGISTICS' customers have separate environments, and one cannot access the other's environment, ensuring security, high availability, reliability and scalability. Customers cannot access each other's data.

Customers can customize the settings for their environment, but they cannot access the application code.

5. SETTINGS

As configuration requirements, all assets must:

- Always keep an up-to-date backup of current settings.
- Maintain a hardening script of network machines.
- Keep the hardening script up to date: each new policy needs to be added to the script.

After following all these steps, the system can be used.

6. GENERAL PROVISIONS

Only software approved by the IS department will be allowed to connect to the DMS LOGISTICS System network.

Applications that are not required for the job should be uninstalled and removed.

Assets will be configured to prevent and block the execution of unapproved software.

All computers follow a default security configuration. If any changes are required, it must be evaluated and authorized by the IS department.

The default passwords must be changed after the software is installed.

The use of utility programs that can override the controls of systems and applications is prohibited. For more details, see the Network Management Policy.

Third-party suppliers should not receive any access to the DMS LOGISTICS network without prior permission from the IS department. Any improper alteration or access without permission must be reported immediately to the IS department so that it can be investigated and, if necessary, stopped.

Visitors should not have access to the DMS LOGISTICS corporate network.

To access the system, a request must be made to the Information Security department. Only after authorization and release by the Information Security department will it be possible to access the DMS LOGISTICS System.

All systems are accessed upon authentication. Each user must be duly identified by a unique and non-transferable identity, enabling them to be bound and held accountable for their actions within the organization.

It is up to the user to ensure that their ID and password are not used by third parties, preventing them from being used to obtain unauthorized access to DMS LOGISTICS systems.

You may not access or change network settings in any way. Any and all similar situations should be reported to the IS department.

Changes in the configuration of networks and systems must be made in accordance with the provisions of the Change Management Policy. The network infrastructure follows a set ofCISO-approved policies. Any change must be approved in advance by the CISO.

The use of removable media will be controlled. For more information, see the Mobile Device Policy.

7. PENALTIES

Failure to comply with the principles and guidelines of this and any other Security Policy of DMS LOGISTICS, its aggregate rules and procedures, subjects the offender to the penalties provided for by law and internal regulations.

8. IMPLEMENTATION AND UPGRADE

The Hardening Policy of the DMS LOGISTICS TICS system must be updated whenever necessary or in an interval not exceeding one (1) year.

9. ANNEX A - CONTAINER SECURITY

Container security is an additional security measure that aims to protect DMS LOGISTICS processes. She saw the implementation of security tools and policies to ensure that everything in the DMS LOGISTICS container is working as intended, including infrastructure protection, software supply chain, runtime, etc.

When protecting your containers, DMS LOGISTICS' main focuses are:

- The security of the container host;
- Container network traffic;
- The security of the application within the container;
- Malicious behavior within your application;
- Protect your stack from the container;
- The fundamental layers of its application;
- The integrity of your development pipeline.

9.1. Continuous Container Security

DMS LOGISTICS' protection process is ongoing. It is integrated into the development process and is automated to reduce human intervention. It should be extended to the maintenance and operation of the underlying infrastructure to the extent permitted by AWS.

It protects the build pipeline container images and the host, platform, and runtime application layers. Implementing security as part of the continuous delivery lifecycle is aimed at reducing DMS LOGISTICS' risks and vulnerabilities on an ever-increasing

attack surface.

This ongoing process is related to:

- Protection of applications and container pipeline.
- Protection of container deployment environments.
- Infrastructure protection.

9.2. Security in The Container Pipeline

Image Collection

Containers are created from file layers. The base image is the most important for security purposes because it is used as a starting point for creating derived images. With this in focus, only images from official or internally developed repositories are used.

DMS LOGISTICS, when collecting container images, verifies:

- Signature by reliable source;
- Updating the operating system layers and execution environment;
- Periodicity of container update;
- Identification and tracing of known issues;
- Access Management

Following the collection of the images, the dissemination of all container images used by the team and access to them begins. That is, protect the images downloaded and created. It makes use of a private registry to control access through role assignments, as well as manage content, assigning data to the container that provides information to identify and track known vulnerabilities, and automate and assign policies on stored container images.

From the access management, it is checked:

- Which role-based access control for container image management will be used
- Definition of application of tags to classify the images
- Visible metadata logging for known vulnerabilities
- Use logging to assign and automate policies

9.3. Security Testing and Deployment

The last step in the pipeline is deployment. At this point, after you complete the builds, they are managed and policies are automated to flag builds that have security issues,especially when encountering new vulnerabilities.

Next, component analysis tools are run that track and flag problems.

- By integrating security testing and automating deployment, you see:
- Avoid patching running containers
- Use triggers to rebuild and replace containers with automated updates

9.4. Infrastructure Protection

Another layer of container security is the isolation provided by the host operating system. The host operating system is activated through a container execution environment. It must be managed by an orchestration system.

