SECURITY INCIDENT MANAGEMENT POLICY

Code: POL-TI-012
Revision: 01
Data: 13/03/2023

WWW.DMSLOG.COM

1. DEFINITIONS

The main objective of DMS LOGISTICS' Incident Management Policy is to define the strategic guidelines for actions related to Information and Communications Security, 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 DMS LOGISTICS.

The objective of the rules for Incident Management is primarily to ensure the protection of information assets against threats, internal or external, minimize any risks to information security, reduce exposure to loss or damage arising from security failures and ensure that adequate resources are available, maintaining an effective security program and making its Employees aware of it.

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. PURPOSE

- "Threat" means risk or potential danger of an incident, which may result in damage to DMS LOGISTICS.
- "Privacy and Data Protection Area" means the area responsible for supporting the DPO.
- "Asset" means something that has value to DMS LOGISTICS and needs to be adequately protected.
- "National Data Protection Authority" or "ANPD" means the administrative authority in charge of the Protection of Personal Data. National public

administration body responsible for ensuring, implementing and supervising compliance with the General Law for the Protection of Personal Data throughout the Brazilian territory.

- "Committee on the Security and Protection of Personal Data" means a committee specifically dedicated to dealing with information security events.
- "Employees" means all employees of DMS LOGISTICS, including directors, interns, apprentices and any other person who has a direct link with DMS LOGISTICS.
- "Personal Data" means any data relating to an individual (natural person) who is or can be identified from the data or from the data in conjunction with other information.
- "Incident Response Team" means persons or area(s) appointed by theInformation Security Management for the identification of internal or external Security Incidents, whether or not involving Personal Data, whether in the detection of alerts from DMS LOGISTICS' network monitoring systems or by notifications made by Users of the Information or by any person reporting to be of their knowledge, or even victim of suspicious activity or in disagreement with the Information Security Policy and other policies of DMS LOGISTICS.
- "Event" means any occurrence visible in a network or information system. Examples: a user who accesses a shared file, a server that receives a request for a Web page, a user who sends an e-mail, or a firewall that blocks a connection attempt,among others.
- "Adverse event" (or offensive) means an event, confirmed or under suspicion, with negative consequences. Examples: information system failures, unauthorized use of information system privileges, unauthorized access to sensitive data, or execution of data-destroying malware, among others.
- "Data Officer" or DPO means the person who at DMS LOGISTICS is responsible for coordinating and ensuring compliance with this Policy, with the Data Protection Legislation and who will act as a channel of DMS LOGISTICS with the Data Subjects and with the National Data Protection

Authority.

- "Security Incident" means any event or set of unwanted information security events, confirmed or under suspect, that has a significant possibility of affecting the operations or threatening the information of DMS LOGISTICS and/or that indicates possible violation of PSI and its aggregate standards and procedures, failure of controls or previously unknown situation, that may be relevant to information security.
- "Relevant security incident" means a security incident that affects systems or services considered as relevant by DMS LOGISTICS with consequences of interruptions of various internal and/or external business processes, not predictable and difficult to manage, causing great financial impact, as well as on the image of DMS LOGISTICS.
- "Information" means the set of data that, processed or not, may be used for the production, processing and sharing of knowledge, contained in any medium, medium or format.
- "Risk" means the combination of the likelihood of an unwanted event materializing and its potential impacts.
- "SI" means the security area of the information.
- "IT" means the area of Information Technology.
- "Information User(s)" means employees, employees, trainees, apprentices and any other person who has a direct relationship with DMS LOGISTICS, as well as representatives, suppliers, service providers and third parties at the service of DMS LOGISTICS.
- "Personal Data Breach", "Personal Data Security Incident" or "Personal Data Breach Incident" means Security Incident involving Personal Data.
- "Black Team" is a cyber security group designed to carry out offensive security tests in physical environments.
- "Red Team" is a cyber security group designed to conduct offensive security tests in digital environments.
- "Blue Team" is a cyber security group designed to conduct defensive

operations and provide defensive security and incident response.

- "Purple Team" is a cyber security group aimed at maximizing the performance of the red team and blue team. He plays with a combination of the two teams.
- "Orange Team" is a cyber security group designed to help developers think like an attacker, using information from the red team, in order to create applications and systems that are secure and free from possible attacks.
- "White Team" is a cyber security group designed to manage the other teams, promoting interaction between them, establishing rules, policies and security standards and ensuring that these requirements are followed.
- "CISO" is the figure of the Chief Information Security Officer, who is responsible for ensuring data security as a priority and in the organization.
- "DPO" is the figure of the Data Protection Officer, in the LGPD defined as data in charge, responsible for maintaining information security standards in the organization and communicating with the National Data Protection Authority (ANPD).

3. GUIDELINES

Incident Management aims to ensure that events confirmed or under suspicion are reported, recorded and handled effectively, orderly and in a timely manner.

Any adverse event, under suspicion or confirmation, related to the security of our systems or our network, must be documented in our task grouping, described and evidenced the event, prioritizing this demand as "Hotfix" (high priority for resolution).

The person responsible for notifying the event must generate a member of the team to be responsible for the entire process of solving the task and ensure that it is resolved and delivered in a timely manner.

The incident management and data breach process must have the support of Top Management and must adopt the following guidelines:

3.1. PREVENTION OF INFORMATION AND PERSONAL DATA SECURITY INCIDENTS

- DMS LOGISTICS will carry out impact assessments on data protection, breach of confidentiality, integrity, authenticity and non-repudiation before starting any project or implementing any technology that processes Personal Data. The associated risks will be identified in the impact assessments.

- After Determining whether a high risk exists, the Security Committee – and if the Security Incident also involves Personal Data, the Data Controller – will take appropriate technical and organizational measures to protect the Personal Data from accidental or unlawful destruction or accidental loss, alteration, disclosure or unauthorized access.

3.2. INCIDENT IDENTIFICATION

- The members of the Security Committee, when reported by the Users of Information or their managers about the suspicion of a Security Incident,must evaluate whether the incident involves Personal Data, in which case they will notify the Data Controller in this regard, through the email: dpo@dmslog.com.

