SOMUM Solutions Inc.
247 Notre-Dame East Street
Suite 150
Victoriaville QC G6P 4A2
819-758-6275

POLICY NAME	IT Security Policy				
EFFECTIVE DATE	10/03/2022	LAST REVISION DATE	09/05/2024	VERSION NUMBER	1.3

VERSION HISTORY				
VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0	Antony Carrière Stéphane Carrière	10/03/2022	First Version	Antony Carrière
1.1	Antony Carrière Pierre-Alain Gélinas-Girard	7/03/2023	Revision of Certain Points	Antony Carrière
1.2	Antony Carrière Félix Marier	20/03/2024	Addition of New Certifications	Antony Carrière
1.3	Antony Carrière Félix Marier	09/05/2024	Addition of Roles and Internal Responsibilities / Management of Waivers and Exceptions	Félix Marier

The use of the masculine gender in this document is solely intended to lighten the text and refers equally to both men and women.

SOMUM

Table des matières

1. Introduction

At SOMUM, security is of utmost priority. Our policy establishes the principles and measures we put in place to ensure the security of our systems, data, and the personal information of our users.

This policy aims to provide a general framework for access, use, and security of information technology at SOMUM. It defines the expected behaviors of users regarding the use of computer hardware, software, and access and use of the computer network (intranet and extranet).

It emphasizes the importance of ensuring the smooth operation of electronic processes to provide quality services. Its goal is to preserve the confidentiality, availability, integrity, and value of the company's IT assets.

2. Security Objectives

- Protect sensitive and personal data from unauthorized access.
- Prevent cyberattacks and security breaches.
- Ensure the availability, integrity, and confidentiality of systems and data.
- Comply with all laws and regulations regarding data protection.

This policy aims to achieve the following objectives:

- Ensure that users adhere to best practices and rules related to the use of information technology.
- Ensure rigorous enforcement of IT security standards.
- Conduct periodic reviews of audit results and controls to detect anomalies and potential incidents.
- Recommend actions to correct abnormal or hazardous situations, particularly concerning operational processes, major IT strategies, and equipment purchases.
- Inform SOMUM's executive committee about security-related activities, incidents, and efforts.
- Ensure compliance with operational elements requiring approval following various guidelines.

3. Legal and Regulatory Framework

- Charter of Human Rights and Freedoms (R.S.Q., c.C-12)
- Act Respecting the Protection of Personal Information in the Private Sector (LPRPSP)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Civil Code of Quebec (L.Q. 1991, c C-64)
- Copyright Act (RSC 1970, c C-42)
- Criminal Code (C-46)
- Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (R.S.Q., c.A-2.1)

4. Normative Framework

This policy is based on the international standard ISO/IEC 27002:2005, which establishes security techniques and best practices for information security management.

5. Definitions

To facilitate the understanding of this policy, here are some key terms defined:

Company: Refers to the legal entity, namely SOMUM.
Owner: Refers to a department, service, or administrative unit that is the primary user of an application. They are responsible for the use of the application and the processing of the information derived from it.

6. Scope of the Policy

This policy applies universally to all employees, affiliated organizations, and third parties who use SOMUM's technological infrastructures.

It outlines the fundamental principles that enable users to obtain the necessary permissions to perform their tasks securely.

7. Supporting Documents of the Policy

This policy consolidates the guidelines, rules, and regulations already approved by various bodies, including SOMUM's board of directors.

8. Data Ownership Policy

8.1. Introduction

The data ownership policy aims to establish the principles and guidelines governing data ownership within SOMUM. This policy defines the rights and responsibilities related to the ownership, use, and management of data generated, stored, or processed in the course of the owner's activities.

8.2. Definitions

- **Data:** Any information generated, stored, or processed in the course of the owner's activities, whether digital or in another form.
- **Data Owner:** The entity or legal person that holds ownership rights to specific data and is responsible for its appropriate use.
- **User:** Any person authorized to access, use, or manipulate data as part of their duties within the owner's business/organization.
- **Data Manager:** The designated person responsible for overseeing the management, security, and integrity of data within the owner's business/organization.

