INFORMATION SECURITY MONITORING NOTICE - CANADA

Effective: 3rd April 2023

INTRODUCTION

The legal entity named on the contract of employment of the Employee, or the engagement of the Contractor (the "**Company**") has prepared this Information Security Monitoring Notice[1] (the "**Notice**") to supplement the Employee and Contractor Data Protection Notice (the "**DPN**") that you receive as an employee or contractor to set out its practices regarding the monitoring of data and other materials (including but not exclusively, business and personal[2] messages, communications and information) transmitted, received, processed and/or stored by the Company's electronic systems and devices. These include, but are not limited to, network, voice, computer, company issued mobile devices, instant messaging, web applications, mobile applications, social media, audio conferencing, video conferencing and fax infrastructure ("**Electronic Communications**"), printer use, the Internet, and physical access logs.

This Notice applies to all individuals or groups that have been provided with access to the Company's systems, facilities and/or information for a business purpose or supervisory function, including employees, consultants, contractors, non-executive directors and other workers in the Company (each an "**Authorized User**"). Appendix A sets out a non-exhaustive list of the communications and records which we monitor and from which we may collect any individually identifiable information on Authorized Users ("**Personal Data**") and the purposes for which we may use, transfer and disclose Personal Data.

In the event this Notice is provided to an Authorized User in a language other than English, any discrepancy, conflict or inconsistency between the two language versions shall be resolved as set out in the relevant DPN.

Irrespective of location, monitoring tools and processes are routinely deployed by the Company to the Company's electronic systems and devices to the extent not prohibited under local laws or regulations. All monitoring activity that takes place on the Company's electronic systems and devices is conducted in accordance with this Notice.

Any Personal Data collected in the course of the monitoring processes will be treated in accordance with the relevant DPN as issued from time to time. The processing of Personal Data is carried out with the aid of manual and electronic tools.

This Notice references key portions of relevant policies of the Company, but does not contain all of the Company's policies and requirements applicable to the use of Electronic Communications and the Internet. Authorized Users are required to comply with the requirements noted in the Company's Code of Conduct, Electronic Communications Guide and the Global Information Security Policy documents, as well as any other applicable standards issued by the Company from time to time. All capitalized terms used but not defined in this Notice shall have the meanings assigned to them in the Company's Global Information Security Policy documents.

Communications by certain regulated Company personnel are subject to additional detailed supervisory requirements and Authorized Users are reminded to consult the relevant policies and procedures for their

[1] The Information Security Monitoring Notice (ISMN), was previously titled The Cyber Security Monitoring Notice (CSMN) and may also be referred to as such in other company documentation

[2] In line with the Code of Conduct, authorized users are permitted limited personal use of company managed devices and applications, the internet and email for personal communications. The use of the resources may be monitored and inspected to maintain the integrity of the systems (e.g., monitoring for the introduction of malware or inappropriate data transmissions) and avoid activities that may give rise to company liability or risk.

line of business for further information.

All Electronic Communications, including emails (encrypted and unencrypted) and connections to the Internet and intranet websites using Company computing or network resources are the property of the Company and may be subject to monitoring and surveillance.

Subject to applicable law, this includes but is not limited to:

- **Conducting monitoring activities without giving prior notice ("covert monitoring"), in circumstances where it is permitted to do so (for example where it has suspicions of data exfiltration, criminal or other unlawful activities or breach of the Company's Compliance or Global Information Security Policies or breach of any other obligation owed to the Company);**
- **Monitoring and/or blocking of inbound and outbound emails and other messaging marked to indicate that they are personal or private or otherwise of a personal nature where it has a suspicion that such emails and their contents or attachments contravene or breach applicable law or Company's Compliance or Global Information Security Policies or any other obligation owed to the Company.**

PERSONAL DATA COLLECTION AND PURPOSES OF USE

Certain monitoring activities of the Company's electronic systems and devices are practiced throughout the Company for the purposes set out in Appendix A of this Notice.

The categories of Personal Data that the Company may process whilst undertaking the monitoring outlined in this Notice and the legal grounds for such processing (including consent, where necessary) are as set out in the relevant DPN.

