## Draft Regulation

Act respecting the governance and management of the information resources of public bodies and government enterprises
(chapter G-1.03)

**Terms and conditions of application of sections 12.2 to 12.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises**

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting the terms and conditions of application of sections 12.2 to 12.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises, appearing below, may be made by the Government on the expiry of 45 days following this publication.

The draft Regulation provides for the terms and conditions of application of sections 12.2 to 12.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03) that deal with information security and allows the coming into force of those provisions.

The draft Regulation sets out the rules applicable to public bodies concerning their obligations to ensure the protection of the information resources and information under their responsibility and, in the event of a breach, whether actual or apprehended, of the confidentiality, integrity and availability of such information resources or information, to take measures to correct the impacts or reduce the risk of such a breach. The draft Regulation further provides, in the area of cybersecurity, that communication activities be carried out by cybersecurity practitioners and that special rules be applied when personal information is communicated or such information is to be communicated outside Québec.

Study of the draft Regulation shows no impact on the public or on enterprises considering the objective of ensuring the protection of their information.

Further information on the draft Regulation may be obtained by contacting Christiane Langlois, Senior Director, Direction principale de la sécurité de l'information gouvernementale, Sous-ministériat adjoint à la sécurité de l'information gouvernementale et à la cybersécurité, Ministère de la Cybersécurité et du Numérique, 880, chemin Sainte-Foy, 3e étage, Québec (Québec) G1S 4X4; email: christiane.langlois@mcn.gouv.qc.ca.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to the Minister of Cybersecurity and Digital Technology, 900, place D'Youville, 9e étage, Québec (Québec) G1R 3P7; email: cabinet@mcn.gouv.qc.ca.

Éric Caire
*Minister of Cybersecurity and Digital Technology*

## Regulation respecting the terms and conditions of application of sections 12.2 to 12.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises

Act respecting the governance and management of the information resources of public bodies and government enterprises
(chapter G-1.03, s. 22.1.1)

**DIVISION I**
INTRODUCTORY

**1.** In this Regulation,

(1) "security event" means any form of breach, present or apprehended, such as a cyber attack or a threat to the confidentiality, integrity or availability of information or an information resource under the responsibility of a public body;

(2) "cybersecurity practitioner" means the government chief information security officer, the deputy chief information security officer or a public body's personnel member assigned to functions in the field of cybersecurity;

(3) "Act" means the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03);

(4) "Minister" means the Minister of Cybersecurity and Digital Technology;

(5) "administrative unit specialized in information security" means the Centre gouvernemental de cyberdéfense referred to in section 12.5 of the Act or a cyber defence operations center referred to in section 9 of the Directive gouvernementale sur la sécurité de l'information, approved by Décret 1514-2021 dated 8 December 2021 (2021, G.O. 2, 7694).

**2.** This Regulation applies to the public bodies listed in section 2 of the Act.

**DIVISION II**
INFORMATION SECURITY OBLIGATIONS

**3.** A public body must manage effectively the security of information resources and information it holds, in particular by putting in place cybersecurity measures, including cyber defence mechanisms, to ensure the diligent taking charge of security events.

A public body must also follow good practices in information security in order to reduce risks of a breach to an acceptable level.

**4.** A proactive cyber defence team must be established and maintained within an administrative unit specialized in information security. Such a team is charged with testing applicable cybersecurity measures, including cyber defence mechanisms, and seeing to the handling of security events related to cybersecurity.

**5.** The Centre gouvernemental de cyberdéfense referred to in section 12.5 of the Act may provide its services to another administrative unit specialized in information security or a public body to carry out cybersecurity activities, such as penetration tests.

**6.** A public body must, during each security event, assess the risk of such an event by taking into consideration the sensitivity of the information resource or information concerned, the apprehended consequences of its use and the probability that it be used in particular for harmful purposes.

**DIVISION III**
COMMUNICATIONS BETWEEN CYBERSECURITY PRACTITIONERS

**7.** The communications provided for in the third paragraph of section 12.2 and section 12.3 of the Act must be made by any means that provides proper protection. They may be made using automated systems in the form, for example, of bulletins or warnings.

Where a security event is related to cybersecurity, the activities allowing the communications referred to in the first paragraph are carried out by cybersecurity practitioners as part of their respective responsibilities.

For such an event, the communications referred to in the first paragraph must be based on the obligation to take cybersecurity measures to follow good practices generally recognized by international benchmarks, such as ISO standards or the National Institute of Standards and Technology (NIST) benchmark.

**8.** The information that is the subject of the communications referred to in section 7 may include personal information.

Where personal information may be communicated in a form that does not allow the direct identification of the person concerned, it must be communicated in that form.

The second paragraph does not apply where there are grounds to believe that there is urgency to act in a matter of cybersecurity or that there is a risk that irreparable harm may be caused to an information resource or information under the responsibility of a public body. In that case, public bodies share the personal information concerned through their cybersecurity practitioners, by applying measures that ensure the confidentiality of such information.

There is urgency where the impact of a security event must be corrected or risks due in particular to the severity of the apprehended consequences must be reduced. A malicious software, phishing or an information leak may be a cause of the urgency.

**9.** The communications referred to in this Division are for the benefit of the public body responsible for ensuring the security of its information resources and information it holds or for the benefit of the person concerned by the personal information that is the subject of a breach or a risk of a breach.

**DIVISION IV**
COMMUNICATIONS OUTSIDE QUÉBEC

**10.** An agreement referred to in section 12.4 of the Act, concerning the communication of information outside Québec, must

(1) identify the representatives authorized to make the communications between the parties;

(2) limit access to the information only to authorized representatives, where the information is necessary in the performance of their duties;

(3) include protection and security measures to ensure the protection of the information to be communicated;

(4) provide for obligations related to the preservation and destruction of the information;

(5) provide that the Minister is to be immediately notified of any violation of or attempt to violate any of the obligations set out in the agreement by any person and of any event likely to affect the confidentiality of the information.

**DIVISION V**
MISCELLANEOUS AND FINAL

**11.** Any agreement referred to in section 12.4 of the Act, entered into with any person or body in Canada or abroad before (*insert the date of coming into force of this Regulation*) and approved by an order in council made under the first paragraph of section 3.8 of the Act respecting the Ministère du Conseil exécutif (chapter M-30), is deemed to fulfil the conditions set out in section 10.

**12.** This Regulation comes into force on the fifteenth day following the date of its publication in the *Gazette officielle du Québec*.

105622