BARSALOU
LAWSON
RHEAULT

PL01 – Information security Policy

Policy - Information Security

Table of content

1 PREAMBLE

In order to conduct its business effectively, *Barsalou Lawson Rheault* (hereinafter "BLR") generates, stores, processes and communicates information in many forms. It recognizes that these information assets, essential to its business, must be assessed, used appropriately and adequately protected throughout their lifecycle. To this end, it is necessary to implement a coherent set of security measures determined by a security risk management approach based on best practices, in compliance with the legislative and regulatory requirements.

The information assets covered by this Information Asset Security Policy include not only information, but also equipment and media (paper or digital). They include data, documents, internal communication links, hosting sites, computers (IT), mobile devices and other portable equipment. The Policy represents a target to be achieved by BLR within 3 years of its adoption.

2 INTRODUCTION

2.1 DEFINITIONS

The definitions of the various terms used in this policy and in other associated documents are available in the Information Security Glossary.

2.2 OBJECTIVES

This document constitutes BLR's *Information Asset Security Policy* (hereinafter the "Policy") which establishes the practices to be adopted in order to comply to various legal and administrative obligations and to protect all information assets and prevent potential security incidents, including fraud, information leaks, computer attacks, accidental errors, deliberate actions and invasion of privacy. In this way, BLR protects its assets and mitigates risks related to the confidentiality, integrity, and availability of information.

2.3 SCOPE

This Policy applies to any information asset held by BLR and associated companies including information collected in the context of contractual, regulatory and legal activities.

Without limiting the foregoing, for the purposes of this Policy, the following will be considered as stakeholders of BLR, its staff, administrators, subcontractors, suppliers, partners and agents.

2.4 COMMITMENT OF THE MANAGEMENT COMMITTEE

This Policy is part of a prevention and awareness global approach toward information security. To do this, the collaboration of all stakeholders is essential. The management committee undertakes to take all the necessary means to support the actions that must be taken in the implementation of this Policy, as well as in the implementation of the associated frameworks.

2.5 POLICY AND SUPPORTING SECURITY FRAMEWORK OWNER

This Policy and the various associated security frameworks report to the Chief Information Security Officer (CISO). The CISO must ensure its maintenance, revision and communication.

2.6 MONITORING AND CONTROL OF INFORMATION SECURITY ACTIVITIES

In order to monitor its risk exposure, BLR must have a monitoring infrastructure and supporting processes in place. It must make it possible to constantly monitor the effectiveness of its methods, processes and protection mechanisms and to improve them according to the evolution of the risks facing BLR.

BLR reserves the right, without notice, to monitor any information assets and any information held, processed and executed on its systems and mobile devices. This privilege must always be conducted in accordance with the laws and when reasonable grounds recommend it.

2.7 CONSEQUENCES

Failure to comply with this Policy or associated security frameworks may cause BLR to withdraw access rights to an employee as well as to apply disciplinary or legal measures. Any stakeholder who becomes aware of the non-compliance or omission of this Policy must notify CISO or member of Management Committee.

2.8 COMPLIANCE WITH THE POLICY

The security requirements must be applied in support of the business needs of BLR and must in no case become a constraint without added value or which prevents BLR from offering its services to its customers.

Considering the above, it is possible that, in the course of normal operations, specific situations make it impossible to comply with certain information security requirements. In such a context, a clear procedure for managing non-compliance with security requirements is required to ensure that they are correctly analyzed, approved and followed.

3 GENERAL PRINCIPLES

3.1 INTERNAL ORGANIZATION

In order to ensure effective management of information security within BLR, it is important to define BLR organizational structure supporting the planning, development, implementation and control of security measures. The Management Committee is responsible for ensuring that BLR information security structure is defined and implemented.

3.2 ASSESSMENT AND MANAGEMENT OF RISKS RELATED TO INFORMATION ASSETS

The security measures put in place are based on the assessment, periodic analysis and treatment by BLR of risks relating to confidentiality, integrity and the availability of information.

A risk assessment must be performed before proceeding with the acquisition of new systems or making a change that may impact the security of BLR's information assets. In all cases, this assessment must be documented by following a defined process.

3.3 HUMAN RESOURCES SECURITY

BLR shall establish human resource security processes with the goal of reducing the risk of human error, theft, fraud or misuse of BLR's information assets prior to hire, during the period employment and after the employee leaves.

3.4 INFORMATION ASSET MANAGEMENT

In order to put in place and maintain appropriate protection, each information asset must be inventoried and assigned an owner who knows its value and its importance to the organisation. The owner will establish its classification according to its value and its importance to the organisation in order to establish an appropriate level of protection.

3.5 ACCESS CONTROL TO INFORMATION ASSETS

3.5.1 "NEED TO KNOW" PRINCIPLE

Information must only be disclosed to those persons who need this information in the course of their duties and in accordance with the legislative and regulatory obligations.

3.5.2 ACCESS MANAGEMENT

Access management must be conducted according to formal processes and procedures, agreed upon and communicated to the persons concerned.