- Once the SecurityIncident is confirmed, the Incident Response Team should be called upon to categorize and prioritize care based on: (i) the potential impact as per the information security risk assessment conducted in conjunction with the Security Incident Severity Classification Table (Annex E); (ii) the time and resources required to recover impacted assets.

- Every incident categorized as being of critical severity should be notified immediately to the CISO (Chief InformationSecurity Officer), who can allocate the professionals needed to resolve the incident.

- If the occurrence sets up an Incident involving Personal Data, the Data Controller must receive the notification and prepare the Personal Data Breach Incident Report, with the support of the IS Manager, IT and other impacted areas.

- The Incident Response Team should present the actions that will be prioritized based on the category and impact of the scenario encountered

and carry out the necessary communications.

- All Security Incidents involving Personal Data will be evaluated by the Committee on Security and Protection of Personal Data, which shall define what measures will be adopted.

3.3. INCIDENT LOG

- If the incident involves Personal Data, the CISO, the Data Officer and other members of the Security Committee will record the Security Incident or Personal Data Breach, with the description of the incident, time period, consequences, identification of the persons who evaluated and to whom the incident was reported, actions taken to resolve the incident and the consequences that the incident caused, such as the unavailability, loss, disclosure or alteration of the Information and/or Personal Data.

- The Data Controller will assess the type and level of risk created by the breach and will then record the incident in DMS LOGISTICS' internal files.

- If the Security Incident involves Personal Data, the Data Controller will determine whether there is a risk to the rights and benefits of the Data Subjects. Risks to rights and freedoms include, but are not limited to, loss of control or confidentiality of Personal Data, unauthorized reversal of pseudonymization, reputational damage, discrimination, identity theft or fraud, and financial loss, and other economic or social disadvantages.

- The Data Officer will assess whether the likelihood and severity of the potential risks create a high risk. That assessment shall involve an analysis of the type of violation; nature; the sensitivity and volume of Personal Data affected; the severity of the possible consequences for data subjects; the number and characteristics of the data subjects affected; the characteristics of the recipient of the Personal Data and the ease of identification of the Data Subjects.

- The Committee on Security and Protection of Personal Data will define what measures will be adopted, including notification to the ANPD and/or Data Subjects.

- The Committee will pass on the situation to the management, which will

then make its final analysis before forwarding to the ANPD.

- If necessary, notification will be made to the ANPD and the Data Subjects, based on the level of risk, with the support of the CISO, the Committee on Security and Protection of Personal Data and the Data Controller.

3.4. SECURITY INCIDENT CONTAINMENT

- The Data Officer, with the support of IT, IS and the Security Committee, shall guide the Managers and areas responsible/affected by the Security Incident involving Personal Data as to the corrective measures to be taken to mitigate the risk as much as possible.
- In the event of a Security Incident, the Data Officer shall submit a report to the Security Committee to define what actions will be taken by DMS LOGISTICS.
- IT, SI and the Security Committee shall provide support with the necessary techniques to contain/recover the incident, such as collecting evidence legally or isolating technology resources so as not to lose information from the incident.

3.5. INCIDENT MITIGATION

3.5.1 PREPARATION

- Manage the tasks for incident analysis, including knowledge of the entire environment used;
- Implement defense mechanisms and threat control;
- Develop procedures to handle incidents efficiently;
- Get resources and staff needed to deal with problems;
- Establish infrastructure to support incident response activity.

3.5.2. DETECTION

- Detect the incident, determine the scope and parties involved with the incident;

- Identify all affected systems and services related to the incident;
- Assess the impact of the incident and the potential risks of the affected systems (leaked data, information from partner institutions, impact on the organization itself and impact on reputation);
- Identify the existence of otherwinds and alerts related to the incident in question;
- Identify what type of information and processes may have been affected;
- Identify those responsible for the compromised system, support teams and owners of the information.

3.5.3. CONTAINMENT

- Contain the incident in order to mitigate the damage and prevent other resources from being compromised;
- Disconnect the compromised system or isolate the affected network;
- Disable the system to prevent further losses when there is loss or theft of information during the attack;
- Change routing policies of network equipment or block traffic patterns, stopping the malicious flow;
- Disable vulnerable services, inhibiting compromise of other systems.

3.5.4. ERADICATION

- Eliminate the causes of the incident, removing all related events;
- Ensure that the causes of the incident have been removed, as well as all activities and files associated with the incident;
- Ensure the removal of all access methods used by the attacker:new access counts; backdoors and, if applicable, physical access to the compromised system, etc.

3.5.5. RECOVERY

- Restore the system to its normal state;
- The Disaster Recovery Plan must be initiated as specified in the respective plan.
- Restore the integrity of the system;
- Ensure that the system has been recovered correctly and that the functionalities are active;
- Implement security measures to avoid new commitments;
- Restore from the last and healthy full backup stored.

3.5.6. ACTION EVALUATION

- Evaluate the actions taken to resolve the incident, documenting details, and discuss lessons learned;
- Characterize the set of lessons learned in order to improve existing procedures and processes;
- Identify incident characteristics that can be used to train new team members;
- Provide statistics and metrics related to the incident response process;
- Obtain information that can be used in legal proceedings.

3.6. RISK ANALYSIS

In order to analyze the risks involved in the Security Incident, a risk analysis conducted by the Security and Protection of Personal Data Committee and the Incident Response Team shall be carried out.

3.7. NOTIFICATION TO ANPD

A Pedestrian Data Breach That is likely to pose a risk to the rights and freedoms of the Holders must be reported to the ANPD without undue delay, when possible,

within 2 (two) business days after DMS LOGISTICS becomes aware of the breach. The reasons for any delay in communication to the ANPD must be justified.

DMS LOGISTICS is considered aware of a breach when there is a reasonable degree of certainty that a Security Incident has occurred.