8.3. Data Ownership

8.3.1. **Ownership of the Company/Organization:** All data generated, collected, or processed in the course of the business/organization's activities (owner) is the exclusive property of SOMUM, except for information subject to the Copyright Act (RSC 1970, c. C-42).

8.3.2. **Exceptions:** Data subject to specific intellectual property rights remains subject to those rights, and its ownership is determined under applicable laws and regulations.

8.3.3. **Responsibility of the Data Owner:** The data owner is responsible for its use, security, and compliance with the policies and procedures of the owner.

8.4. User Responsibilities

8.4.1. **Appropriate Use:** Users must use the data only in the course of their professional duties and follow the policies and procedures of the owner's business/organization.

8.4.2. **Data Protection:** Users are required to protect the data from unauthorized access, misuse, and unauthorized disclosure.

8.4.3. **Compliance with Policies:** Users must comply with all data security policies and procedures established by the owner's business/organization.

8.5. Data Management

8.5.1. **Designation of a Data Manager:** A data manager is designated to oversee the management, security, and integrity of data within the owner's business/organization.

8.5.2. **Data Security:** The data manager is responsible for implementing appropriate security measures to protect the data from unauthorized access, alteration, or destruction.

8.6. Policy Enforcement

This policy applies to all employees, contractors, consultants, and third parties accessing or manipulating data on behalf of SOMUM.

8.7. Policy Review

The data ownership policy will be periodically reviewed and updated to reflect relevant legal, technological, and organizational developments.

8.8. Policy Adoption

This policy is adopted by the management of SOMUM and comes into effect from the date of its approval.

Effective Date: 10/03/2022

9. Information Classification Policy

9.1. Introduction

The information classification policy aims to establish a clear framework for the classification and protection of information within SOMUM. This policy defines the categories of information classification and the appropriate security measures for each category.

9.2. Categories of Classification

9.2.1. **Public:** Information in this category can be distributed without restriction both internally and externally at SOMUM. It is generally informative, and its disclosure is not likely to cause any harm or damage to the company.

9.2.2. **Private:** Information in this category is strictly reserved for internal use. Users may use it to perform their work, but its disclosure to the public could have indirect impacts on SOMUM.

9.2.3. **Confidential:** Information in this category must be protected by legal or contractual obligations. It is generally strategic and requires the highest level of security. Its disclosure could cause significant harm to SOMUM.

9.3. Classification Criteria

The classification criteria are determined by service managers (owners) who establish the access rights granted to users under their responsibility.

9.4. Examples of Confidential Information

1. Any information contained in a tax file.
2. Any confidential information as defined by the Act respecting access to documents held by public bodies and the protection of personal information (RLRQ, c. A-2.1).
3. Any confidential information as defined by Section 295 of the Excise Tax Act (RSC 1985, c. E-15).
4. Any information related to processing, verification, and control procedures in use.
5. All data, analyses, or results are included in reports produced under a contract.
6. Any other privileged information directly or indirectly related to a contract or concerning information that they may have become aware of during the execution of said contract.

9.5. User Responsibilities

Users of SOMUM, including subcontractors and employees, must adhere to the defined classification categories and take all necessary measures to protect information according to its classification.

9.6. Dissemination of Confidential Information

Users, including subcontractors and employees, must not make public announcements, issue press releases, or publish texts containing confidential information without prior authorization from the client's public relations director.

9.7. Adoption of the Policy

This information classification policy is adopted by the management of SOMUM and takes effect from its approval date.

Effective Date: 10/03/2022

10. Access to Information Technology Policy

10.1. Introduction

SOMUM's Access to Information Technology Policy aims to establish clear guidelines for the responsible access and use of the company's IT resources. This policy emphasizes the importance of user accountability and defines the fundamental principles governing the assignment of access codes.

10.2. User Responsibilities

10.2.1. Users are required to comply with the regulations, guidelines, and objectives established regarding access to and use of SOMUM's information technology.

