Security

is everyone's responsibility!

Desjardins

April 2025

Table of contents

The Desjardins Group Security Office is responsible for supporting the entire organization in identifying and responding to all types of security challenges.

Mission of the Desjardins Group Security Office

The mission of the Desjardins Group Security Office (DGSO) is to protect Desjardins Group members and clients, their assets and their personal information. The DGSO is responsible for identifying and responding to all types of security challenges in any manner of situations.

The DGSO is headed up by Desjardins Group's Chief Security Officer, who reports to the Senior Executive Vice-President and Chief Operating Officer.

Currently, more than 1,700 professionals work in the DGSO, all experts in their respective fields. In addition to fulfilling its main mission, the DGSO ensures Desjardins Group's different business sectors are adequately supported and fosters greater organization-wide awareness about security. It also also ensures consistency in different security practices for:

- Fraud prevention
- Financial crime prevention
- Personal information protection
- Data governance
- Information security
- Physical security

Accomplishments

Desjardins Group continually invests in security enhancements to address the risks it faces. The DGSO takes a rigorous approach to improving operational control and the efficiency of its teams, all in the name of better protecting Desjardins Group's members and clients.

Throughout 2024, Desjardins Group continued to show its commitment to helping our employees and members and clients adopt security best practices and reflexes. This is reflected in the following DGSO's accomplishments.

2024 – Fraud and Security Awareness Campaign

Building on the campaign launched in September 2023, Desjardins Group carried on its communications initiative targeting members and clients to continue strengthen their trust. Various communications went out on social media, radio and television. Some were even placed inside seniors' residences.

The topics covered included phishing, romance scams, phone scams, classified ad scams, investment fraud, fake supplier scams and CEO fraud (business executive scams).

January 2024 – Data Privacy Week

From January 22 to 26, 2024, Data Privacy Week was observed across Canada. Desjardins Group highlighted this event by offering several activities to help employees review personal information protection best practices.

March 2024 – Fraud Prevention Month

Desjardins Group offered its employees activities designed to help sharpen awareness about fraud. A special newsletter issue devoted to fighting fraud was also published to help employees deepen their understanding of security issues.

July 2024 – Summer security campaign

Every week during the summer months, Desjardins Group employees got to solve a new challenge to help raise awareness about fraud and security. The weekly challenges sparked discussions between employees and their colleagues.

September 2024 – *An Act to modernize legislative provisions as regards the protection of personal information* (Law 25)

On September 22, 2024, when the most recent provisions of Quebec's Law 25 came into force, Desjardins Group promptly complied with them. All members, clients and employees can now exercise their right to data portability. We created a FAQ to help employees distinguish between the different types of requests that members and clients can make under Law 25.

October 2024 – Cyber Security Awareness Month

Throughout the month, we organized several activities focused on phishing, including a quiz, to help employees learn more about the subject and be on the look out for phishing threats in their professional and personal lives.

Mandatory security training

Security is everyone's responsibility!

Desjardins Group's commitment to security extends to its people. The organization has an engaged workforce equipped with the tools and accountability needed to implement robust and thorough security processes.

Mandatory training for all employees and consultants

All Desjardins Group employees and consultants must take the following mandatory training :

- Introduction to Security - This training path has 7 videos to help employees learn about the different security practices overseen by the DGSO.
- Protecting Personal and Confidential Information Is Everyone's Business! - This course teaches employees how to identify personal information and confidential information, understand the roles and responsibilities of the organization and its employees.
- Privacy Policy and Consents - This course recaps the evolution in Desjardins Group's privacy policy and how to distinguish the different types of consent to better guide members and clients on a daily basis.
- Preventing Fraud - This training teaches employees how to recognize situations of external and internal fraud.
- Committing to the fight against tax evasion - This training explains the role Desjardins Group plays in fighting tax evasion.
- Committed to the Fight Against Money Laundering and Terrorism Financing - This training explains the role Desjardins Group plays to counteract money laundering and terrorist financing activities.
- Complying with International Economic Sanctions Obligations - This training explains Desjardins Group's role in applying international economic sanctions and measures.
- Fire Alarm Evacuation - This training covers the key aspects of preparing for and dealing with emergencies, including when an evacuation during a fire alarm is necessary.

Continuous training program

In addition to the mandatory security training mentioned above, there is also a mandatory continuous training program that changes every year. The program helps employees stay vigilant and knowledgeable about security.

In 2024, the continuous training program covered subjects including fire alarm evacuation best practices; detecting data exfiltration situations; scam indicators; work environments deemed secure for protecting confidential information; and preventing, detecting and responding to corruption.

Mandatory security training

Security is everyone's responsibility!