SENSITIVE PERSONAL DATA

The Company may collect and process certain special categories of Personal Data including Sensitive Personal Data as set out in the relevant DPN in the course of conducting the activities described in this Notice.

Global Information Security monitoring activities do not actively monitor for Sensitive Personal Data, however some Sensitive Personal Data may inevitably be disclosed during monitoring for other types of data.

ACCESS BY COMPANY PERSONNEL

Access to Personal Data processed pursuant to this Notice is restricted to those individuals who need such access for the purposes listed in Appendix A. In addition to those individuals as set out in the relevant DPN, access will be granted on a strict need-to-know basis, to limited members of the Global Information Security Department and where necessary Internal Enterprise Investigations.

DISCLOSURE

The monitoring tools and processes described in this Notice may be deployed by the Global Information Security teams of the Company and any of its affiliates and branches including those located in the U.S., the U.K., Singapore, Hong Kong and India as well as within the specific country/region of operation. Personal Data may be stored in an Authorized Users home jurisdiction and/or other jurisdictions in which the Company has operations.

Given the global nature of the Company's activities, the Company may therefore transfer your Personal Data to countries located outside of your home country, as set out in the relevant DPN.

The Company may disclose, in accordance with applicable law, relevant Personal Data to any of its affiliates, and branches and they may process such Personal Data for the purposes set out in this Notice. In addition, the Company may disclose, in accordance with applicable law, relevant Personal Data to certain third parties as set out in relevant DPN.

SECURITY

The Company maintains appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage to Personal Data.

MODALITIES OF THE PROCESSING AND DATA RETENTION

In processing Personal Data for the purposes set out in this Notice, the Company does not use automated decision making on Authorized User processes where the decision would have a legal or similarly significant effect on the authorized user when conducting monitoring as described in this Notice. 'Automated decision making' is the process of making a decision by automated means without any human involvement.

The retention periods for each type of data and jurisdiction are outlined on the Global Records Retention Schedule found on the Global Records Management page on Flagscape. Retention requirements are available upon request for new Authorized Users who do not yet have access to the internal site. The Company will delete Personal Data after the applicable retention period.

DISCIPLINARY ACTION

Authorized Users who violate any of the policies referenced in this Notice may be subject to investigation, suspension of access and/or disciplinary proceedings (up to and including termination of employment or contract services). Authorized Users who are not employees may be subject to referral to their employer for disciplinary action. Authorized Users who violate applicable laws or regulations may be referred to law enforcement and/or regulatory officials in accordance with legal and regulatory requirements. Any material or evidence identified via (including but not limited to) the monitoring of telephone calls, emails and Internet or intranet use (including personal telephone calls, emails and Internet usage) may be relied upon in any disciplinary proceedings and internal or external investigations. Authorized Users are expected to cooperate in inquiries, inspections, monitoring and recording activities if asked. Refusing to cooperate with a security investigation may result in legal or disciplinary action, including termination of employment or contract services.

CONTACT DETAILS

For questions or more information about this Notice or Global Information Security monitoring activities, Authorized Users should contact Global Information Security.

You may have the right to lodge a complaint with the Data Protection Authority for your country, for applicability and further information refer to the relevant DPN.

For questions regarding local laws and restrictions, Authorized Users should contact their local compliance officer, Data Protection Officer or legal department.

CHANGES TO THIS NOTICE

This Notice is not contractual and the Company reserves the right to modify or withdraw the Notice at any time. Should the Company make substantial changes to this Notice, it will notify Authorized Users as soon as reasonably possible by reissuing a revised Notice and/or taking other steps in accordance with applicable

laws.

Related Documents

Code of Conduct

Electronic Communications Retention – Enterprise Policy

Global Information Security Policy documents

Harassment & Discrimination Prevention – Enterprise Policy

Reputational Risk – Enterprise Policy

Violence Free Workplace – Enterprise Policy

Information Security Monitoring Notice - Flagscape

For additional policies, standards and guidelines, please see the Global Policy Source Flagscape page.

APPENDIX A

Refer to the matrix linked here to view the categories of data that may be collected for each purpose of use, summarized below. The matrix is available upon request for new Authorized Users who do not yet have access to the internal site.

