VULNERABILITY MANAGEMENT POLICY

Code: POL-TI-007
Revision: 01
Data: 28/02/2023

1. INTRODUCTION

Technological advancement has brought great benefits to institutions and information is one of the most critical assets. On the other hand, information security incidents have become one of the major problems for the area of Information Security and Communications.

Therefore, there is a need to ensure solutions to prevent the impacts caused by incidents and one of the preventive actions is linked to the management of vulnerabilities of the assets that support the systems and network infrastructure. Vulnerabilitymanagement takes into account the likelihood of an information security incident occurring when a vulnerability is exploited.

Technical Vulnerability Management aims to take DMS LOGISTICS to the level of maturity of security processes, minimizing the impacts on the business.

The storage and processing of personal data is a potential vulnerability. Therefore, the regulation of Annex A brings how risks must be managed, evaluated and treated.

Annex B brings the retention and disposal deadlines adopted by DMS LOGISTICS.

2. TARGET AUDIENCE

This Policy targets all DMS LOGISTICS employees.

3. OBJECTIVE

The purpose of this document is to establish vulnerability management practices and impact assessment capable of proactively preventing the exploitation of any vulnerabilities and potential loss of data of DMS LOGISTICS.

DMS LOGISTICS creates and documents systematic practices, in a transparent manner, to maintain control programs, assess the vulnerability of new software or hardware, and mitigate other technical and non-technical vulnerabilities.

The objective of this initiative is to implement greater protection of SIC resources, ensure best compliance practices and reduce the impact of threats to DMS LOGISTICS and the information under its tutelage.

4. CONCEPT

The technical vulnerability management process is the set of coordinated activities that aims to reduce to acceptable levels the security vulnerabilities found during the "Security Analysis" or "Vulnerability Analysis" process in a given asset, set of assets or environment.

It establishes rules for the mapping, monitoring, verification and review of systems.

The technical vulnerability management process is presented in the ABNT NBR ISO/IEC 27002 standard.

5. BENEFITS OF IMPLEMENTATION

It is possible to list several benefits of implementing the vulnerability management process, such as:

- Knowledge of the environment;
- Support in the process of Software and Hardware Inventory (responsibility for activities);
- Transparency;
- Clear information about each asset and what needs to be implemented;
- Assistance for decision making;
- Prioritization of actions.

6. NORMATIVE REFERENCES

- ABNT NBR ISO/IEC 27001:2022 – Information Technology – Security Techniques – Information Security Management Systems – Requirements;
- ABNT NBR ISO/IEC 27002:2022 – Information Technology – Security Techniques – Code of Practice for Information Security Controls;
- ABNT NBR ISO/IEC 27005:2019 – Information technology — Security techniques — Information security risk management;
- ABNT NBR 16167:2020 – Information Security – Guidelines for classification, labeling and treatment of information;
- BACEN Resolution 4658/18
- ABNT NBR ISO/IEC 31000: 2018 - Risk Management
- General Law on the Protection of Personal Data (LGPD), Law No. 13.0709/2018

7. THE VULNERABILITY MANAGEMENT PROCESS

The process of managing technical vulnerabilities is carried out with the monitoring of the environment and is segmented into several steps, as demonstrated below:

- Notification of those responsible;
- Definition of the scope to be analyzed;
- Notification of those responsible and scheduling of analyses;
- Execution of analyses;
- Consolidation of data (classification and validation of analysis results);
- Mitigation process;
- Validation of the environment (new cycle and/or retest);
- Release of the environment;
- Preparation of reports;
- Final report;
- Ending.

8. USO DE ENDPOINT PROTECTION

All DMS LOGISTICS equipment that has access to the system must use the endpoint protection approved and used by the company.

The solution currently in use is CrowdStrike Falcon Endpoint Protection Pro.

Changing or disabling endpoint protection software is prohibited. Only the IT area, after analysis of the Information Security team, can take any action in this regard.

All files received through external networks or storage devices must be scanned for malware before use.

The corporate email service has predetermined anti-spam and anti-malware rules on the service's server, and in addition, all attachments that are saved on the local computer are scanned by the installed Endpoint Protection solution.

Suspicious emails and content will pass through quarantine to prevent dissemination to DMS LOGISTICS' email system or networks. Suspicious emails should be reported to the IS area of DMS LOGISTICS, so that the appropriate protection measures can be taken.

If the user suspects suspicious activity or unreliable emails, he/she must follow the procedures described in the Non-Compliance Treatment and Incident Management Policy (POP-SGI-002).