10.2.2. Each user is responsible for the appropriate use of the IT resources made available to them and must take all necessary measures to ensure the security and confidentiality of information.

10.3. Assignment of Access Codes and Passwords

- **10.3.1.** All personnel must be registered with the Human Resources department to obtain an access code to SOMUM's technological resources, assigned based on their duties and activities.
- **10.3.2.** Access to systems must be promptly updated in the event of transfers or departures, in collaboration with the Human Resources department.
- **10.3.3.** The selection, use, and management of passwords must meet industry standards.
- **10.3.4.** The use of the network, including wireless networks, is strictly controlled to prevent unauthorized use of equipment, with appropriate configurations against intrusion attempts.

10.4. Remote Access

The management of Information Technology and Communications must ensure the following procedures:

- **10.4.1.** Configure the network to ensure a sufficient level of performance and reliability to meet system security requirements.
- **10.4.2.** Properly configure remote access hardware and software against intrusion attempts.
- **10.4.3.** Control remote access using robust identification, authentication, and encryption techniques.
- **10.4.4.** Grant remote access only to users or third parties who need it for their functions.

10.5. Monitoring and Tracking

- **10.5.1.** SOMUM reserves the right to monitor the use of the network and IT resources for security and compliance purposes.
- **10.5.2.** User activities may be monitored to detect any abusive or unauthorized use of IT resources.

10.6. Sanctions

- **10.6.1.** Any failure to comply with the rules outlined in this policy may result in disciplinary action, including the revocation of network access privileges.
- **10.6.2.** Serious violations may also be subject to legal measures and prosecution.

10.7. Adoption of the Policy

This Access to Information Technology Policy is adopted by the management of SOMUM and takes effect from its approval date.

Effective Date: 10/03/2022

11. Access to Applications Policy

11.1. Introduction

The Access to Applications Policy of SOMUM aims to ensure that each user has access to the information resources essential for performing their functions. This policy defines the processes and responsibilities related to access to the company's administrative applications.

11.2. Access to Administrative Applications

- **11.2.1.** Access to administrative IT applications is defined by the primary owner of each strategic application. The owner is ultimately responsible for access to their application.
- **11.2.2.** Access rights and roles are authorized by the owner, and the process for identifying and authorizing access is formal, either in writing or via dedicated software for this purpose.
- **11.2.3.** Access defined in the system and infrastructure must comply with the permissions indicated by the owner, and a periodic review of access rights must take place at least once a year.

11.3. Access to Critical Applications

- **11.3.1.** Applications deemed critical for SOMUM's operations require specific validation for access.
- **11.3.2.** Access to these critical applications is strictly controlled and can only be granted with the approval of the primary owner of the application and the management of Information Technology and Communications.

11.4. Identification and Authentication Procedures

- **11.4.1.** Each user must have a unique identifier to access administrative applications.
- **11.4.2.** Passwords must meet the company's security standards and be protected against any unauthorized disclosure.

11.5. Surveillance and Review of Access

- **11.5.1.** SOMUM conducts regular monitoring of access to applications to detect any anomalies or suspicious activity.
- **11.5.2.** A periodic review of access rights is carried out to ensure that only authorized users have access to the appropriate applications.

11.6. Adoption of the Policy

This Access to Applications Policy is adopted by the management of SOMUM and comes into effect as of its approval date.

Effective Date: 10/03/2022

12. Outsourcing and Third-Party Management Policy

12.1. Introduction

This policy applies to outsourced processes as well as the internal operations of SOMUM. Third parties, including subcontractors and external service providers, are required to comply with the requirements of this policy, as well as the security standards, technical documentation, and security procedures, just like SOMUM staff.

12.2. Third-Party Access to Strategic Software Applications

- **11.2.1.** Any access by third parties to strategic software applications must be authorized by the management of Information Technology, Telecommunications, and Communications.
- **11.2.2.** Each authorization of third-party access is recorded in a register managed by the management of Information Technology, Telecommunications, and Communications.