A partial and incomplete notice may be sent to the ANPD as soon as possible in some circumstances. These circumstances include complex violations that require detailed investigations or when multiple similar violations occur in a short period.

The notification to the ANPD shall include, among other points described in the annex Notification to the Authority:

- A description of the nature of the Personal Data affected;
- information on the holders involved;
- an indication of the technical and security measures used for data protection,subject to trade and industrial secrets;
- the risks related to the incident;
- the measures that have been or will be adopted to reverse or mitigate the effects of the injury;
- an indication of the technical and security measures used for data protection, subject to trade and industrial secrets;
- the reasons for the delay, where the communication was not immediate;
- Identify touchpoints for further details;
- Describe possible consequences of the data breach incident;
- I believe we see measures to address the data breach incident, including measures taken to mitigate potential adverse effects of the data breach incident .

3.8. NOTICE TO DATA SUBJECTS

The Data Controller will communicate high-risk breaches to the affected data subjects without undue delay.

Communication with the data subject must contain clear and simplified language, based on guidelines from the Legal,Data Officer and the Security Committee.

Communication with data subjects should be delivered by available means that maximize the chances of communication, and may require the use of various methods of communication and the provision of information and formats.

3.9. DECISION NOT TO NOTIFY

DMS LOGISTICS is exempt from the mandatory notification requirement when the risk to data subjects is extremely low or does not exist.

If the decision not to notify is made, the justification for that decision shall be documented.

DMS LOGISTICS shall continue to monitor the circumstances and effects of a breach and may need to make or update notifications to the ANPD and the Data Subject as new information emerges.

All actions taken in connection with violations must be fully documented, even if no notification is required.

3.10. POST INCIDENT

The post-Security Incident, or Personal Data breach, has its beginning after the resolution and closure of the incident,in which the Incident Response Team, IS, IT and Security Committee will analyze the causes that motivated the incident and what are the measures that can be taken so that the event does not occur again.

3.11. RECOMMENDATIONS AND RESPONSES TO INCIDENTS

If there are recommendations to be made to users, system administrators, or other security teams, these should be made in the process of closing the incident.

3.12. LESSONS LEARNED

The objective of this step is to improve the procedures performed in the response step and improve the Assets to protect them from future incidents.

The Incident Response Team shall communicate to stakeholders the outcome of the analysis.

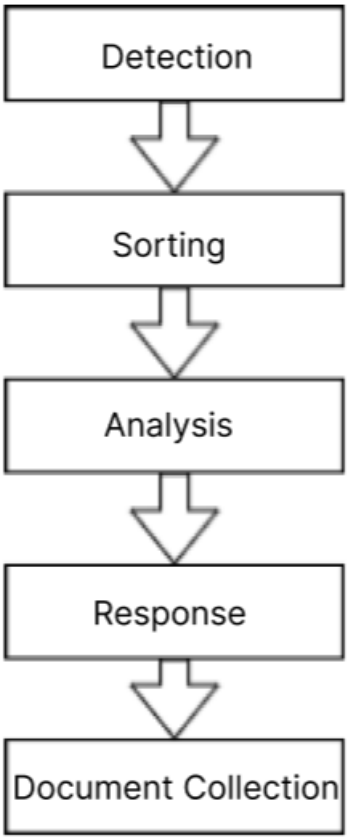
Incidents that occur should be analyzed in conjunction with DMS LOGISTICS' business continuity procedures. This analysis aims to identify the improvement of the indicators of probability and consequence of the predicted incidents and the actual occurrences of incidents.

Based on the report and information obtained during the resolution of the incident, the Incident Response Team should create an action plan that includes those responsible to ensure that all stakeholders know what is expected of them. Stocks should be categorized as short or long term.

A knowledge base should be maintained with the history of treated incidents, to facilitate the treatment of future incidents with similar characteristics and to generate indicators.

4. INCIDENT HANDLING PHASES

The handling of incidents has five phases, which must follow a defined order, namely:



- Detection: Report or Identify the event.
- Screening: Evaluate, Categorize and Prioritize the event.
- Analysis: Understand the incident.
- Answers: Actions to resolve the incident.
- Evidence Collection: Define and apply procedures for the identification, collection, acquisition and preservation of information that can be used as evidence of the event that occurred

5. MAIN THREAT

This plan should be activated when there are incident scenarios that present a risk to the continuity of service delivery.

EVENT / ACCIDENT	POSSIBLE CAUSES
Interruption of electricity supply	Caused by a factor external to the electrical network of the company or its location with interruption duration exceeding 12 hours and/or internal factor that compromises the company's electrical network with short circuits, fire and infiltrations.
Failure to air conditioning the environment two servers	Overheating of assets due to failure in the sizing of load in the room, especially in the servers and switches.
Network Unavailability / Internet / Circuits	Rupture of interconnection cables resulting from internal or external effects such as the execution of works, inclement weather, natural disasters or accidents.
Human error	Accident while handling critical equipment.
Insider attacks	Attack on company assets (Invasion of employee databases).
Fire	Fires that compromise the company's services.

Natural Disasters	Earthquakes, storms, floods, etc.
Hardware failure	Failure that requires replacement of part or repair, whose repair or acquisition depends on the purchase process and / or availability in suppliers.
Cyber attack	A virtual attack that compromises the performance, data, or configuration of the services and systems the company uses.
Information Leakage	Malicious or attacking user who can share information from employees, third parties and/customers.

6. ROLES AND RESPONSIBILITIES

6.1. COMMITTEE ON SECURITY AND PROTECTION OF PERSONAL DATA

- Evaluate the Business Continuity Plan periodically and decide for its activation when incidents occur, responding at the institutional level for the execution of the plan and other related occurrences.
- Monitor the initiatives related to the theme of protection of Personal Data of DMS LOGISTICS, including the training of Information Users, events related to Security Incidents and status of the process of implementation of privacy tools/software.
- AnalyzeDMS LOGISTICS' report(s) regarding Security incidents involving Personal Data, with the support of IS and the Data Controller.
- It is responsible for all communications during a disaster. Specifically, they will communicate with employees,customers, authorities, suppliers, and even the media if necessary.
- The leader of this team is the CISO, who will administer and maintain the Crisis Management Plan. It shall provide support to the Senior Management of DMS LOGISTICS on decisions to be taken regarding the processing of Personal Data that present risks, such as the results of impact assessments

on the protection of Personal Data, and the breach of Personal Data.