All employees need to follow the rules for the safe use of email. In case of suspected phishing or any other suspicious activity should be reported immediately to the

Information Security Team. The employee who identified the suspicious activity must complete the forms in Annexes A and B in the Incident Management Policy and follow the procedures described therein (see Incident Management Policy).

All files received from a source external to the DMS LOGISTICS System must be scanned for viruses and malware before opening and using.

Any device not owned and not authorized by DMS LOGISTICS, when connected to the organization's network, can compromise and bring damage to the security of the network. In order to mitigate this risk, a specific authorization must be obtained from the IS department prior to any connection to the IS network.

Any detection of viruses and malware that is not automatically identified and quarantined by endpoint protection constitutes a security incident and needs to be reported to the Information Security Team through the Security Incident Reporting Form

The Information Security Team shall maintain and update a database with the vulnerabilities found and reported, as well as the initiatives taken to remedy them, as a tool of control and transparency.

9. MONITORING AND ALERTING

DMS LOGISTICS adopts solutions and tools to protect the Confidentiality, Authenticity and Integrity of the data and assets of the DMS LOGISTICS System, in order to protect you against unauthorized transfer, modification or breach of confidentiality, in accordance with the guidelines of the General Data Protection Law and good market practices.

For this, the DMS LOGISTICS system uses the systems listed below:

- AWS GuardDuty
- AWS CloudWatch
- AWS CloudTrail
- AWS Trusted Advisor
- NewRelic

These tools, described in the Network Management Policy, are the equivalent of a SIEM.

To this same end, users should only be granted access to the network and network services that they have been authorized to use. All permissions and methods of access must be requested by call registered in Jira, and addressed to the Information Security Manager of DMS LOGISTICS. For more details, see the Network Management Policy.

All systems are accessed through authentication and each user must be duly identified by a unique and non-transferable identity, allowing them to be linked and held accountable for their acts within the organization.

10. PATCH MANAGEMENT

The DMS LOGISTICS Information Security Team has full responsibility for the implementation, operationalization and procedures of patch management.

All information resources are regularly monitored to identify available updates. The delay in updating operating systems or platforms represents a vulnerability to the company's information resources, so that the scanning and implementation of existing updates must be carried out within an acceptable period that represents the least risk to the integrity of the company.

Software upgrades and system configuration changes must be tested before being widely applied and adopted in DMS LOGISTICS devices, and must be conducted in accordance with change control guidelines.

In this same sense, the Information Security team performs and maintains an inventory of information technology resources to register the brands, models and versions of its hardware, as well as the operating systems, databases, servers and other software used by the company. This inventory is updated annually or whenever there are changes. It is found in Appendix B of the Acceptable Use of Assets Policy.

11. PENETRATION TESTS (PENTEST)

Penetration tests of internal and external networks will be conducted at least annually or after significant events and changes in the security environment, and may be performed at any time if a need is identified.

The Company may hire a third-party company to do so. After conducting this process, the Information Security Steering Committee shall discuss the treatment options to be adopted, considering the selection of controls to maintain the risks within limits acceptable to the Company, considering the possible financial, operational and reputational impacts in case of a security event, as well as the probability of the event happening.

All vulnerabilities identified during penetration testing will be patched , followed by further testing to verify that the vulnerabilities have been successfully patched.

12. VULNERABILITY AWARENESS AND TRAINING

Awareness campaigns will be carried out for all DMS LOGISTICS employees, as well as training on best practices for the use of software and hardware owned by the company or externally, aiming at protection against vulnerabilities. This measure aims to contribute to the creation, development and maintenance of a culture of information security and communications within the company, as expressed in the Security Policy.

13. TEAM CHOICE

The choice of the team responsible for the execution of the process with regard to the analysis and scanning activities may vary, according to the need.

14. TERMINATION OF VULNERABILITY MANAGEMENT POLICY

After the full restoration of essential technological systems and resources, everyone should be communicated, including guidance on what care should be taken to avoid recidivism.

All information regarding the vulnerability event should be collected and analyzed in order to make the Business Continuity Plan more robust with the knowledge acquired according to ABNT NBR ISO/IEC 27001, control 5.27 Learning from information security incidents.

15. PENALTIES

Failure to comply with the rules contained in this Vulnerability Management Policy subjects the offender to the penalties provided for by law and in the internal regulations of DMS LOGISTICS.