12.3. Responsibilities of Third Parties

- **11.3.1.** Third parties are required to comply with SOMUM's security policies and procedures when accessing the company's systems and data.
- **11.3.2.** Third parties must provide appropriate security assurances to protect SOMUM's confidential information from unauthorized access, disclosure, or alteration.

12.4. Audit and Monitoring

- **11.4.1.**SOMUM reserves the right to audit and monitor third-party activities to ensure compliance with the company's policies and security standards.
- **11.4.2.** Third parties must fully cooperate with SOMUM during security audits and provide all required information.

12.5. Adoption of the Policy

This outsourcing and third-party management policy is adopted by the management of SOMUM and comes into effect from its approval date.

Effective Date: 10/03/2022

13. Data Protection

1. Sensitive and personal data are encrypted when stored or transferred.
2. Regular backups are performed to prevent data loss in the event of a disaster.
3. Data is retained only for as long as necessary and is securely deleted when no longer needed.

14. Requirements

Users are required to comply with the fundamental requirements outlined in this policy, as well as the established security standards, relevant technical documentation, and current security procedures.

14.1. Security Program

This policy requires the IT, information technology, and communications management to implement a security program. This program coordinates all aspects of the policy and ensures its requirements are met. Its main functions include:

- General administration;
- Training and awareness;
- Asset identification;
- Security risk management;
- Access control;
- Security and reliability audits;
- Physical security;
- Information technology security;
- Emergency and threat management;
- Business continuity planning;
- Security incident investigations.

It is imperative for users to immediately report any security incident or violation of the policy by a user to management.

14.2. Training and Awareness

1. Develop and deploy a security awareness program to inform employees about their security responsibilities and provide them with regular reminders in this regard;
2. Communicate to employees the access privileges and restrictions associated with their roles.

All employees receive training on best practices for information security and are regularly made aware of potential threats. Employees are encouraged to report any security incident or potential violation of the security policy.

14.3. Proactive Analysis of Technological Threats

The IT, information technology, and communications management is responsible for protecting essential electronic information systems against evolving threats that could compromise the confidentiality, integrity, availability, intended use, and value of these systems.

This approach must be agile to respond to rapid changes and ensure service continuity. Therefore, IT, information technology, and communications management must implement fundamental security controls for constant monitoring to identify and analyze threats while establishing effective mechanisms to address them.

14.4. Use of Email and the Internet

Management implements security measures to protect SOMUM's network from intrusion threats, including deploying firewalls and antivirus software on servers and workstations.

Additionally, initiatives are established to raise awareness and guide staff on the appropriate use of email and the Internet. Downloading data from the Internet and opening email attachments must be done with caution to minimize the risks of executing malicious code.

It is essential to emphasize that the use of email and the Internet must be strictly professional and related to SOMUM's activities. Attachments to messages must be transmitted securely to avoid disclosing confidential or protected information.

14.5. Security of IT Facilities

The IT, information technology, and communications management is responsible for identifying areas that require restricted access. It installs security systems and the necessary equipment based on a threat and risk assessment.

Furthermore, management ensures that measures are implemented to protect both the IT equipment and the information contained within them.

Additionally, protocols are established to ensure the complete erasure of content from storage media containing classified and protected data, as well as licensed software, before their disposal.

14.6. Physical Security of the Workplace

Using IT equipment for purposes other than those necessary for SOMUM's operations is strictly prohibited. The IT, information technology, and communications management ensure that appropriate security measures are maintained to secure unattended workstations.

Moreover, users are responsible for taking all necessary measures to ensure the adequate protection of classified and protected information for which they are responsible.

14.7. Acquisition and Maintenance of Hardware and Software

Any acquisition of hardware or software products must be approved by the IT, information technology, and communications management. In this context, management ensures that:

1. The acquisition of new commercial products aligns with SOMUM's directives;
2. The acquisition and development of new products to consider security requirements;
3. New products are compatible with existing systems;
4. Used products are properly registered;
5. New software and updates are only applied after being tested and approved by the application owner.