When a user changes jobs (including dismissal, transfer, promotion or long-term leave), its manager must review its access.

The owners, in collaboration with the CISO, must ensure that a periodic review of user accounts is conducted.

3.5.3 ACCESS CONTROLS

Any information asset that keeps information not classified as public must have an active authentication mechanism to ensure that this information is not unduly disclosed, altered, deleted or made unavailable.

Users must have a unique identifier and must not share it under any circumstances.

3.6 PHYSICAL AND ENVIRONMENTAL SECURITY

All information assets must be protected by physical security measures based on their level of security, the associated risks as well as their value to BLR.

Access to office spaces and computer rooms containing information not classified as public must be physically limited by an appropriate security mechanism.

3.7 IT OPERATIONS MANAGEMENT AND TELECOMMUNICATIONS

Unless it has been designated as "public", all information must be protected from unauthorized disclosure to third parties. Third parties may have access to information not classified as public only if a need has been demonstrated and such disclosure has been authorized by the owner or by law.

3.8 ACQUISITION, DEVELOPMENT AND UPDATING OF SYSTEMS

The security requirements to be met during the acquisition, development, implementation and maintenance of an information asset must be determined. Security requirements must take into account technological developments and new security challenges.

3.9 INCIDENT MANAGEMENT

BLR must establish and define the responsibilities and procedures to be implemented in the event of a security incident in order to ensure an effective and relevant response while ensuring the establishment of a team capable of handling incidents.

3.10 DISASTER RECOVERY

BLR must implement an information technology recovery plan ("*Disaster recovery plan*") aimed at reducing the impact of an unavailability of an information asset and thus ensuring an IT recovery as soon as possible. Recovery measures must be checked periodically to ensure that they are effective and relevant.

3.11 TRAINING AND AWARENESS

BLR must educate employees about the threats and consequences of a security breach so that everyone can recognize risky situations and act on them.

An information security training and awareness program tailored to the different roles of employees must be defined.

It is the responsibility of BLR to provide anyone who needs to access information assets required guidelines to understand their responsibilities in terms of information security.

All relevant documents must be communicated to employees, including this Policy and the associated frameworks.

4 ROLES AND RESPONSIBILITIES

4.1 MANAGEMENT COMMITTEE

BLR's management committee is responsible for ensuring that adequate security frameworks are developed and maintained within the organisation. The committee is responsible for approving this Policy and taking all necessary means to implement it and the other associated documents.

4.2 CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO is BLR's primary representative for all matters relating to the security of information assets. Without limiting the generality of the foregoing, the CISO must, among other things:

- Report annually to the Management Committee on compliance with the Policy and submit a compliance report.
- Keep the Policy up to date according to the needs, obligations and concerns of BLR. Ensures the involvement of the various stakeholders in the development of this Policy and other associated frameworks.

- Define the security criteria for technologies used within BLR.
- Provide advice relating to IT security.
- Conduct risk and vulnerability assessments in all projects involving an information asset making it possible to define security needs to ensure the protection of information assets.
- Educate all users on information security.
- Ensure effective management of security incidents and the maintenance Disaster Recovery Plan (DRP) based on the Business Continuity Plan (BCP).

4.3 INFORMATION ASSET OWNER

The information asset owner is the manager of a business line of BLR. He is responsible, from a business point of view, for the information assets that are required to conduct the activities of its department such as:

- Determine the value of its information assets for its management and ensure their classification in accordance with it.
- Identify and ensure the implementation of security measures and controls to ensure the protection of information assets according to the assigned security level and risk assessments.
- Ensure the maintenance of security measures for all its assets throughout their life cycle (creation, maintenance, retention, destruction, etc.).
- Approve the allocation of access rights to the information assets under its responsibility according to the required needs.
- Ensure that a Disaster Recovery Plan, specific to its information assets, is in place and is tested on a regular basis.

4.4 USER OF INFORMATION ASSETS

The user of an information asset is a person who has been granted access to one or more of BLR's information assets by an owner. A user can be a permanent, temporary, administrator, contractor, consultant or third party.

When the value of the information asset justifies it, special arrangements with a third party (such as confidentiality agreements) must have been concluded prior to the contract award or assignment.

Its role consists, among others, of conducting the following tasks:

- Use information assets only for purposes expressly approved by the owner.
- Respect all the security measures in place.
- Refrain from disclosing information in their possession (unless it has been designated as public) without the prior permission of the owner.
- Inform the information security officer of all situations where he believes the security of an information asset is vulnerable or has been compromised.
- Comply with this Policy and any other document that refers to or supports it.

5 REVIEW AND APPROVAL

This Policy is effective upon adoption by the Management Committee and may be revised at any time by the Chief Information Security Officer (CISO).

Changes may be proposed by various BLR stakeholders, which must be submitted in writing to the Chief Information Security Officer (CISO).

This Policy should be reviewed at least every two years to ensure its relevance to BLR's mission, the activities of its users, and any substantial changes in legislation or regulatory requirements.

6 EFFECTIVE DATE

This Policy is effective as of August 1st, 2023. It supersedes all previous guidelines on this subject.