16. IMPLEMENTATION AND UPDATE

It is recommended that the program and its activities be reviewed every six months, or as described in the company's regulatory system, not restricted only to these. If an interested party identifies an improvement, it should be implemented as soon as possible.

17. ANNEX A - RISK MANAGEMENT

Discovering vulnerabilities in a timely manner is important, but being able to estimate the risk associated with the business is just as important.

Early in the life cycle, one can identify security issues in the architecture using threat modeling. Subsequently, we can find security issues using code review or penetration testing.

With this approach it is possible to estimate the severity of all these risks to the business and make a decision based on these risks. Having a risk management will save time and eliminate the discussion about priorities. This system will help DMS LOGISTICS to take the appropriate measures taking into account the severity of the risk, whether minor risks or more serious risks, all will be taken care of.

17.1. APPROACH

There are several different approaches to risk analysis. The OWASP approach presented here is based on standard methodologies and is customized for application security. A normal risk model is presented below:

Risk = Probability * Impact

In the sections below the factors that make up "probability" and "impact" to the security of the application are discriminated against.

17.1.1. IDENTIFY A RISK

The first step is to identify the security risks that must be assessed. The analyst needs to gather information about the threat agent involved, the attack that will be used, the vulnerability involved, as well as the impact of a successful exploit on the business. There can be multiple groups of potential attackers, or even multiple possible business impacts. In general, the best approach is to use the worst-case option, which will result in greater overall risk.

17.1.2. FACTORS FOR ESTIMATING PROBABILITY

Once the analyst has identified a potential risk, classified this risk in terms of severity, the first step is to estimate the "probability". At the highest level, this is a rough measure of how likely this particular vulnerability is to be discovered and exploited by an invader. There is no need to be more precise in this estimate. In general, the identification of the probability between low, medium or high is sufficient.

There are a number of factors that can help determine the probability. The first set of factors is related to the threat agent involved. The goal is to estimate the probability of a successful attack from a group of possible attackers. Note that there may be multiple disease agents that can exploit a particular vulnerability, so it is generally best to use a worst-case scenario. For example, a source may be a much more likely attacker than an anonymous intruder, but it depends on a number of factors.

Note that each element has a set of options, and each option has a low probability from 0 to 9 associated with it. These numbers will be used later to estimate the overall probability.

Threat Factors

- **Skill level**

How technically qualified is this group of threat actors?

Security penetration skills (9), networking and programming skills (6), advanced computer user (5), some technical skills (3), no technical skills (1)

- **Againstivo**

How motivated is this group of threat actors to find and exploit this vulnerability?
Little or no reward (1), possible reward (4), high reward (9)

- **Opportunity**

What resources and opportunities are required for this group of threat actors to find and exploit this vulnerability?
Full access or expensive resources required (0), special access or resources are required (4), some accesses or resources are necessary (7), do not have access or resources required (9)

- **Size**

How big is this group of threat actors?
Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

- **Vulnerability factors**

The next set of factors is related to the vulnerabilities involved. The goal here is to estimate the likelihood that the particular vulnerability involved will be discovered and exploited.

- **Ease Of discovery**

How easy is it for this group of threat actors to discover this vulnerability?
Virtually impossible (1), difficult (3), easy (7), automated tools available (9)

- **Ease of exploration**

How easy is it for this group of threat actors to actually exploit this vulnerability?
Theoretical (1), difficult (3), easy (5), automated tools available (9)

- **Conscience**

How well known is this vulnerability to this group of threat actors?
Unknown (1), hidden (4), obvious (6), public knowledge (9)

- **Intrusion detection**

How likely is an exploit to be detected?

Active detection in the application (1), Logged in and analyzed (3), Logged in without analysis (8), not registered (9).

17.1.3. FACTORS FOR ESTIMATING IMPACT

When considering the impact of a successful attack, it is important to realize that there are two types of impacts. The first is the "technical impact" on the application, the data it uses, and the functions it offers. The other is the "business impact" on the business and company that operates the application.

Business impact is the most important thing, however, you can't have access to all the information you need to figure out the business consequences of a successful exploitation. In this case, providing as much detail about the technical risk will allow the business representative to make a decision about the risk of the business.

Again, each element has a set of options, and each option has an impact index , from 0 to 9 associated with it. We're going to use those numbers after estimating the global impact .

- **Technical Impact Factors**

The technical impact can be divided into factors aligned with the areas of security: confidentiality, integrity, availability and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were exploited.

- **Loss of confidentiality**

How much data could be released and how sensitive is it?