14.8. Backup

The IT, information technology, and communications management implement adequate measures to protect SOMUM's information assets. This includes establishing a backup and recovery procedure, conducting recovery tests at regular intervals, storing copies in a separate physical location, and regularly monitoring backup equipment.

14.9. Business Continuity

To ensure the continuity of essential services, the IT, information technology, and communications management develops an IT continuity plan as part of operational continuity planning. This plan must include:

a) A framework defining the authorities and responsibilities for the development and approval of the continuity plan;
b) An impact analysis to prioritize essential services and assets;
c) Plans, measures, and preparations to maintain the ongoing availability of essential services and assets, as well as other services or assets identified by a threat and risk assessment;
d) Activities for reviewing, testing, and verifying the continuity plan.

Furthermore, management establishes a redundancy mechanism for critical components and ensures regular maintenance of equipment to guarantee the continuity of essential services in the event of a failure, without necessarily requiring the activation of the business continuity plan.

14.10. Security Incident Investigations

- The IT, information technology, and communications management establishes reporting and investigation procedures for security incidents and takes corrective actions to address them.
- In the event of a security incident, SOMUM has an incident response plan in place to mitigate damage, investigate the incident, and take the necessary corrective actions. Clients and relevant authorities are notified of any data breaches within the timeframes prescribed by law.

15. Disposal of Hard Drives and Other Storage Devices

Objective:
To ensure the irreversible destruction of sensitive data before disposing of hard drives and other storage devices.

Data Reformatting and Destruction:

15.1. Hard Drive Reformatting:

- Before disposal, employees must reformat the hard drives in such a way that the data becomes completely unrecoverable.
- The reformatting process must ensure the irreversibility of data deletion.

15.2. Destruction by an Approved Agency:

- If data reformatting proves impossible, the employee must contact a disposal agency that guarantees complete data destruction.
- This agency must be approved by the Security Director, Antony Carrière.

Secure Storage Before Destruction

15.3. Storage in Secure Lockers:

- Hard drives or any other devices pending disposal must be stored in secure lockers.
- Storage in these lockers must be maintained until direct transport to the approved disposal management partner.

15.4. Data Retention Period:

- Employees must not retain data for destruction for more than 24 hours under any circumstances.
- These 24 hours is deemed sufficient to remove the devices and dispose of them properly for disposal.

15.5. Responsibility:

- All employees are responsible for adhering to this policy to ensure the security and confidentiality of company data.
- Failure to comply with this policy may result in disciplinary action under company regulations.

This policy must be read and understood by all relevant employees, and training will be provided to ensure its proper implementation.

16. Compliance and Audit

SOMUM complies with all applicable laws and regulations regarding data protection, including the GDPR. Regular audits are conducted to assess the effectiveness of security measures and ensure that all requirements are met. For instance, for the financial sector, the firm Okiok has verified the systems and conducted penetration testing.
www.okiok.com

17. Certifications

1. TIER III
2. SSAE 16, SOC II / Type II
3. CSAE 3416 (NCMC 3416 in French)
4. PCI Security Standards Council, Data Security Standard (DSS)
5. Certified Protected A by the Government of Canada
6. TGV Certification

18. End of Employment and Return to Organization Assets

Upon termination of their employment or contract, users, employees, and contractors are required to return all organization assets entrusted to them. This includes, but is not limited to, the following:

18.1. Computer Hardware:
Laptops, desktops, tablets, mobile phones, USB drives, and any other computer equipment or peripherals belonging to SOMUM.

18.2. Software and Licenses:
Any software, licenses, or access keys assigned to the user during their employment or contract.

18.3. Documents and Data:
All physical or electronic documents, as well as confidential or proprietary data and information of SOMUM.

18.4. Access Cards and Identifiers:

Physical access cards, login identifiers, passwords, and any other means of access to SOMUM's systems or premises.

18.5. Other Organization Property:

Any other property or materials provided by SOMUM to the user during their employment or contract.

It is the user's responsibility to take the necessary steps to return these assets in an appropriate condition and within the timelines specified by SOMUM. Any failure to meet this obligation may result in disciplinary or legal consequences.