- Provides the server infrastructure needed for IT staff to perform their critical operations and processes during a contingency.
- Ensures that essential activities function as required to meet business objectives in the event of discontinuation of activities for some reason;
- Provision that employees sign a term of responsibility and confidentiality of information;
- It makes wide disclosure and monitors the correct use of information and data security of the company, employees and customers, to meet and comply with Law 13.709/2018 – General Data Protection Law (LGPD) and ISO 27001.
- Approves and undertakes actions or investments that promote the continuous improvement of the process.
- Supports whenever necessary in the interaction and scheduling with the other areas in order to provide faster service to the process.
- Supports internal investigation procedures when necessary.
- Creates and manages a security incident response team.

6.2. SI

- Review this Policy and propose changes.
- Create a response plan forSecurity Incidents.
- Classify the severity of Security Incidents that have occurred.
- Establish and improve Security Incident prevention programs and systems.
- Monitor information security systems.
- Prepare periodic reports onSecurity Incidents that have occurred.
- Analyze and collect technical evidence in cases of security incidents.
- Investigate security incidents, reporting the information pertinent to the

event involving Personal Data to the Data Controller, suggesting the technical measures to be adopted.

- Analyze Security Incident Reporting, as well as support the Data Officer in the incident investigation processes and in the preparation of the Personal Data Breach Incident Report.
- If the Security Incident involves Personal Data, notify the Data Controller to report it to the Data Protection Committee.
- Determine the continuous monitoring of the technological environment from the point of view of information security, in order to identify events that may impact the availability, integrity and confidentiality of Personal Data that are processed by DMS LOGISTICS.
- Follow all the phases described in this document, from the identification to the solution of the incident.
- Communicate to the areas responsible for managing changes in case of Personal Data breach incidents that involve impacts on the production environment.
- Support with the necessary technical measures for containment/recovery of the incident.
- Monitor compliance with this Policy.

6.3. DATA OFFICER

- After analyzing the Security Incident Report by IS and having been notified about a possible Personal Data Breach Incident, it prepares the Personal Data Breach Incident Report, with the support of the Manager, as well as IT and IS.
- Prepare a report on risks to the processing of Personal Data and incidents of Personal Data breach to the Committee on Security and Protection of Personal Data.
- Initiate investigation processes of theData Breach Index and indicate the areas involved that should participate in the process.

- Assess the need to communicate the Personal Data Breach Incident to the National Data Protection Authority and Personal Data Subjects, with prior reporting to the Security Committee and the Board of Directors.
- Monitor and support the implementation of action plans to correct gaps in privacy initiatives.
- Guide the IS area on security measures that should be implemented in the systems, according to ANPD guidelines.
- Be responsible for the interface with the ANPD, whenever necessary.

6.4. BOARD OF DIRECTORS

- To become aware, through the Committee on Security and Protection of Personal Data, and measures on cases of Incidents and Violation ofPersonal Data that have consequences outside of DMS LOGISTICS and that involve the press or external community.
- If the Security incidents involve Personal Data, the respective knowledge by the Board of Directors will be through theInformation Security Committee.

6.5. TI

- Approve and undertake actions or investments that promote the continuous improvement of the process.
- Assist in the analysis of Personal Data breach incidents through the presentation of audit trails of the systems under its management.
- Analyze and collect technical evidence in cases of security incidents.
- Investigate security incidents involving Personal Data, reporting the information pertinent to the event to the Data Officer, IS and Security Committee, suggesting the technical measures to be adopted.
- Assist in incident investigation processes when required.
- Support with the necessary technical measures for containment/recovery of incidents.

7. TRIGGERING INCIDENT MANAGEMENT TEAMS

This plan will be triggered when any of the incident scenarios occur, the insurgency or occurrence of an unknown risk or if a vulnerability has a great possibility of being exploited. The plan may also be triggered in cases of testing or by determination of the company's senior management to evaluate its efficiency, effectiveness and effectiveness.

In case of an incident, the responsible parties listed below must be activated:

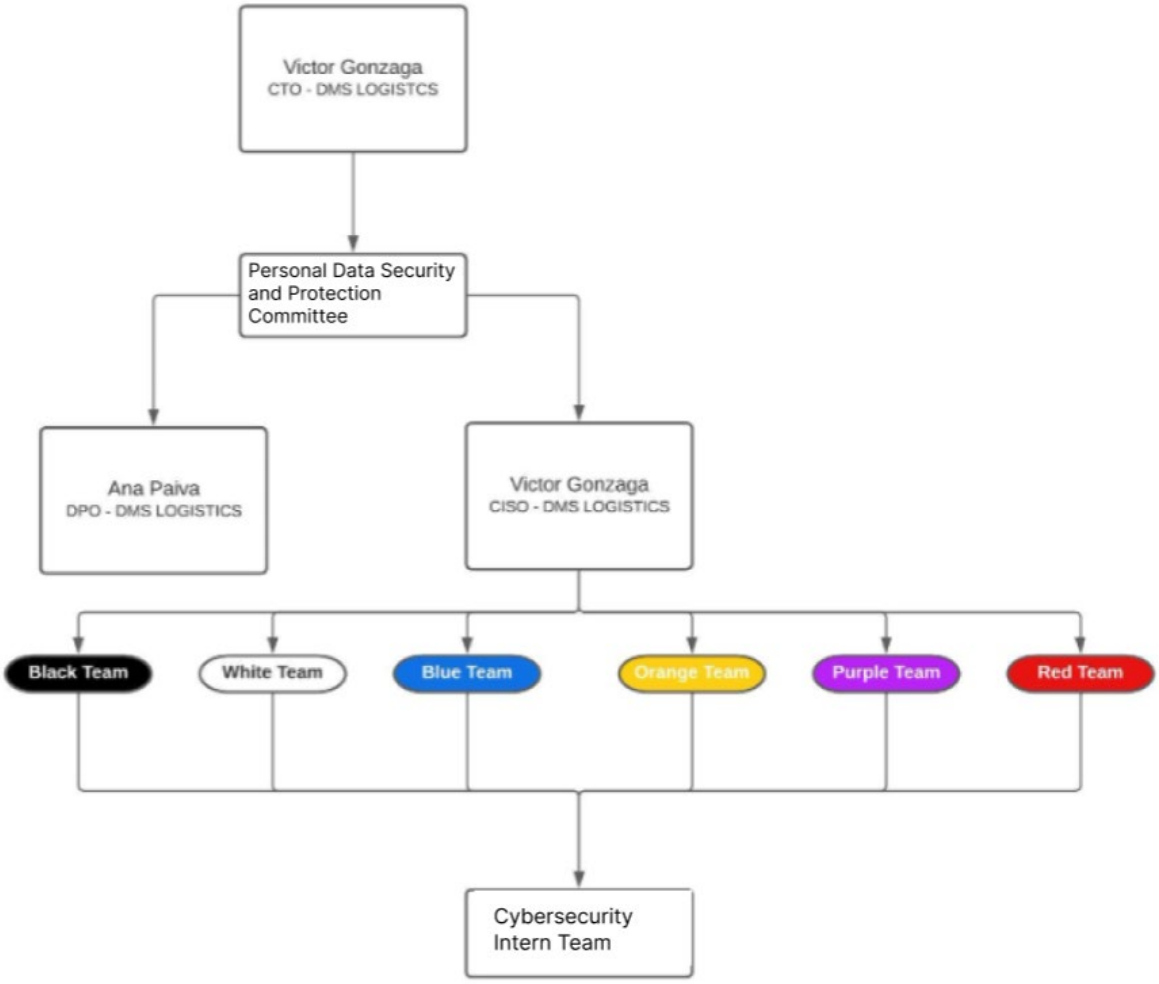
Members of the Committee on Security and Protection of Personal Data

CONTATO	FUNCTION / AREA	EMAIL
Victor Gonzaga	CISO	victor.gonzaga@dmslog.com
Ana Paiva	DPO / Head do RH e DP	dpo@dmslog.com
Natalie Corrêa	Member / Team Leader Support and Quality	natalie.correa@dmslog.com
Monique Pestana	Member / Team Leader DevOps and QA	monique.pestana@dmslog.com
Felipe Location	Member / Team Leader Development	felipe.lage@dmslog.com
Leonardo Sabbadim	Member / Team Leader Quality Assurance	leonardo.sabbadim@dmslog.com

IncidentManagement Team Members

CONTACT	FUNCTION / AREA	EMAIL
Victor Gonzaga	CISO	victor.gonzaga@dmslog.com
Ana Paiva	DPO / White Team	dpo@dmslog.com
Xx	Blue Team Leader	dpo@dmslog.com
Xx	White Team Leader	dpo@dmslog.com
Xx	Orange Team Leader	dpo@dmslog.com
Xx	Red Team Leader	dpo@dmslog.com

8. ORGANIZATION CHART OF THE SECURITY INCIDENT MANAGEMENT TEAM



9. PRIORITIZATION OF INCIDENTS

The following services are considered essential, in order of prioritization, for the activation and execution of this plan.

Service / Area	Criticality
Information Security and IT	Loud

Monitoring with technological resources	Loud
Service Bus and Password Control	Loud
Links the Internet	Loud
Institutional email/webmail	Low
RH	Average
VPN	Low

10. SANCTIONS AND PUNISHMENTS

Violations, even if by mere omission, negligence, recklessness or unconsummated attempt to violate this Policy as well as other safety rules and procedures, will be subject to disciplinary action.

The Committee on Security and Protection ofDa of Personnel, in Security Incidents and Personal Data Breaches, and the Data Controller, in cases of Personal Data Breach, will support internal investigation procedures, when necessary.

The procedures for the investigation and application of disciplinary measures shall comply with the internal regulations and decisions of the Board of Executive Officers.

In the case of third parties hired or service providers, the Information Security structure must analyze the occurrence and deliberate on the effectiveness of sanctions and punishments according to the terms provided for in the contract.

11. MISSING CASES

The omitted cases will be evaluated by the Committee on Security and Protection of Personal Data for further deliberation.

The guidelines established in this Policy and in other security standards and procedures are not exhausted due to the continuous technological evolution and constant emergence of new threats. In this way, it is not an exhaustive list, being the obligation of the user of the information of DMS LOGISTICS to adopt, whenever possible, other security measures beyond those provided herein, in order to guarantee anti-protection to the information of DMS LOGISTICS.

12. IMPLEMENTATION AND UPGRADE

The DMS LOGISTICS Security Incident Management Policy shall be updated whenever necessary or at an interval not exceeding one (1) year.

13. ANNEX A – SECURITY INCIDENT REPORTING FORMAT

Name:

Charge:

Area/Department:

Description of the Incident or suspected Incident:

Date and time the incident was discovered:

Nature of the data involved (where possible):

Information on impacted holders (where possible):

Affected sites and systems:

Has the incident been resolved? How soon? In what way?

Potential impacts of the incident: [Damage to systems/loss of data/violation of legislation/violation of internal policies]

Is there or is it suspected that there is the involvement of any Employee in the security incident? If so, what is the name and participation of this Contributor?

14. ANNEX B – PERSONAL DATA BREACH INCIDENT FORM

Part 1 - Notification of Personal Data Breach	
Information	DATA TO BE FILLED IN BY THE AREA
Date of incident	
Date of discovery of the incident	
Location of incident	

Affected countries (if applicable)	
Name of the employee responsible for identifying the incidents	
Contact details of the employee responsible for identifying the incident	
Brief description of the incident	
Number of Personal Data Subjects Affected	
Has Personal Data been put at risk? Please detail	
Brief description of the measures taken after discovery of the incident	
Completion by the Personal Data Protection Officer	
Received by:	
Date received:	
Areas to be involved:	
Date of notification of involvement of the other areas:	
PART 2 – SEVERITY ASSESSMENT	
Details of systems, equipment, records involved in the incident	
Details of what data has been breached (destruction, improper alteration, improper sharing, etc.)	

