ACCEPTABLE USE OF ASSETS POLICY

Code: POL-TI-001
Revision: 01
Data: 13/03/2023

1. PURPOSE

The Asset Use Policy sets out rules and criteria for accessing, using and monitoring DMS Logistics' technology assets.

The objective is to ensure the protection of DMS Logistics information assets against internal or external threats, minimize any risks to information security, reduce exposure to loss or damage resulting from security breaches and ensure that adequate resources are available, maintaining an effective security program and making its employees aware of it. Its application protects employees, customers, suppliers and the corporate environment from illegal and/or harmful actions, intentional or not.

DMS Logistics aims to establish a corporate culture in 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.

This Policy seeks to ensure the proper and correct use of office assets, including internet, internal network, physical equipment (hardware), software and technology resources in general. These assets are intended for use related to DMS Logistics' business activities in the activities of your business.

In addition, it seeks to enable asset management, from an integrated view of its life cycle and taking into account the risks and cost optimization to achieve the maximum effectiveness, contributing sustainably to achieve the goals and objectives of the company.

2. SCOPE

The Asset Use 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, regardless of geographical location;
- The rules and guidelines apply to all employees at all hierarchical levels of the company, visitors and to third parties who have contact with information produced within the scope of their actions. It is essential to note that the provisions are applicable to all possible formats of processing of personal data, whether digital or physical means.

- It is the responsibility of all stakeholders, employees, stakeholders and users to know these guidelines and adopt the following recommendations.

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 security culture;
- That the level, complexity and costs of Information 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 sole responsibility for data from other companies that travel in the assets of DMS Logistics.

4. GENERAL GUIDELINES

4.1. RESPONSIBILITY AND COMMITMENT

Inappropriate use of assets can compromise DMS Logistics' security, exposing it to external attacks, network compromise, systems, equipment and legal problems.

Employees, trainees, young apprentices, customers, suppliers and all who, in any way, provide services, have a partnership or use, for any reason, the assets and systems of DMS Logistics, in any function or hierarchical level, are co-responsible for the protection and safeguarding of the assets and information to which they are users and the environments to which they have access, independent of the security measures implemented by the security management officers.

The following are responsible for DMS Logistics' assets:

Information Security Manager

- Monitor, supervise, guide and approve the configuration of equipment, tools and systems granted to employees with all the necessary technical controls to ensure the security of data, systems, assets and personal information;
- Ensure that everyone has access to and knowledge of this Policy and other Information Security norms and standards.
- Supervise the procedures provided for in this Policy.

Collaborators

- Comply with and ensure the materialization and effective implementation of this Policy;
- Notify the Information Security Manager in case of loss, theft, inappropriate use of assets, data, information, equipment or non-compliance with the provisions of this Policy.

4.2. ACCESS CONTROL

Access to DMS Logistics' systems is controlled and granted only to authorized employees and visitors.

Access permits should be granted on the basis of the principles of need to know and least privilege for the performance of professional activities.

The Directors, collaborators and third parties are responsible for the use and confidentiality of their access credentials. It is not allowed, in any case, to share, reveal the u make unauthorized use of credentials of third parties, being directly responsible for the conduct and / or damage caused, upon determination of responsibility in administrative disciplinary proceedings duly instituted.

Access can be monitored, registered,or blocked without notice.

4.3. OWNERSHIP AND USE OF ASSETS

All data, code and information collected, created, processed and stored, whether in a cloud environment or on physical devices, are the property of DMS Logistics.

The use of DMS Logistics' assets is directed towards the execution of the company's business objectives. The equipment, data and information must be used only for this purpose, being expressly forbidden the use of personal data and information, whether of employees, customers or third parties for other purposes.

Access to the Internet is allowed, according to specific rules, treated in its own topic in this Policy. It establishes the rules for its access and use in the corporate environment.