Mandatory training for managers

The following training courses are mandatory for managers. It is also available for all Desjardins Group employees and consultants :

- Desjardins Identity and Access Management (IAM): A Specific Training Program Designed for Managers! - This course covers identity and access management best practices and the responsibilities of managers.
- Anti-Corruption – This course explains what corruption is and teaches employees how to recognize high-risk situations and respond appropriately. The aim is to protect the organization and do what's best for members, clients and communities.

Mandatory security training for board members

Security is everyone's responsibility! training is mandatory for all Desjardins Group board members, no matter which board they serve on.

This training covers the potential consequences of non-secure practices and the main risks for the organization, and explains how board members can apply appropriate security measures to rectify high-risk situations.

Mandatory training for DGSO employees and consultants

All DGSO employees and consultants are required to complete the courses listed below. They're also mandatory for other Desjardins Group employees and consultants if the topic is specific to their job:

- MISSION POSSIBLE: Fighting Money Laundering and Terrorist Financing and BEHIND THE SCENE: Fighting Money Laundering and Terrorist Financing - These courses help employees identify and understand how and where criminal activities related to money laundering and terrorist financing take place.
- Anti-corruption - The training mentioned above, which is mandatory for all Desjardins Group managers, is also required for DGSO employees.
- Unusual Operation Notification - This course is designed to help employees be more vigilant about reporting unusual transactions and events. The aim is to better protect the organization's reputation by ensuring regulatory compliance.
- Introduction to Data Governance - This course explains what data governance is and why it's important for Desjardins employees to do their part.

Mandatory security training

Security is everyone's responsibility!

Phishing tests

As part of its ongoing awareness program, Desjardins Group continued to regularly send out phishing tests to employees and board members in 2024. These tests are designed to make employees and board members more aware of phishing.

In 2024, the difficulty factor for the phishing tests kept increasing and Desjardins Group gave employees the opportunity to voluntarily take an additional test in March as part Fraud Prevention Month. New threats have been added to the tests to represent the latest phishing methods, such as QR code phishing. Personalized tests targeted by business sector were also sent to sharpen employee reflexes.

Security for Everyone dashboard

The Security for Everyone dashboard is available to all Desjardins employees. This educational platform includes mandatory training as well as continuous training activities, informative videos and useful resources. It also allows managers to monitor their employees' security posture. Completing the mandatory security training activities and responding to phishing tests have an impact on our security posture.

In 2024, Desjardins Group continued to optimize the Security for Everyone dashboard to personalize the experience for employees based on their expertise and get an overview of their security profile.

Security Forum

The DGSO held the 16th and 17th editions of its Security Forum in March and October 2024. This semi-annual event is open to all employees. It's designed to give them the tools they need and help them adopt secure practices on a daily basis. Internal and external experts give talks on current topics.

The 3 lines of defence and external audits

In line with industry best practices, Desjardins Group uses a 3 lines of defence model. The DGSO is part of the first line of defence.

To ensure effective protection mechanisms and security, the DGSO has an organizational structure that fosters collaboration, transparency, and the sharing of security data between its security practices.

The DGSO prepares quarterly integrated security reports in connection with Desjardins Group's risk management reporting. These reports are intended for the Desjardins Group's governance bodies.

Desjardins Group's second line of defence provides governance and oversight of the DGSO's operations. This role is assumed by the Risk Management Executive Division.

The Desjardins Group Monitoring Office is the third line of defence. It provides an independent assessment of the relevance and effectiveness of the management framework. As required by regulations, it also conducts an independent compliance assessment of each of Desjardins Group's reporting entities every 2 years.

Desjardins Group is periodically audited by regulatory authorities to ensure compliance with its legal obligations. In addition, external audits are conducted by independent entities using standard control frameworks. These audits make it possible to certify compliance with standards such as ISO 27001, an international standard for information security management systems.

Chief officer roles

at Desjardins Group

Chief Anti-Money Laundering Officer and Head of Economic Sanctions:

Responsible for ensuring sound management of risks associated with money laundering, terrorist financing and international economic sanctions. The organization's program, policies, procedures and training are regularly adjusted, mainly to reflect regulatory changes. These measures help detect and report transactions associated with money laundering and terrorist financing.

These roles are assumed by senior management

Chief Anti-Corruption Officer:

Responsible for overseeing the implementation of control measures to mitigate corruption risk, with support from a specialized team. Desjardins Group has a strict anti-corruption policy and endeavours to comply with all applicable laws and maintain the public's trust. The organization's anti-corruption framework is designed to prevent, identify, assess, handle, report and impose penalties for cases of corruption, in compliance with best practices and applicable laws.

Chief Anti-Tax Evasion Officer:

Responsible for overseeing the organization's regulatory compliance program, including compliance with the intergovernmental agreement between Canada and the United States, known as the Foreign Account Tax Compliance Act, and the Common Reporting Standard developed by the Organisation for Economic Co-operation and Development. These require Desjardins Group to obtain tax residence and US citizenship information from members and clients, where applicable, and report it to the Canada Revenue Agency every year.