Nature/category of the data targeted by the Personal Data incident (types of data involved)	
Volume of data affected by the incident	
Is this information safeguarded? If not, could this Personal Data Breach have operational, legal and reputational actions for the Company?	
How many individuals were affected?	
Is there sensitive Personal Data involved?	
Is there Personal Data of minors involved?	
Was it possible to identify everyone involved in the incident?	
Does the Personal Data breach affect any right to the holder, which is guaranteed by data protection legislation?	
Can the Information accessed by third parties be used for illicit purposes? Ex.: registrations, purchases and opening of bank accounts.	
PART 3 – MEASURES TAKEN	
Technical and legal measures adopted	
Recommended action plans	

Notification to the National Data Protection Authority is required? From which countries? (if necessary)	
Notification required for Personal Data Subjects?	
Notification to other interested parties required?	
What security measures are applicable to the area/resource originating from the incident?	
SIGNATURES	
Information User:	
Data Officer:	
Data:	
Evaluation and decision of the Data Protection Committee:	

15. ANNEX C – NOTIFICATION TO THE AUTHORITY

15.1. COMMUNICATION

- Type of communication:
    - Complete.
    - Partial.
- For partial communication:
    - Preliminary.
    - Complementary.
- Criteria for communication:

- The security incident may entail a relevant risk or damage to the holders.
- I'm not sure about the risk level of the security incident.

15.2. TREATMENT AGENT

The notifier is:

- Controller.
- Operator.

If operator, inform if there has already been communication to the controller: [Response]

Data of the treatment agent:

CPF or CNPJ number: [XXX]

Name or Corporate Name: [XXX]

Nature of the Organization (Public or Private): [Answer]

Address: [Reply]

City: [Answer]

Status: [Response]

ZIP Code: [Answer]

Phone: [Reply]

Email: [Reply]

Notifier data:

Name: [Answer]

Email: [Reply]

Phones: [Response]

Data of the person in charge:

-Same data as the notifier.

Name: [Answer]

Email: [Reply]

Phone: [Reply]

15.3. SECURITY INCIDENT

Briefly describe how the personal data security incident occurred.

[Reply]

When did the incident occur?

[Date and time]

- I'm not aware. Justify: [Response]

- I'm not sure. Justify: [Response]

When was the organization aware of the security incident?

[Date and time]

Describe how the organization was aware of the security incident.

[Reply]

If the initial communication of the incident was not communicated within the suggested period of 2 working days after becoming aware of the incident, please justify the reasons.

[Reply]

If the incident was not reported immediately after your knowledge, justify the reasons for the delay.

[Reply]

What is the nature of the data affected?

- Racial or ethnic origin.

- Religious conviction.
- Political opinion .
- Union membership.
- Affiliation to an organization of a religious, philosophical, or political character.
- Data regarding health.
- Data regarding sexual life.
- Genetic or biometric data.
- Data of proof of official identity (For example, number RG, CPF, CNH).
- Financial data.
- Information systems usernames or passwords.
- Dado de geolocalização.

Other: [Answer]

How many holders are affected?

[Reply]

What is the category of the affected holders?

- Employees
- Service providers
- Clients
- Consumers
- Users
- Healthcare patients
- Children or adolescents

Other: [Answer]

15.4. SECURITY MEASURES USED FOR DATA PROTECTION

What Technical and administrative security measures have been taken to prevent the recurrence of the security incident?

[Reply]

What security, technical and administrative measures were taken after the security incident became aware?

[Reply]

What security, technical and administrative measures have been or will be adopted to reverse or mitigate the effects of the damage of the security incident to data subjects?

[Reply]

Has the processing agent carried out an impact report on the protection of personal data?

[Reply]

15.5. RISKS RELATED TO THE SECURITY INCIDENT

What are the likely consequences of the security incident for the affected holders?

[Reply]

Considering the affected holders, in your opinion, can the incident have cross-border consequences?

[Reply]

15.6. COMMUNICATION TO DATA SUBJECTS

Have the holders been notified about the security incident with personal data?

- Yes
- No
- I don't know

Provide details.

[Reply]

If the affected holders have not been informed, what are the reasons for the non-communication or their delay?

[Reply]

Best regards

DMS LOGISTICS

16. ANNEX D – NOTIFICATION TO THE HOLDER

[RECIPIENT]

[ADDRESS]

Dear [Personal Data Subject],

We regret to inform you of a breach of security that has resulted in the [destruction OR loss OR alteration OR accidental [or unlawful] disclosure OR unauthorised access] of your Personal Data.

The breach was discovered in [DATA] and probably occurred in [DATA].

As a result of our investigation, we conclude that such breach affects the following types of information:

- [TYPES OF INFORMATION. FOR EXAMPLE, PERSONAL DATA AND SENSITIVE PERSONAL DATA].

The violation occurred in the following circumstances and for the following reasons:

- [CIRCUMSTANCES].
- [REASONS].

We take the following measures to mitigate any adverse effects:

- [MEASURES].

We recommend that you take the following steps to mitigate possible adverse effects:

- [MEASURES].

We inform the Data Protection Authority of the breach in [DATA].

Any additional clarifications may be obtained through the contacts indicated below:

- [NAME OF DATA CONTROLLER]
- [NAME OF DATA CONTROLLER]
- [ADDRESS]
- [PHONE NUMBER]
- [EMAIL ADDRESS]
- [WEBSITE ADDRESS].