Minimally disclosed non-sensitive data (2), minimally disclosed critical data (6), completely disclosed non-sensitive data (6), critical data disclosed completely (7), all data disclosed (9)

- **The loss of integrity**

Can the amount of data be corrupted and how damaged is it?

Minimally corrupted data (1), minimally corrupted significant data (3), slightly corrupted data but extensively (5), extensively corrupted significant data (7), all data fully corrupted (9)

- **The loss of availability**

How much would service be lost and how vital is it?

Minimally interrupted secondary services (1), primary services minimally interrupted (5), secondary services extensively interrupted (5), primary services extensively interrupted (7), all services completely interrupted (9)

- **Loss of accountability**

Are the actions of threat actors "made on the basis of an individual?" Fully traceable (1), possibly traceable (7), completely anonymous (9)

Business Impact Factors

Business impact stems from technical impact, but it requires a deep understanding of what is important to the company. In general, we must support our risk analysis with business impact, especially if your audience is executive level. The business is what justifies the investment in fixing security issues.

The following factors are common areas for many companies:

- **Financial loss**

How much financial damage will result from an exploit?

Less than the cost to fix the vulnerability (1), smaller effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)

- **Reputational damage**

How much would an exploit result in reputational damage to the point of damaging the business?

Minimal damage (1), loss of large bills (4), loss of clientele (5), damage to the brand (9)

- **Non-compliance**

How much can an exploit affect compliance?
Minor violation (2), clear violation (5), high-profile violation (7)

- **Privacy violation**

How much personal information can be disclosed?
One individual (3), hundreds of people (5), thousands of people (7), millions of people (9).

17.1.4. DETERMINING THE SEVERITY OF THE RISK

At this stage the probability estimate and the impact estimate are put together to calculate the global severity for this risk. This is done to find out if the probability is low, medium, or high and then do the same for the impact. The scale from 0 to 9 is divided into three parts:

Probability levels	**Impact**
0 to 3	Low
3 to 6	Medium
6 to 9	High

- **Repetitive method**

To have more efficient risk management it is necessary to go through a more formal process of classification of the factors and calculate the result. Remember that there are a lot of uncertainties in these estimates and that these factors are meant to help the tester arrive at a reasonable result. This process can be supported by automated tools to make calculation easier.

The first step is to select one of the options associated with each of the factors and enter the associated number in the table. Then just average the scores to calculate the overall probability. For example:

Threat Agent					Vulnerability factors			
Level of Skill	Reason	Opportunity	Size		Ease of Discovery	Ease of Explore	Conscience	Detection of Intruder
5	2	7	1		3	6	9	2
Overall Probability: 4,375 (Average)								

Next, the tester needs to figure out the overall impact. The process is similar here. In many cases, the answer will be obvious, but the tester can make an estimate based on the factors , or they can average the scores for each of the factors. Again, less than 3 is low, 3 to less than 6 is average, and 6 to 9 is high. For instance:

Technical impacts		Business impacts

Loss of confidentiality	Loss of integrity	Loss of Availability	Loss of accountability		Damage Financial	Damage to reputation	No Cumprimentor	Rape of privacy and
9	7	5	8		1	2	1	5
Overall technical impact: 7.25 (High)					Global Business Impact: 2.25 (Low)			

- **Determining gravity**

The analyzer arrives at the probability and impact estimates, and it can now combine them to get a final severity rating for this risk. If he has good information about the business impacts, he will use it instead of the technical impact information. But if he does not have information about the business, then the use of technical impact is the best choice.

Severity of total risk				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Info	Low	Medium
		Low	Medium	High
	Probability			

In the example above, the probability of the business impact is average and the technical impact is high, so from a purely technical perspective it turns out that the overall severity is high. However, note that the impact on business is actually low, so the overall severity is best described as low as well. This is why understanding the business context of vulnerabilities being assessed is so crucial to making good risk decisions. Failure to understand this context can lead to a lack of trust between business and security teams that is present in many organizations.

17.1.5. DECIDING WHAT TO FIX

After the risks to the application have been sorted there will be a list of priorities of what to correct. As a general rule, the most serious risks should be corrected first.

Remember that not all risks are worth correcting and the loss is not only expected but justifiable based on the cost of fixing the problem. For example, if it would cost $100,000 to implement controls to contain $2,000 of fraud per year, it would take 50 years to get a return on investment to end the loss. But keep in mind that there can be damage to the organization's reputation as a result of fraud, which could cost the organization much more.

