Issued: 2021-06-01	**Section:** **Subsection:**	CYBERSECURITY AND TELECOM CYBERSECURITY	**Issuer:** Cybersecurity
Replaces: N/A	**Subject:**	Directive regarding the responsible disclosure of security vulnerabilities	**Approved:** December 7, 2021 **Effective:** December 7, 2021

BACKGROUND

The Société des alcools du Québec (SAQ) agrees to the responsible disclosure of security issues found on its websites, in its applications and in its information technology infrastructure, including cloud technologies. We are committed to protecting Quebecers' personal data and appreciate the community's support in helping us fulfill this mission.

The SAQ acknowledges that the community of security experts may be of assistance in reinforcing the corporation's security posture.

However, in view of the mission of our systems, this does not mean that the SAQ condones the use of active search techniques for uncovering security flaws during peak traffic periods. The SAQ has implemented procedures appropriate for this type of activity.

GUIDELINES REGARDING ACTS PERFORMED IN GOOD FAITH

The purpose of this directive is to specify how breaches should be investigated and disclosed.

1) Subject to the other conditions mentioned herein, the SAQ will not take legal action against a person who has uncovered a security flaw while acting in good faith and taking reasonable means to prevent its publication, any data tampering or unauthorized access to the SAQ's various services.
2) In the case of a security flaw that potentially provides access to personal data, please contact us immediately and cease any further investigation.
3) The SAQ does not agree that you may store or extract data.
4) You must never publish non-public SAQ data obtained during your investigations.
5) We try to reply via email in the 72 hours following disclosure of the flaw to our teams. We also aim for a 72-hour response time if you report a flaw possibly involving the execution of remote code. Replies to disclosures of minor problems will be sent in the seven calendar days following receipt.
6) Following analysis of the flaw, our teams will contact you as needed to establish a schedule during which the details of the flaw may be publicly released.

7) Any successful attack by you must be reported to us in seven calendar days at the address provided below.
8) Any attempt at extortion will result in legal action.
9) Any demonstration of security vulnerabilities must be solely to prove that a vulnerability exists.
   Here are some examples of acts that could result in legal action being taken (not an exhaustive list):
   a. Extracting a significant part of a database;
   b. Installing a persistence mechanism on systems;
   c. If an exploit succeeds, performing reconnaissance in our network;
   d. If an exploit succeeds, moving laterally through our network;
   e. If an exploit succeeds, using a password-extraction tool (Mimikatz, for example);
   f. Publishing personal or private information on the Internet;
   g. Large-scale data tampering;
   h. Denial-of-service attacks;
   i. Fraudulent use of any information obtained;
   j. Use of phishing, social engineering.

REWARD

You shall require no compensation for your involvement.

RESPONSIBLE DISCLOSURE PROCEDURES: HOW TO REPORT A VULNERABILITY

Disclosures should be emailed to the following address: **divulgation-securite@saq.qc.ca**. No automatic confirmation of receipt will be sent. To ensure we can reproduce and verify the potential vulnerability, we would appreciate receiving the following information:

1. The date, time, time zone and source address of the test;
2. The targeted system or systems (e.g. IP address, port number, URL);
3. The attack class: injection, known vulnerability (CVE-);
4. Description of the attack, payload and tools used and the steps to reproduce the attack;
5. Screen shots or logs and, if applicable, the type of data that are accessible.