4.4. GUIDELINES ON THE USE OF ASSETS

The installation of equipment, computer resources, systems and services for use in the network or in the premises of DMS Logistics is controlled and allowed by formal authorization, granted by the Information Security manager.

- DMS Logistics may deploy monitoring systems on workstations, servers, e-mail, internet connection, mobile or wireless devices and other network components – the information generated by these systems may be used to identify users and their accesses made, as well as mani jumped material;

- 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. To Cease the system, a request must be made to the Information Security department. Only after authorization and release by the Information Security department, it will be possible to access the DMS Logistics System.
- Each user must be fully 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.

Ensure that the devices of your responsibility are properly locked during your absence. The equipment will be blocked after a 10-minute inactivity. However, whenever the user leaves their workstation , it will be blocked;

Do not leave login and password exposed;

Passwords should not be left on sticky notes pasted on or under the computer , nor can they be left written in an accessible place;

Access passwords must be strong;

Passwords are not stored in plain text;

The Two-Factor Authentication (MFA) feature must be utilized.

- Installation and execution of unauthorized software is not permitted.

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

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

Do not under any circumstances lend or share your access credentials. Giving access to third parties not authorized by the IS Manager is strictly prohibited. The act's practice will be the responsibility of all those involved, being subject to the administrative and criminal sanctions applicable both to the holder of the credentials and the one who uses them improperly.

External devices, when connected to the DMS Logistics network, must first be authorized by the SI Manager before being connected.

Users must be classified in a privilege group, with access only to the functionalities necessary for the execution of their work, based on the principles of need to know and least privilege.

All permissions and methods of access must be requested via open ticket and registered in Jira, and previously analyzed and authorized by the DMS Logistics Tecnologia team.

Users should be vigilant before opening attachments sent by email, especially those that are promotional or sent by strangers.

4.5. INTERNET USE

The use of the Internet service must be in accordance with predefined profiles, respecting the storage of the information and its authenticity.

Corporate email, instant messaging, intranet, and Internet services should be used in the activities of interest to DMS Logistics.

Colaboradores and authorized visitors will be able to use the internet connection to:

- Perform work tasks
- Do research and collect information that can improve your work

4.6. INTERNET ACCESS PROFILES

Employees and visitors who use the DMS Logistics connection must access the System with their corporate accounts with the use of secure and authorized devices.

One should always use strong passwords, with the use of letters, numbers and special characters .

The following profiles are established for Internet access:

Standard: Allows access to all Internet sites, including those that serve material containing audio and video, social networks and blogs.

All employees of DMS Logistics, apprentices and trainees must be registered in the "Standard" profile.

Investigation: Allows unrestricted access, on a temporary basis, to all Internet sites. The profile "Investigation" may be assigned to an employee by formal act to act in processes of Treatment and Response to Incidents in Computer Networks.

- The access report must be included in the document that makes up the result of the investigative process.
- The term of validity of the attribution of this profile will be the same defined for the conclusion of the investigative process.

4.7. RESTRICTIONS AND CONDUCT

It is possible to apply to all access profiles, except for the "Investigation" profile, access and navigation to:

- Sites that contain pornographic or obscene material;
- Sites that contain illegal material;
- Game sites;
- Sites that pose a risk to Information Security.

The following ducts are prohibited when using the Internet:

- Engage in activities that are contrary to the interests of DMS Logistics, that violate its Policies or the legislation in force in the country;
- Practice acts of commercialization of products, for their own benefit or that of third parties, that are not of interest to DMS Logistics;
- Violate personal, copyright and/or intellectual rights, reveal industrial and/or trade secrets, make copies or disseminate source code, infringe patents, install or distribute "pirated" or other software that is not licensed for legal use by DMS Logistics;
- Copy, use, share or disclose personal data of employees, stakeholders without express authorization of DMS Logistics;
- Practice acts of invasion of accounts and devices of third parties, whether individuals or legal entities;
- Use the assets of DMS Logistics for involvement in criminal activities such as illegal hacking, fraud, purchase/sale of illegal goods and services, practice of terrorism, pornography, pedophilia or participation in religious movements, political or or any extremist bias;
- avail themselves of resources or devices for access to computers or networks external to DMS Logistics for the purpose of obtaining unauthorized information or causing the interruption or degradation of network services;
- Use a modem or network device that connects DMS Logistics' internal network to other networks or to the Internet;
- Visit potentially dangerous websites that could compromise devices or network access;
- Download files or programs from the Internet that are contrary to the guidelines of this or other DMS Logistics Policies.
- Download movies, music, magazines, books, software and other materials that are copyrighted by third parties.