18. ANNEX B - DATA RETENTION AND DISPOSAL POLICY

DMS LOGISTICS is responsible for ensuring compliance with the General Law on the Protection of Personal Data (LGPD) and its requirements relating to the collection, storage, retrieval and destruction of records of personal data and/or sensitive data ("Personal Data").

This policy complements, and does not replace, the General Data Privacy Policy and related policies .

The DMS LOGISTICS System maintains sets of Personal Data stored ("Records") in accordance with contractual, regulatory and other legal requirements applicable to the modalities of processing of Personal Data.

It is important that these Records are protected from loss, destruction, forgery, unauthorized access, and unauthorized release. For this, a variety of s controls are used, such as backups, access control and encryption.

This control applies to all operations, people and processes that constitute the information system of the DMS LOGISTICS System, including employees, board members, directors, suppliers, customers and third parties who have access to the data processed by the DMS LOGISTICS System.

18.1. RISK CLASSIFICATION

The DMS LOGISTICS System classifies records into categories that establish retention and disposal requirements for each category.

All Personal Data will be retained for the time necessary to fulfill the purpose for which it was collected, for lawful, specific and informed purposes.

There is a variety of processing of Personal Data whose archiving period is not determined by law, such as, for example, the time of storage of the Personal Data of a commercial prospectus. For such data, the DMS LOGISTICS System stipulates a period of action that is consistent with market practices and the nature of the processing, as long as there is no specific determination by the regulatory authority.

For other Registrations, including those of a tax, labor and social security order, DMS LOGISTICS reserves the right to keep them stored until the end of the limitation period stipulated by law.

18.1.1. CATEGORY OF RECORDS:

- Business Records: information recorded in any medium, created or captured that reflects circumstances, events, activities, transactions or results created or maintained as part of the conduct of business of the DMS LOGISTICS System, such as the sale of products from the DMS LOGISTICS System portfolio; conclusion and execution of contracts; and credit analysis and protection.
- Marketing and Communication Records: personal information obtained by the DMS LOGISTICS System in (i) advertising campaigns, promotional actions and surveys; (ii) social networks; and (iii) customer service.

The Records that are used for marketing or research purposes will remain stored in the DMS LOGISTICS system only for as long as the interest of the holder in receiving these materials lasts, being possible the exclusion at any time, which allows the revocation of consent, if this is the legal basis that justifies the respective modality of treatment.

- Human Records Records: Personal Data collected for (i) HR management, such as management of working time, wages, benefits, social security contributions and taxes; vacations, leaves, absences; (ii) career management, such as training, evaluations, professional experience, mobility in the DMS LOGISTICS System; (iii) HR administration for corporate communication, work in the company's social network and use of computer and telephony tools; organizational charts, corporate services, budgeting and budgeting, reporting, research, reorganizations, acquisitions and spin-offs; (iv) occupational health, such as medical certificates, medical records, occupational health certificates and all others related to the employee's health; (v) recruitment and selection, such as name, gender, marital status, age, contact details, RG, CPF, proof of address, bank details, function information, skills, experiences, qualifications, references, resume, interview and evaluation data, interview notes and registros and any other information that the candidate makes available to the DMS LOGISTICS System; and (vi) business travel management, such as information for travel organization (preferences, location, etc.); CNH and expenses.

Some Personal Data is retained after the termination of the employment contract, internship or temporary employment contract to comply with the legal storage periods defined by labor or tax legislation.

Employment contracts,employee registration forms and the respective Social Security Professional Profiles (PPP) will be stored for an indefinite period, even after the contractual termination.

- Security Records: information collected to manage access and permanence in the facilities of the DMS LOGISTICS System such as name, RG, CPF, photo, biometrics, badge control, CCTV installations, login and password for access to the information systems of the DMS LOGISTICS System.

18.2. RETENTION AND DISPOSAL OF PERSONAL DATA

For each of these scenarios, the following table shows the maximum retention period of Personal Data by the DMS LOGISTICS System, by Registration category, description, as well as the disposal format.