Best regards

DMS LOGISTICS

17. ANNEX E – CLASSIFICATION OF SECURITY INCIDENTS

Severity	Legality	Confidentiality	Integrity	Availability	SLA
Criticism	High-impact legal misconduct that can result in prosecution and high fines. Non-compliance with legal provisions. Possibility of high-impact litigation. Occurrence of breach of contract with third parties and customers.	In the event of an incident affecting systems or services considered relevant by DMS LOGISTICS, there are consequences for various internal and/or external business processes, which are not predictable and difficult to manage. Possibility of exploitation of vulnerabilities by attackers due to the use of information made public due to a security incident.	In the event of a security incident affecting systems or services considered relevant by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, partially predictable and difficult to manage. Possibility of erroneous decision making by DMS LOGISTICS due to the lack of integrity of information	In the event of a security incident affecting systems or services considered relevant by DMS LOGISTICS, there is a consequence for one or more internal and/or external business processes, partially predictable and difficult to manage. Stoppage of the activities of a business unit of DMS LOGISTICS or several Areas. Discontent with employees and customers. (> 50 %).	0 to 2 hours

			affected by the security incident.		
Loud	High-impact legal misconduct that can result in prosecution and high fines. Non-compliance with legal devices. Possibility of high-impact litigation. Occurrence of breach of contract with third parties and customers.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for various internal and/or external business processes, which are not predictable and difficult to manage. Possibility of exploitation of vulnerabilities by attackers due to the use of information made public due to a security incident.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, partially predictable and difficult to manage. Possibility of erroneous decision making by DMS LOGISTICS due to the integrity of information affected by a security incident.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, partially foreseeable and difficult to manage. Stoppage of the activities of a business unit of DMS LOGISTICS or several Areas. Discontent of employees and customers (> 50%).	0 to 2 hours
Average	High-impact legal misconduct that can result in prosecution and high fines. Legal fault with procedures for investigation of incidents and / or illegal.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, partially predictable and manageable.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, partially predictable and manageable.	In the event of a security incident affecting your services or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, partially predictable and manageable. Stoppage of the activities of a DMS LOGISTICS business unit. Discontent of employees and customers (> 25 %).	Up to 24 hours
Low	Low-impact legal misconduct that can result in prosecution and low fines.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, predictable and easily manageable.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, predictable and easily manageable.	In the event of a security incident affecting systems or services by DMS LOGISTICS, there are consequences for one or more internal and/or external business processes, predictable and easily manageable. Stoppage of activities and a small group of users. Discontent of employees and customers (> 25%).	Up to 48 hours

18. ANNEX F – OPERATIONAL PROCEDURES IN THE EVENT OF AN INCIDENT

This regulation indicates which operating procedures should be adopted in the following scenarios:

EVENT / ACCIDENT	POSSIBLE CAUSES
Interruption of electricity supply	Caused by a factor external to the electrical network of the company or its location with interruption duration exceeding 12 hours and/or internal factor that compromises the company's electrical network with short circuits, fire and infiltrations.
Failure to air conditioning the server environment	Overheating of assets due to failure in the sizing of load in the room, especially in the servers and switches.
Network Unavailability / Internet / Circuits	Rupture of interconnection cables resulting from internal or external effects such as the execution of works, inclement weather, natural disasters or accidents.
Human error	Accident while handling critical equipment.
Insider attacks	Attack on company assets (Invasion of employee databases).
Fire	Fires that compromise the company's services.
Natural Disasters	Storms, floods etc.
Hardware failure	Failure that requires replacement of part oreparo, whose repair or acquisition depends on the purchase process and / or availability in suppliers.
Cyber attack	A virtual attack that compromises the performance, data, or configuration of the services and systems the company uses.
Information Leakage	Malicious user or attacker who manages to share information of employees, third parties and/or customers.

18.1. INTERRUPTION OF ELECTRICITY SUPPLY

These indications are aimed at the guidance and standardization of operating procedures in case of lack of electricity in the physical facilities of DMS LOGISTICS. They must be followed by all employees, regardless of hierarchical position.

DMS LOGISTICS, in its physical facilities,uses the electric energy coming from the electric power concessionaire. To minimize the risk of data loss and abrupt downtime due to lack of power, the company uses UPS scaled to current demand.

AllDMS LOGISTICS equipment is connected to the UPS, allowing for a safe shutdown operation.

If there is an interruption in the supply of electricity, they automatically start operating, allowing employees time to save work and shut down equipment safely.

The actions to be taken in this contingency plan are divided into four stages:

1. Check if the electrical breakdown has hit adjacent neighboring buildings. If so, go to step 3. If not, go to step 2;
2. Verify that the general key is unarmed. If so, the cause may have been an overload and it may be necessary to turn off non-essential equipment that requires more energy, such as air conditioning. If the problem has not been identified, call the power utility according to step 3;
3. With the installation number in hand or copy of the electric bill, call and report the situation to the Concessionaire, register the protocol number and check the forecast of energy restoration. Then proceed the step;
4. Turn off the equipment according to safety protocols and remove them from the outlets, to avoid overloading when the power returns.

The resumption of activities is conditioned on the restoration of electricity and the hours of operation of the company. Therefore, the management/coordination must evaluate the feasibility of resuming activities for the same day or for another day.

After the return of electricity, the equipment must be observed. If there is any abnormality, it should be reported to the industry leader. If necessary, the leader will communicate to the Committee on Security and Protection of Personal Data about the problem, requesting an analysis of the equipment.

DMS LOGISTICS does the preventive maintenance of its equipment. They are reviewed every 6 (six) months.

18.2. NETWORK/INTERNET UNAVAILABILITY

These indications are aimed at the orientation and standardization of operational procedures, incase of network and/or internet unavailability in the physical facilities of DMS LOGISTICS. They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

In case of network and/or internet unavailability, employees must follow the step-by-step below:

At the first indication of unavailability of network and / or internet, verify the occurrence of interruption in the supply of electricity; If so, with the installation number in hand or copy of the electric bill, call and report the situation to the Concessionaire, record the protocol number and check the forecast for energy restoration;

If the interruption in the supply of electricity is identified, check if UPS and generators are active;

If the UPS and generators are not active, activate them and wait for the necessary period to use the network equipment and / or internet and check if the unavailability has ceased;

If there is no interruption in the supply of electricity and/or the UPS and generators are active and it is identified that the unavailability of the network and/or i/oriternet remains:

Check if the unavailability of the network and/or internet is limited to only one device or all devices;

Disconnect the device(s) from the mains for one (1) minute and reconnect them. Wait for the period necessary for the use of network and/or internet equipment

If the unavailability of the network and / or internet persists, call the Information Technology (IT) department to check access conditions, firewall services and internet links.