19. Use of Removable Media and USB Drives

Removable media, including USB drives, must never leave the workplace, except in exceptional and authorized cases. These cases only include the transmission of bid documents, which must be placed in a sealed envelope to ensure the security of the information.

The use of removable media is governed by the requirements arising from the classification of the information contained within. Any employee handling removable media must adhere to the information classification policies and take appropriate measures to ensure the security and confidentiality of the data during their use.

20. Roles and Responsibilities in Internal Personnel Security

SOMUM is a small team, and we have delegated the responsibility for security, planning, and the management of personal information to two key individuals: Antony Carrière and Pierre-Alain Gélinas-Girard. Antony serves as the responsible officer, while Pierre-Alain is his deputy. In all cases, whether for the management of waivers or exceptions, it is Antony or Pierre-Alain who are tasked with these responsibilities.

20.1. Responsibilities of Information Security Personnel:

- Develop, implement, and maintain information security policies, standards, procedures, and guidelines.
- Oversee and control access to computer systems, networks, and sensitive data.
- Identify and assess potential risks to information security.
- Ensure awareness of information security within the organization.
- Manage information security incidents and related investigations.
- Conduct regular information security audits.

20.2. Responsibilities of Enterprise Personnel:

- Report any violation of the information security policy to the information security team.
- Adhere to the organization's information security policies, standards, procedures, and guidelines.
- Protect login credentials and passwords and do not share them with others.
- Report any suspicious activity or information security breach.

21. Management of Waivers and Exceptions

21.1. Waiver Management Procedure:

21.1.1. Any request for a waiver of the information security policy must be submitted to the information security team for evaluation.

21.1.2. The information security team assesses the waiver request based on its potential impact on information security.

21.1.3. Once evaluated, the information security team communicates its decision to the requester.

21.1.4. If the waiver is approved, it is documented, and compensatory measures are implemented to mitigate potential risks.

21.1.5. All approved waivers are periodically reviewed to determine if they remain appropriate.

21.2. Exception Management:

21.2.1. Any exception to the information security policy must be submitted to the information security team for evaluation.

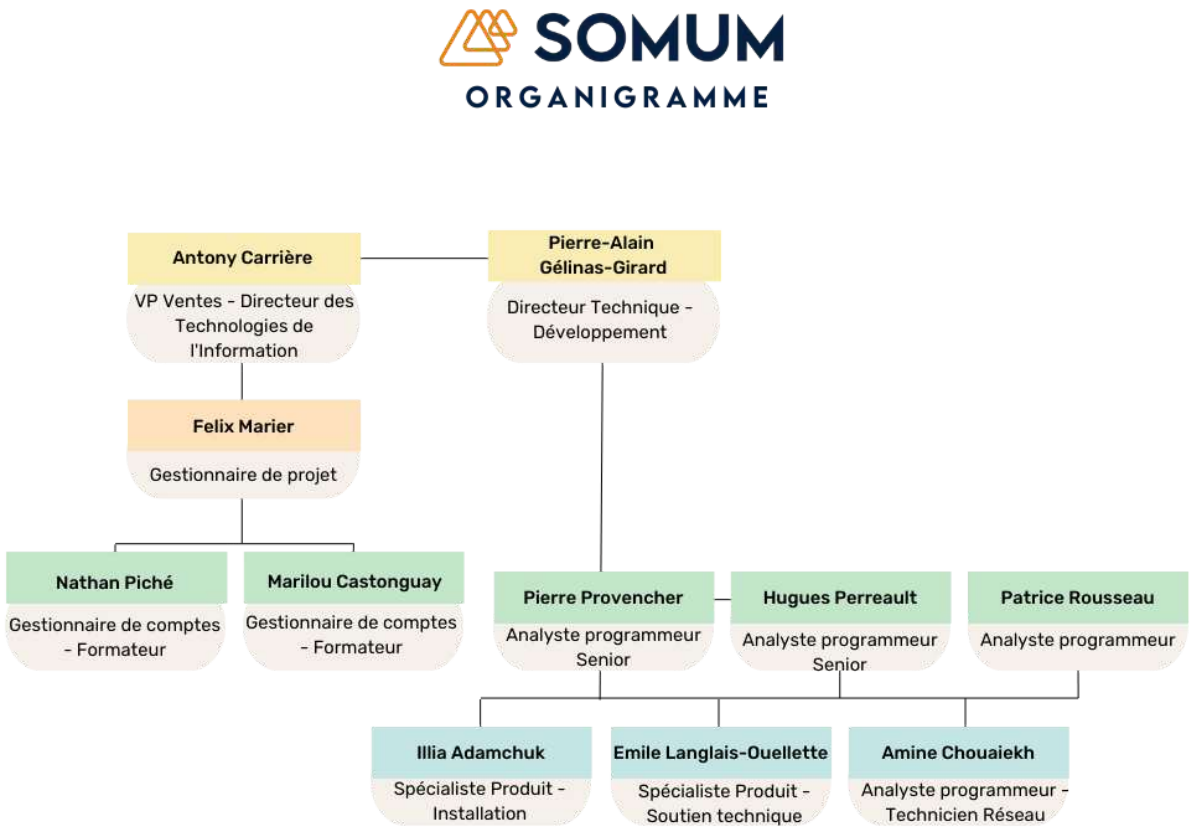
21.2.2. The information security team assesses the exception based on its impact on information security and the proposed compensatory measures.

