CIRCULAIRE 075-22
Le 21 juin 2022

AUTOCERTIFICATION

MODIFICATION DES RÈGLES DE BOURSE DE MONTRÉAL INC. VISANT LA MISE EN PLACE

D'EXIGENCES EN MATIÈRE DE SIGNALEMENT D'INCIDENTS DE CYBERSÉCURITÉ

Le comité spécial et le comité des règles et politiques de Bourse de Montréal Inc. (la « **Bourse** ») ont approuvé des modifications aux règles de la Bourse visant la mise en place d'exigences en matière de signalement d'incidents de cybersécurité.

Ces modifications ont été autocertifiées conformément au processus d'autocertification prévu par la *Loi sur les instruments dérivés* (RLRQ, chapitre I-14.01).

La version amendée des articles que vous trouverez ci-jointe entrera en vigueur le **6 septembre 2022**. Veuillez noter que la nouvelle version des règles sera également disponible sur le site web de la Bourse (www.m-x.ca).

Les modifications visées par la présente circulaire ont fait l'objet d'une sollicitation de commentaires publiée par la Bourse le 6 mai 2022 (voir la circulaire 051-22). Suite à la publication de cette circulaire, aucun commentaire n'a été reçu par la Bourse.

Pour de plus amples renseignements, veuillez communiquer avec Dima Ghozaiel, Conseillère juridique par courriel au dima.ghozaiel@tmx.com.

Dima Ghozaiel
Conseillère juridique
Bourse de Montréal Inc.

ANNEXE 1 – MODIFICATION PROPOSÉE

VERSION MODIFIÉE

Article 3.113 Avis à la Division de la Réglementation en cas d'incident de cybersécurité

(a) Pour les fins du présent Article, un « incident de cybersécurité » comprend tout acte visant à obtenir un accès non autorisé au système informatique ou à l'information qui y est stockée d'un Participant Agréé, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage et qui donne lieu, ou qui est raisonnablement susceptible de donner lieu, à des répercussions importantes touchant:

(i) les activités normales du Participant Agréé relativement à son accès au Système de Négociation Électronique, ou

(ii) la capacité du Participant Agréé à se conformer à l'une ou l'autre de ses obligations prévues par la Réglementation de la Bourse.

(b) Le Participant Agréé doit signaler par avis écrit à la Division de la Réglementation, de la façon prescrite par cette dernière, tout incident de cybersécurité,

(i) dans les trois jours civils suivant la découverte d'un incident de cybersécurité, et y préciser, sauf accord contraire de la Division de la Réglementation, les renseignements suivants :

(1) une description de l'incident de cybersécurité;

(2) la date à laquelle, ou la période durant laquelle, l'incident de cybersécurité s'est produit et la date à laquelle le Participant Agréé l'a découvert;

(3) une évaluation provisoire de l'incident de cybersécurité, notamment les répercussions qu'il risque d'avoir sur les activités du Participant Agréé;

(4) la description des mesures d'intervention immédiate que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(5) le nom et les coordonnées d'une personne physique chargée de répondre, au nom du Participant Agréé, aux demandes de renseignements de la Division de la Réglementation au sujet de l'incident de cybersécurité.

(ii) dans les 30 jours civils, sauf accord contraire de la Division de la Réglementation, suivant la découverte de l'incident de cybersécurité et y préciser les renseignements suivants :

(1) la description de la cause de l'incident de cybersécurité;

(2) une évaluation de l'étendue de l'incident de cybersécurité, notamment les répercussions sur les activités du Participant Agréé;

(3) la description détaillée des mesures que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(4) les dispositions que le Participant Agréé a prises ou prendra pour améliorer son état de préparation à un incident de cybersécurité.

VERSION AU PROPRE

Article 3.113 Avis à la Division de la Réglementation en cas d'incident de cybersécurité

(a) Pour les fins du présent Article, un « incident de cybersécurité » comprend tout acte visant à obtenir un accès non autorisé au système informatique ou à l'information qui y est stockée d'un Participant Agréé, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage et qui donne lieu, ou qui est raisonnablement susceptible de donner lieu, à des répercussions importantes touchant:

(i) les activités normales du Participant Agréé relativement à son accès au Système de Négociation Électronique, ou

(ii) la capacité du Participant Agréé à se conformer à l'une ou l'autre de ses obligations prévues par la Réglementation de la Bourse.

(b) Le Participant Agréé doit signaler par avis écrit à la Division de la Réglementation, de la façon prescrite par cette dernière, tout incident de cybersécurité,

(i) dans les trois jours civils suivant la découverte d'un incident de cybersécurité, et y préciser, sauf accord contraire de la Division de la Réglementation, les renseignements suivants :

(1) une description de l'incident de cybersécurité;

(2) la date à laquelle, ou la période durant laquelle, l'incident de cybersécurité s'est produit et la date à laquelle le Participant Agréé l'a découvert;

(3) une évaluation provisoire de l'incident de cybersécurité, notamment les répercussions qu'il risque d'avoir sur les activités du Participant Agréé;

(4) la description des mesures d'intervention immédiate que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(5) le nom et les coordonnées d'une personne physique chargée de répondre, au nom du Participant Agréé, aux demandes de renseignements de la Division de la Réglementation au sujet de l'incident de cybersécurité.

(ii) dans les 30 jours civils, sauf accord contraire de la Division de la Réglementation, suivant la découverte de l'incident de cybersécurité et y préciser les renseignements suivants :

(1) la description de la cause de l'incident de cybersécurité;

(2) une évaluation de l'étendue de l'incident de cybersécurité, notamment les répercussions sur les activités du Participant Agréé;

(3) la description détaillée des mesures que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(4) les dispositions que le Participant Agréé a prises ou prendra pour améliorer son état de préparation à un incident de cybersécurité.