- In addition, employees are prohibited from usingDMS Logistics' electronic belt for the following activities:
- Send unsolicited messages to multiple recipients, except if related to legitimate use of the Company;
- Send an e-mail message from the address of your department or using another person's username or e-mail address that you are not authorized to use;
- Send any message by electronic means that makes its sender and/or DMS Logistics or its units vulnerable to civil or criminal actions;
- Disclose unauthorized information or screenshots, systems, documents and the like without express and formal authorization granted by the owner of that information asset;
- Falsify address information, tamper with headers for and hide the identity of senders and/or recipients, in order to avoid the punishments provided;
- Delete pertinent e-mail messages when any of DMS Logistics' units are subject to some kind of investigation.
- Produce, transmit or disseminate a message that:
- Contains any act or provides guidance that conflicts with or is contrary to the interests of DMS Logistics;
- Contain electronic threats, such as: spam, mail bombing, computer viruses;
- Contain files with executable code (. exe, .com, . bat, . pif, . js, . vbs, . hta, . src, . cpl, . reg, . dll, . (inf) or any other extent posing a safety risk;
- Seek unauthorized access to another computer, server, or network;
- Aim to disrupt a service, servers, or computer network through any unlawful or unauthorized method;
- Aim to circumvent any security system;
- Aim to secretly surveil or harass another user;
- Aim to access confidential information without explicit authorization from the owner;
- Aim to improperly access information that may cause harm to any person;
- Include encrypted or otherwise masked images;
- Contains attachment(s) greater than 15 MB for sending (internal and

internet) and 15 MB for receiving (internet)

- Has content deemed inappropriate, obscene or illegal.

It is forbidden:

- Install or remove software from DMS Logistics equipment without prior authorization from the IS Manager;
- Prevent or disable any software or hardware update recommended by the Information Security team;
- Install, uninstall or enable any software or hardware, rendering it totally or partially inoperable;
- Perform any type of maintenance on the office equipment without the help of the responsible area;
- Change the network settings and the Integrated Input and Output System - BIOS of the machines, as well as make any changes that may cause any future damage;
- Compromise equipment belonging to DMS Logistics, for improper use or intentionally ;
- Make vulnerable the security of portable computer assets, among them, external HD, notebook, data show, pen drive;
- Take any conduct that compromises the security of DMS Logistics' network or computer equipment;
- Spoofing addresses and/or login accounts in order to hide from DMS Logistics' security systems;
- Gain unauthorized access to any server, network, or account by bypassing security systems in order to gain improper access or privileges;
- Share, without prior authorization, documents or files with third parties;
- Prevent the full and proper functioning of the assets by changing parameters and configurations of the software;
- Use or propagate software such as viruses, Trojan horses, keyloggers, or programs that control other computers through the courses provided by DMS Logistics.

4.8. MONITORING

To guarantee the rules mentioned in this Policy, DMS Logistics. reserves the right to:

- Deploy monitoring systems on corporate devices, e-mail, Internet connections, and other network components. The information generated by these monitoring systems can be used to identify users and their accesses made;
- Inspect files that are on the internal network or on the corporate device, in order to ensure strict compliance with this Policy.

The routine verification of the application of the protocols provided for in this policy and those present in the information security policy, will occur every six months involving the people and organizations linked to DMS Logistics, through the provision of signature of binding terms and training, among other appropriate measures.