21.2.3. Once evaluated, the information security team communicates its decision to the requester.

21.2.4. If the exception is approved, it is documented, and compensatory measures are implemented to mitigate potential risks.

21.2.5. All approved exceptions are periodically reviewed to determine if they remain appropriate.

22. Organizational chart



SOMUM
ORGANIGRAMME

Antony Carrière	DIRECTEUR DE LA SÉCURITÉ DE L'INFORMATION	Responsable de la supervision générale de toutes les activités de sécurité de l'information.	Définit les politiques de sécurité de l'entreprise et veille à leur mise en œuvre.	Dirige les évaluations des risques et les audits de sécurité.
Pierre-Alain Gélinas-Girard	RESPONSABLE DE LA SÉCURITÉ DE L'APPLICATION ET DES ACTIFS	Chargé de superviser la sécurité de l'application SOMUM et des actifs informatiques associés.	Assure la conformité aux politiques de sécurité établies par le directeur de la sécurité de l'information.	Gère les incidents de sécurité et les enquêtes en cas de violation de la sécurité.
Amine Chouaeikh	ANALYSTE PROGRAMMEUR - TECHNICIEN RÉSEAU	Responsable de la mise en œuvre des mesures de sécurité techniques.	Surveille en permanence les systèmes et les réseaux pour détecter les menaces potentielles.	Répond aux incidents de sécurité et met en œuvre des correctifs de sécurité.

23. Secure Programming Recommendations

As part of our IT security policy, we place paramount importance on secure programming. All our programmers must comply with the recommendations of OWASP (Open Web Application Security Project) to ensure the security of our applications.

Recommended Practices

- Programmers should regularly refer to OWASP guidelines to ensure that their programming practices meet the highest security standards.

23.1. Guarantee Methods

To ensure compliance with these recommendations, we have implemented the following measures:

1. **Regular Technical Meetings:** At each technical meeting involving all technical staff, the chosen security methods are shared and discussed ensuring a common understanding and uniform adherence to best security practices.

2. **Regular Code Reviews:** Regular code reviews are conducted by peers to ensure that security recommendations are followed in all software developments.

3. **Ongoing Training:** Our technical staff participates in regular training on best secure programming practices and is kept informed of the latest trends and threats in IT security.

By following these practices, we are committed to ensuring the security and reliability of our applications, effectively protecting our users' data against potential threats.

24. Review and Update

This security policy is periodically reviewed and updated to reflect changes in security threats, technologies, and regulations.

25. Policy Enforcement

Non-compliance with this security policy may result in disciplinary action, including termination, as well as legal action in the event of violations of applicable laws and regulations.