Chief officer roles

at Desjardins Group

Chief Information Security Officer:

Responsible for overseeing Desjardins Group's cybersecurity strategy. This role involves defining, developing and evaluating the effectiveness of the governance framework to address information security risks. It also involves making sure that Desjardins Group's actions are in line with the governance documents it issues. The Chief Information Security Officer also determines the investments required to mitigate information security risks and plans these accordingly. The role also involves developing and updating information security awareness materials for Desjardins Group employees.

Chief Data Officer:

Responsible for providing leadership, structure, expertise and direction to encourage stakeholders across the organization to recognize data as a strategic asset and to manage data in the best interests of Desjardins Group's members and clients.

Chief Privacy Officer:

Responsible for implementing and overseeing Desjardins Group's personal information protection program to ensure that personal information is handled in compliance with applicable laws.

Chief Fraud Prevention Officer:

Responsible for a management framework that encompasses fraud prevention, detection and response to internal and external fraud. This framework considers the life cycle of members and clients, employees, managers, board members, suppliers and Desjardins products. This provides a 360° view that helps the organization protect its people and assets. The approach to fraud prevention is continually updated in response to new threats.

Key governance documents

at Desjardins Group

The DGSO implemented the Desjardins Group Security Policy, which provides a general framework for developing an organization-wide awareness of security and ensuring consistency across security practices. Each security practice is also supported by tactical and operational governance documents to ensure operations run smoothly and strategies are applied effectively. Desjardins Group regularly updates all of its governance documents and enforces strict compliance with them.

General frameworks

- Desjardins Code of Professional Conduct[1]
- Conflict of Interest Management Policy/Directive
- Policy on Fraud, Financial Crimes and Physical Security Risks

Fraud prevention

- Rule on Security and Credit Checks
- Rule on the Authentication of Members, Clients and Prospects

Personal information protection

- Privacy Policy

Physical security

- Desjardins Group Rule on Physical Security

Desjardins Group data governance

- Directive on Data Quality

The DGSO's governance framework is based on 2 international information security governance frameworks: ISO 27000 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Information security

- Information Security and Technology Risk Management Policy and Directive
- Desjardins Group Information Security Policy and Directive
- Acceptable Use of Information Technology Directive
- Desjardins Group Rule on Identity and Access Management
- Desjardins Group Rule on Information Security Classification
- Desjardins Group Rule on Information Security for Supplier Relationships in the Context of Products and Services Acquisitions
- Electronic Monitoring Rule

[1] Every year, all Desjardins Group employees must sign a commitment to comply with this code.

Partnerships

to boost cybersecurity research and innovation

Desjardins Group collaborates and builds security partnerships with industry peers to promote research and innovation in the field. The organization also helps develop local talent.

- As of June 2024, Desjardins Group's involvement with CyberCap and Cybereco helped raise awareness about digital security among 10,103 young people ages 12 to 17. In the space of 3 years, Cybereco ran its Citizenship in the Digital Age and Cybersecurity program more than 402 times. The program encourages young people to choose careers in IT and gets them thinking about how they use technology.

- Desjardins Group is continuing its partnership with Université de Montréal's Research Chair in Cybercrime Prevention, which contributes to the advancement of research on cybercrime.

- Desjardins Group's continuing partnership with Université du Québec à Chicoutimi (UQAC) is to develop computer systems to ensure cyber defence.

- Desjardins Group is backing the launch of 4 new research projects as part of Polytechnique Montréal's Sentinel MI initiative. The goal of these research projects is to help identify, analyze, automate and prevent internal threats.

Partnerships

to boost cybersecurity research and innovation

- The Safari de l'innovation event returned for a third year, giving 6 innovative organizations an opportunity to meet with DGSO employees and present new solutions and approaches to emerging security technologies.

- Once again, Desjardins Group was one of the main sponsors of the Cybereco Cyberconference this year. The event provided an opportunity for cybersecurity experts from the DGSO, including the Chief Information Security Officer, to hold talks and workshops on current topics in the field.

- Many Desjardins Group experts are involved in cybersecurity communities. They participate in cybersecurity events such as InCyber Forum, NorthSec Conference, Hackfest and Canada FinTech Forum. Some experts are also involved in conferences on financial crime prevention, such as those organized by Info-Crime Montréal and the Association of Certified Anti-Money Laundering Specialists (ACAMS).

- And last but not least, Desjardins Group, along with the Department of Finance Canada, is engaged in strategic discussions that focus on money laundering and terrorist financing. In its capacity as co-chair of the Advisory Committee on Money Laundering and Terrorist Financing[2], Desjardins Group encourages collaboration and transparency between the public and private sectors.

[2] Desjardins Group is represented on the Committee by its Chief Anti-Money Laundering Officer and Head of Economic Sanctions.

Desjardins