By making use of the assets provided by DMS Logistics or acting on its behalf, employees agree to the provisions related to information security and related documents, being aware that their acts may be monitored by the responsible area and the IS Manager.

4.9. EDUCATION AND AWARENESS

This Policy and its aggregated documents must be disclosed to create and maintain a corporate culture in Information and Communications Security. In order to reduce risks to information security, all employees should be informed about the appropriate and safe use of technological resources and DMS Logistics information to which they have access.

It is the responsibility of employees, trainees and young apprentices to know and comply with the guidelines, rules and actions defined by this Policy, as well as by its aggregate rules and procedures.

4.10. VIOLATIONS AND PENALTIES

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

4.11. UPDATE

The Asset Use Policy must be updated whenever necessary or in an interval not exceeding one (1) year.

5. ANNEX A - RULES FOR THE USE OF MOBILE DEVICES (BYOD)

Mobile devices such as smartphones, tablets and computers are important tools for DMS Logistics in its corporate activities. However, they can pose a significant risk to data security when, without the adoption of security applications and procedures, they are used as a channel of unauthorized access to company data and its

technology infrastructure. This can lead to data leakage and infection of systems.

Therefore, DMS Logistics has requirements to protect its information technology resources, in order to protect its customers, its intellectual property and its reputation. This document sets out a number of practices for the safe use of mobile devices and applications.

5.1. SCOPE

This regulation 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 assets and information assets owned or held by DMS Logistics;
- All employees, trainees, young apprentices and collaborators of any legal nature of DMS Logistics.
- All mobile devices, whether owned byDMS Logistics or its employees, including smartphones, tablets and computers that have access to the company's networks, data and systems. The list includes, but is not limited to:

A. Desktops, notebooks, tablets;

B. smartphones;

C. Memory cards, pen-drives;

D. External hard drives.

- Apps used by employees on their personal mobile devices that store or access corporate data, such as cloud storage, communication, and instant messaging apps.

5.2. USE OF MOBILE DEVICES

DMS Logistics does not provide mobile devices such as mobile phones and tablets to its employees. The model adopted for this situation is BYOD (Bring Your Own Device). However, we authorize the use of the applications listed below, with due monitoring and auditing, without, however, violating the privacy of the natural person of our employees, following the guidelines of Law No. 12,965/2014 (Marco Civil da Internet). Its use should be in line with:

- DMS Logistics' Information Security Policy;

- Confidentiality Agreement signed by the employee;

Regras para BYOD - Bring Your Own Device

Prior to its first use in any DMS Logistics network or IT infrastructure, every mobile device must be registered with the IS Team. DMS Logistics will maintain a list of all devices approved for use.

Devices that are not registered and approved will not be able to be connected to the company's technology infrastructure. If any user's preferred device is not on the list, it should be requested to be added to the IS Team.

The connectivity of all mobile devices will be managed by the DMS Logistics IS Team. While the team will not be able to monitor all external devices – such as laptops, tablets or personal smartphones – that may require connectivity to the company's networks,users are expected to adopt the same security protocols when using devices that are not owned by DMS Logistics.

5.3. TECHNICAL REQUIREMENTS

- Devices should use the most up-to-date operating systems to ensure that they have the latest security updates;
- Devices must store all passwords saved by the user in a password encryption tool;
- Devices must be configured with secure passwords and that they comply with the security instructions for passwords. Passwords may not be the same as those used in other credentials within the company;
- Only devices authorized by IT Staff will be allowed to connect directly to the internal corporate network.
- Devices will be subject to compliance rules regarding security issues, such as encryption and passwords, established by IT Staff.