Detected external internet problems, open a support call with the internet service provider, aiming at the restoration of service. Inform the forecast of the repair or solution to the other servers.

The Committee on Security and Protection of Personal Data will be convened and will determine the actions for disaster recovery and business continuity, according to the severity of the case.

18.3. HUMAN ERROR DUE TO RECKLESSNESS, MALPRACTICE OR NEGLIGENCE

These indications are aimed at guiding and standardizing operating procedures in case of human error at DMS LOGISTICS facilities. They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

- In case of human error, employees should follow the step-by-step below:
- At the first indication of human error, contact the Committee on Security and Protection of Personal Data and report the events;
- Then follow the Committee's guidelines;
- In the absence or delay in orientations, isolate the device from the network, shutting off the device and disconnecting all its cables;

The Committee on Security and Protection of Personal Data will be convened and will determine the actions for disaster recovery and business continuity, according to the severity of the case.

18.4. INSIDER ATTACKS

These indications are aimed at guiding and standardizing operational procedures in case of internal attacks on DMS LOGISTICS facilities. They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

In case of internal attack, employees should follow the step-by-step below:

- At the first indication of internal attack, immediately contact the Committee for Security and Protection of Personal Data and report the events;
- Then follow the Committee's guidelines;
- In the absence or delay in the orientations, isolate the device from the network, disconnecting the device and disconnecting all its cables;

The Committee on Security and Protection of Personal Data will be convened and will determine the actions for disaster recovery and business continuity, according to the severity of the case.

18.5. FIRE

These indications are aimed at the guidance and standardization of operating procedures in case of fire in the physical facilities of DMS LOGISTICS. They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

In case of fire, employees should follow the step-by-step below:

- At the first indication of fire, transmit the general alarm and immediately call the Fire Department by phone 193;
- If a short circuit is identified, turn off the general electrical switch;
- Remove all equipment from the outlet;
- If possible, use the fire extinguisher to fight the flames at the initial stage;
- Use the fire fighting equipment available in the common areas of DMS LOGISTICS;
- Not being able to eliminate the fire, leave the building quickly, by the stairs. When leaving, close all the doors behind you, without locking them;
- Do not use the elevator as an escape medium;
- Not being possible to leave the building by the stairs, remain on the floor on which it is, awaiting the arrival of the Fire Departments;
- In conditions of intense smoke cover your face with a wet handkerchief;
- Once you are safe, contact the Committee on Security and Protection of Personal Data and report the events.

The Committee on Security and Protection of Personal Data Will convene and determine the actions for disaster recovery and business continuity, according to the severity of the case.

18.6. NATURAL DISASTERS (FLOODS, STORMS)

These indications are aimed at the orientation and standardization of operational procedures, in case of flooding and storms that may compromise the physical facilities of DMS LOGISTICS.

They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

- Turn off the general electrical switch;
- Turn off all equipment from the power grid.

In case of flooding, in addition to the above steps, one should:

- Immediately close the water register, in case of disaster caused by hydraulic pipe rupture;
- Remove all electronic equipment, starting with the most sensitive, from the site of the damage;
- Remove the analog collection such as papers and files, out of place;
- Inform the Committee for Security and Protection of Personal Data;
- Call for help - Fire Department, Civil Defense, electric power concessionaire or professional qualified in hydraulics, according to the situation.

18.7. HARDWARE FAILURE

These indications are aimed at the guidance and standardization of operating procedures in case of hardware failure in the DMS LOGISTICS facilities. They must be followed by all employees, regardless of hierarchical position.

All Employees must know the step-by-step in this regulation and be able to execute it.

In case of hardware failure, employees should follow the step-by-step below:

- At the first indication of hardware failure, open a call to theInformation Technology (IT) department, informing the equipment, type of failure and date of occurrence;
- After opening the call for IT, contact the Committee on Security and Protection of Personal Data and report the events;

The Security andProtection of Personal Data will be convened and will determine the actions for disaster recovery and business continuity, according to the severity of the case.

18.8 CYBER ATTACK

These indications are aimed at the guidance and standardization of operational procedures in case of cyber attack on DMS LOGISTICS' facilities. They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

In case of cyber attack, employees should follow the step-by-step below:

- At the first indication of cyber attack, immediately contact the Committee on Security and Protection Of Personal Data and report the events;
- Then follow the Committee's guidelines;
- In the absence or delay in orientations, isolate the device from the network, disconnecting the device and disconnecting all its cables;

The Committee on Security and Protection of Personal Data will be convened and will determine the actions for disaster recovery and business continuity, according to the severity of the case.

18.9. INFORMATION LEAKAGE

These indications are aimed at guiding and standardizing operating procedures in the event of information leakage at DMS LOGISTICS' facilities. They must be followed by all employees, regardless of hierarchical position.

All employees must know the step-by-step in this regulation and be able to execute it.

In case of information leakage, employees should follow the step-by-step below:

- At the first indication of information leakage, immediately contact the Comitê of Security and Protection of Personal Data and DPO reporting the events;
- Then, follow the guidelines of the Committee and/or DPO;
- In the absence or delay in orientations, isolate the device from the network, disconnecting the device and disconnecting allits cables;

The Committee on Security and Protection of Personal Data and DPO will be convened and determine the actions for disaster recovery and business continuity, according to the severity of the case.

19. REVISION HISTORY

Revision	Data	Description
00	17/02/2023	Issuance of the document.
01	13/03/2023	Review and standardization of the 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