Type of Registration	Description/Data to be deleted	Retention Period	Discard Format
Business	Commercial Contact (name; position; RG, CPF, address; country of origin, profession, telephone; e-mail)	05 years after initial unanswered contact, or promptly, in the event of revocation of the consent or gives the manifestation of disinterest in being Contacted	Elimination by the DMS System LOGISTICS, opt-out, or to any time by holder
Business	General Contracts (name; position; RG, CPF, address; country of origin, profession, telephone; e-mail; bank account; billing data)	5 years after the end of the contract	Elimination by the DMS System LOGISTICS

Business	Tax Documents	5 years from the date of issue of the document	Elimination by the DMS System LOGISTICS
Business	Credit Protection (name; position; RG, CPF, address; country of origin, profession, telephone; e-mail)	During business relationship and another 5 years after the end or promptly, in case of exhaustion of the purpose	Elimination by the DMS System LOGISTICS
Marketing and Communication	Advertising Campaigns, Promotional Actions and Research (name, RG, CPF, address, country of origin, e-mail, phone, replies to research)	Indeterminate or promptly, in case of exhaustion of the purpose or revocation of the assent	Elimination by the DMS System LOGISTICS or Opt-out a any time by holder
Marketing and Communication	Website and Social Networks (geolocation data, IP address, captured online data, cookies)	Indeterminate or promptly, in case of exhaustion of the purpose or revocation of the assent	Elimination by the DMS System LOGISTICS or opt-out a any time by holder

Marketing and Communication	Customer Service – SAC (name, phone, e-mail, address and CPF)	5 years after the last Service	Elimination by the DMS System LOGISTICS

Resources Human	HR Management	During Contract of Work and another 5 years after the end, except FGTS (30 years) and Payroll (10 years) Storage of Employment Contract: indefinite term	Elimination by the DMS System LOGISTICS
Resources Human	Career Management	During Contract of Work and another 5 years after the end	Elimination by the DMS System LOGISTICS
Resources Human	HR Administration	During Contract of Work and another 5 years after the end	Elimination by the DMS System LOGISTICS
Resources Human	Occupational Health	During the contract of work and another 20 years after contract termination	Elimination by the DMS System LOGISTICS
Resources Human	Recruitment and Selection	Pre-interview failure: 15 days Post-interview failure: 90 days (national) or 180 days (international) Approval of the candidate: During Contract of Work and another 5 years after the end	Elimination by the DMS System LOGISTICS
Resources Human	Recruitment and Selection	Indeterminate or promptly, in case of exhaustion of the purpose or after revocation of the consent Candidate approval: During Contract of Work and another 5 years	Elimination by the DMS System LOGISTICS or Opt-out a any time by

		after the end	holder
Resources Human	Travel Management Business	During Contract of Work and another 5 years after the end	Elimination by the DMS System LOGISTICS

Safety	Access to the physical facilities of the DMS LOGISTICS System (biometric data, name, photo, RG, CPF)	5 years after the last access	Elimination by the DMS System LOGISTICS
Safety	CCTV System (images)	3 months after recording	Elimination by the DMS System LOGISTICS
Safety	Badge Information (name, title)	During Contract of Work	Elimination by the DMS System LOGISTICS
Safety	Access to the DMS LOGISTICS System information (login and password)	During Contract of Work	Elimination by the DMS System LOGISTICS

18.3. DISPOSAL BY THE DMS LOGISTICS SYSTEM

As soon as the period expires, and provided that there is no valid reason for us to keep it, the Personal Data in physical copy will be destroyed as confidential waste and those kept electronically will be deleted from the systems of DMS LOGISTICS and d and contracted third parties.

Hypotheses of ongoing investigation, administrative and judicial proceedings are valid reasons for keeping the Records and, regardless of consent, the storage periods indicated above may be extended in these cases.

If the data subject chooses to exercise his right to erasure of this information, the Personal Data will be discarded immediately by the DMS LOGISTICS System, except in cases of compliance with a legal or regulatory obligation.

18.4. FACILITATED CONTACT

Requests received from the holder of Registrations to exercise their rights throughout the processing period will be answered in the manner and within the deadlines required by the applicable regulations.

To exercise their rights, the Owner may send requests through the email dpo@dmslog.com. The holder must clearly indicate his full name, insert a copy of an identification document and indicate the address to which the reply should be sent.

The Foreman can be contacted at dpo@dmslog. com to answer questions or for more information about this Data Disposal and Anonymization Policy.

19. REVISION HISTORY

Revision	Data	Description
00	06/02/2023	Issuance of the document.
01	28/02/2023	Review and standardization of the entire document.

20. 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

DMS
LOGISTICS

WE NEVER PUT QUALITY OR ETHICS AT RISK IN BUSINESS

WE NEVER COMPROMISE ON QUALITY
AND BUSINESS ETHICS

WWW.DMSLOG.COM