DMS LOGISTICS, when deciding how to secure container infrastructure, provides:

- Which containers need to access others;
- How they detect the other containers;
- How to control access to shared resources and how to manage them;
- How to manage host updates;
- Need for simultaneous updating of containers;
- How to monitor the health of containers;
- How to automatically scale the capacity of applications to meet demand.

9.5. Implementation and Update

DMS LOGISTICS' Container Security must be updated whenever necessary or at an interval not exceeding one (1) year.

10. ANNEX B - PATCHING

The machines used in the DMS LOGISTICS environment have, according to the need of the function, three operating systems: Microsoft Windows, Linux and IOS.

Its principles and guidelines are:

- DMS LOGISTICS is responsible for maintaining the confidentiality, integrity and

availability of the data maintained in its IT systems on and off site, including systems and services provided by third parties but managed by the company.

- DMS LOGISTICS has the obligation to provide adequate and adequate protection of all its IT assets, whether physical, virtual, on-premises or in the cloud.

Patches are classified as shown in the tables below, according to the Microsoft severity rating system:

Classification	Description
Critical	They have vulnerabilities whose exploitation could allow the spread of viruses without user action.
Important	They have vulnerabilities that could compromise the confidentiality, integrity, and availability of user data or the integrity and availability of data processing capabilities.
Moderate	Patches whose exploit risks are significantly mitigated through default configurations, auditing, or making it difficult to exploit.
Low	They have vulnerabilities that are extremely difficult to exploit or have minimal impact.

10.1. Responsibilities

The Chief Information Officer is responsible for ensuring that the software update and Patching Policy are complied with.

Gerente de Serviços de TI is responsible for ensuring that software in scope is maintained through regular software updates and patches.

System owners are responsible for ensuring that all software in the scope they manage is maintained through regular software updates and patches.

DMS LOGISTICS' IT department is responsible for ensuring that all software in the scope they manage is maintained through software updates and regulatory patches.

DMS LOGISTICS' IT department is responsible for routinely assessing compliance with the Patching Policy and providing guidance to all stakeholder groups regarding security and patch management issues.

Third-party suppliers are responsible for ensuring that all software in the scope they

manage is maintained through regular software updates and patches, both before and during its operational deployment. When this is not possible, this should be escalated to the IT department of DMS LOGISTICS.

10.2. Guidelines for Software Update and Patching

- All IT systems, whether owned by DMS LOGISTICS or those in the process of development and support of third parties, must be properly licensed, with manufacturer's support and run updated and patched operating systems.
- Any IT system that is no longer licensed or supported by the manufacturer will be removed from the DMS LOGISTICS network.
- Third-party vendors must be prepared to provide evidence of updated patches before IT systems are accepted and begin to be operationalized.
- New systems must be upgraded to the current agreed baseline before they come online, to limit the introduction of new threats.
- Servers must meet the minimum recommended requirements that are specified by the IT department of DMS LOGISTICS, which includes: the standard operating system level; service packs; hotfixes and patching levels. All exceptions must be documented by the IT department of DMS LOGISTICS.
- Oncealerted to a new patch, IT administrators will download and review the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.
- The tests will be carried out using a test system that approximates the production systems. Where there is no test system, patch results from another non-key production system will be used and the results of any patch will be closely monitored for adverse effects.
- A count/backup plan that allows you to return to previous job settings must be in place before any upgrade.
- Systems that are removed from the network for lack of patching will only be reconnected when it is proven that they have been updated and do not pose any further risk to the DMS LOGISTICS network.
- If a critical or security-related patch cannot be centrally deployed by IT, it must be installed in a timely manner, using the best available resources.
- Failureto configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch and/or software management protections is expressly prohibited and constitutes a violation of policy.

10.3. Settings of The Environment The Operacional

All configurations related to the operating environment of DMS LOGISTICS are made through Puppet and versioned in Bitbucket, with this we can ensure that all machines are running the same versions of the software thus avoiding theiferenças between the productive environments.

Puppet is also used for the application of patch patches of the services that are managed by it respecting the following flow:

- The upgrade is done in the development environment
- Tests are performed to verify that this update has not caused any problems in the application. Patch must be scheduled in production
- The monitoring of security patches should be done by subscribing to the list of security announcements of Ubuntu (https://lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce) and Debian (http://www.debian.org/MailingLists/subscribe), as well as following the list of Debian updates - https://www.debian.org/security/. Amazon Linux 2 updates security bulletins and privacy events through Amazon Linux Security Center (ALAS) - https://alas.aws.amazon.com/alas2.html

10.4. Implementation and Update

The patching regulations of DMS LOGISTICS must be updated whenever necessary or in an interval not exceeding 01 (one) year.

11. REVISION HISTORY

Revision	Data	Description
00	09/02/2023	Document creation.
01	24/02/2023	Review and standardization of the entire document.

12. 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