5.4. USER REQUIREMENTS

- Users should upload to their devices only data that is essential to their corporate activity;
- If the user suspects unauthorized access to company data through their mobile devices, they must report the incident immediately to the IT Team, in accordance with the established procedures;
- Users should not install pirated software or illegal content on their devices;

- Apps should only come from official sources and platforms. If an application comes from a trusted source, the user should contact IT Staff.
- Users should check weekly and update at least once a month the systems and apps on their devices.
- Devices are not connected to computers that do not have up-to-date and enabled anti-malware, or that do not meet DMS Logistics requirements.
- Devices must be encrypted according to company standards.
- Users should be cautious when jointly using personal and corporate accounts on their devices. They must ensure that company data is sent only through corporate email.
- All users must ensure physical security measures of the devices, however they are in their possession and while they are momentarily out of their reach.

The above requirements may be checked regularly and if any device is not in accordance with the established requirements, it may result in loss of access to the company's tools and networks, as well as cleaning of corporate data within the provisions.

Users should not attempt to modify or disable the security settings applied by IT Staff for device use

The IS Team reserves the right to refuse the connection of any mobile device to the networks and technology infrastructure of DMS Logistics. This measure will be adopted whenever the IT Team realizes that the devices are being used in a way that puts systems, users, data and customers at risk.

Cases not covered by this document will be submitted to risk assessment and to the Information Security Steering Committee of DMS Logistics.

5.5. CORPORATE TOOLS WITH PERMITTED USE ON EMPLOYEES' MOBILE DEVICES:

- GSuite
- Discord
- WhatsApp

5.6. GSUITE

- Google's suite of corporate tools.
- Gmail - Corporate Email
- Drive - File storage and sharing
- Hangouts / Meet - Video Conferences (Virtual Meetings)
- Calendar - Agenda of active appointments

In case of theft and/or loss of the employee's mobile device, the information security department is triggered, and one of the members of this department will remove the data from the employee's mobile devices.

It should be noted that only DMS Logistics data contained in GSuite applications will be deleted. More information in https://support.google.com/a/answer/7542661?hl=pt-BR.

Another action taken immediately in this type of incident will be the reset of the corporate email password. The employee must register a new password and reconfigure the MFA (Multi-Factor Authentication) mechanism. MFA is mandatory for all DMS Logistics corporate emails.

Below is evidence of the process of remote administration of DMS Logistics' GSuite resources:

EVIDENCE REQUESTED FROM DMS LOGISTICS ON 02/15/2023 .

5.7. DISCORD

Discord is used by employees for general communication between teams, without the traffic of sensitive data.

5.8. WHATSAPP

All of the employees went through Information Security Workshops, where they were instructed and guided individually how to keep their WhatsApp more secure, following the security directives of WhatsApp (https://faq.whatsapp.com/ pt_br/general/26000245), such as:

- Enabling the two-step confirmation code to add an extra layer of security to your account.
- Set an authentic email address to reduce the risk of being denied access to your account if you forget your PIN (https://faq.whatsapp.com/ pt_br/general/26000021).
- Never share the six-digit confirmation code with anyone, not with people you know or organizations you trust.

- Set a PIN to protect your phone.

Whatsapp is a means of communication of DMS Logistics employees and in case of loss or theft of the employee's mobile device, it is temporarily removed from the WhatsApp groups that he is part of that have some link with DMS Logistics.

5.9. IMPLEMENTATION AND UPGRADE

This standard shall be updated whenever necessary or at an interval not exceeding one (1) year.

6. FINAL PROVISIONS

For DMS Logistics, privacy and trust are fundamental to our relationship with you. We are always updating ourselves to maintain the highest safety standards.

Therefore, our Acceptable Use of Assets Policy may be changed at any time. Thus, one should be aware of the published updates.

By continuing with the use of assets, you agree to our Acceptable Use of Assets Policy.

If you have any questions, please contact us through the channel: (email)

This Acceptable Use of Assets Policy was last updated on February 28, 2023.

7. REVISION HISTORY

Revision	Data	Description
00	28/02/2023	Issuance of the document.
01	13/03/2023	Review and standardization of the document.

8. 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