SUPPLIER SECURITY POLICY

MONTREAL

O FUTURO PRESENTE

The aim of this policy is to reduce the number of possible risks associated with access to Montreal data, information systems or resources by service providers, regardless of the type of work provided or the relationship linking the provider to Montreal (legal, contract-based or any other non-employment relationship), in order to protect the confidentiality, integrity and availability of Montreal Informática information and that of its customers.

This information security policy for suppliers must be an integral part of the service contract for all Montreal's critical suppliers. By signing the service contract, the supplier assumes full knowledge of and agreement with the guidelines set out in this document.

GENERAL POLICY PRINCIPLES

Whenever necessary, suppliers will provide Montreal with a list of people, their profile description, roles and responsibilities associated with the service provided, communicating any changes made to their relationship with the Organization (hiring, dismissal, replacement or change of roles or positions).

Suppliers must ensure that all their employees have the appropriate training and are duly qualified to carry out the service provided, whether specifically in relation to the fields that correspond to the activities associated with the provision of the service or with reference to information security.

Suppliers must guarantee, as a minimum, that all their employees associated with the service provided have been made aware of and undertake to comply with the terms of this policy. Montreal may request evidence of the process of disclosure of this information at any given time.

It is desirable that the supplier adopts and monitors good practices to ensure risk management throughout the supply chain, when it does not have any management certification.

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

- Suppliers must protect the confidentiality of all information provided by Montreal during the course of their business operations.
- Suppliers must implement appropriate controls to protect confidential information from unauthorized access, disclosure or misuse.
- Suppliers must implement appropriate controls to prevent unauthorized tampering, modification or destruction of information
- Suppliers must guarantee the continuous and reliable availability of the services provided to Montreal, as agreed in the supply contracts.
- All agreements to preserve the confidentiality and secrecy of information accessed before, during and after the provision of services must be respected and complied with.

© This document is the property of Montreal

Effective from: 01/15/2020 | Last updated: 04/16/2024.

SECURITY AUDITS AND ASSESSMENTS

Montreal reserves the right to conduct security audits and assessments on suppliers to ensure compliance with this policy and relevant security requirements.

Suppliers must allow Montreal to carry out any security audits requested, cooperating with the audit team and providing all required evidence and records.

The scope and depth of the audits will be expressly defined by Montreal, according to the supplier's needs and availability. And the results of inspections and assessments, as well as recommendations for improvement, will be recorded and forwarded for action by the supplier.

SECURITY INCIDENT NOTIFICATION

Service providers undertake to immediately report any incident or threat (observed or suspected) that is detected in Montreal's information systems or that may have affected information owned by Montreal or its clients, informing the Information Security Department at the e-mail address secmi.mg@montreal.com.br

COMPLIANCE WITH LAWS AND REGULATIONS

Suppliers must comply with all applicable laws, regulations and standards relating to information security, privacy and data protection.

USER RESPONSIBILITY

Each user who has access to Montreal information is responsible for the actions taken with their user identifier and all that is derived from it. It is therefore essential that each user maintains the authentication systems associated with their own identifier, ensuring that the corresponding code is known exclusively to the user themselves and must not be disclosed to any other person under any circumstances.

Users must not use any other user's identifiers, even if they have the owner's authorization.
Any user who has access to Montreal information must choose qualified passwords (of at least 8 characters, containing uppercase letters, lowercase letters, digits and special characters, and which do not contain any information that can be easily discovered).

Any user who has access to Montreal information must change the default and temporary passwords the first time they log in and at least every 30 days, as well as whenever there is a possibility that other users have become aware of the password.

© This document is the property of Montreal

Any user who has access to Montreal information must take precautions to ensure that equipment is protected when not under supervision.

Any user who has access to information must respect, as a minimum, the clean desk and clean screen rules, in order to protect paper documents, computerized media and portable storage devices, and reduce the risks of unauthorized access, loss and violation of information during normal working hours and outside of them.

When using Montreal's assets and facilities, the necessary care must be taken to preserve the property. It is everyone's duty to ensure the protection of assets and to adopt habits that avoid waste in general.

CHANGE CONTROL

Review	Date	Elaborator	Approval	Description of change
00	08/27/2020	C. Pontes	L. Alvarenga	Initial preparation
01	10/30/2022	M.Reis	L. Alvarenga	Layout change
02	12/18/2022	M.Reis	L. Alvarenga	Adequacy of the PSI's objective
03	04/16/2024	M.Reis	L. Alvarenga	General revision of the document 2022 version of ISOIEC27001

© This document is the property of Montreal