The Communications and Records (both live and after the event) which we monitor on the Company's electronic systems and devices and from which we may collect Personal Data include, but are not limited to:

- Emails sent;
- Emails received;
- Web / internet usage, FTP, HTTP, HTTPS, Telnet;
- Print usage;
- Files located on desktop (outside My Documents), collaboration sites, open shares, internal Wiki's;
- Removable media, Non-Company managed devices connecting to Company system;
- Instant messaging;
- Telephone calls, VOIP calls, voicemails;
- Application access and usage logs and records;
- System access and usage logs and records (including records showing course of usage and conduct);
- Fax & Document Scanning/Imaging;
- Social media usage and content (external, non-Company);
- Open source and publicly available information;
- Security logs;
- Key logs and screen shots;
- Conferencing technologies;
- Cookies, Beacons, Sinkholes and Honeypots;
- GPS, Wi-Fi Tracking and Location Data;
- Swipe Card entry data;
- Text Messages sent and received.

The Purposes For Which We May Collect, Use, Transfer And Disclose Personal Data:

The Global Information Security Policy is designed to provide the necessary requirements to enable the Company to prepare, prevent, detect, respond and recover from increasing changes in the threat landscape. The Global Information Security Program provides solutions and uses advanced techniques to prevent information security threats from undermining customer confidence and disrupting business operations. Global Information Security protects the Company and its clients by using a risk-based and outcome-focused framework.

- Prepare: We protect by continually updating the Information Security Programme, which includes complying with local or foreign state and/or country specific laws to better anticipate and identify potential threats;

- Prevent: We protect by staying ahead of adversaries through the deployment of preventative controls to prevent loss, misuse and inappropriate use of confidential and proprietary information and reduce the number of incidents;
- Detect: We protect by limiting exposure through the deployment of detective controls including firewall monitoring, anti-spam and virus protection, and other monitoring; continuously monitoring all bank teammates, applications, data, systems and networks;
- Mitigate: We protect by mitigating incidents through an agile and coordinated response capability;
- Respond/Recover: We protect by improving security posture through robust forensics, investigations, and lessons learned capability while addressing any compliance issues, regulatory inquiries, disciplinary actions, or legal claims

AVIS DE SURVEILLANCE DE LA SÉCURITÉ DE L'INFORMATION - Canada

Entrée en vigueur : 3rd April 2023

INTRODUCTION

L'entité juridique nommée sur le contrat de travail de l'Employé.e, ou l'engagement de l'Entrepreneur.e (la « **Société** ») a préparé le présent Avis de surveillance de la sécurité de l'[3]information (l'« **Avis** ») pour compléter l'Avis de protection des données des employés et des entrepreneurs (l'« **APD** ») que vous recevez en tant qu'employé.e ou entrepreneur.e pour établir ses pratiques concernant la surveillance des données et d'autres documents (y compris, mais sans s'y limiter, les messages professionnels et personnels[4], les communications et informations) transmis, reçus, traités et/ou stockés par les systèmes et appareils électroniques de la Société. Ceux-ci comprennent, sans s'y limiter, le réseau, la voix, l'ordinateur, les appareils mobiles fournis par l'entreprise, la messagerie instantanée, les applications Web, les applications mobiles, les médias sociaux, l'audioconférence, la vidéoconférence et l'infrastructure de télécopie (« **Communications électroniques** »), l'utilisation de l'imprimante, l'Internet et les journaux d'accès physique.

Le présent Avis s'applique à toutes les personnes ou à tous les groupes qui ont eu accès aux systèmes, aux installations ou aux renseignements de la Société à des fins commerciales ou de supervision, y compris les employés, les consultants, les entrepreneurs, les administrateurs non dirigeants et les autres travailleurs de la Société (chacun.e étant un.e « **Utilisateur ou utilisatrice autorisé.e** »). L'Annexe A dresse une liste non exhaustive des communications et des dossiers que nous surveillons et à partir desquels nous pouvons recueillir tout renseignement permettant d'identifier les Utilisateurs ou utilisatrices autorisé.e.s (« **Renseignements personnels** ») et les fins pour lesquelles nous pouvons utiliser, transférer et divulguer des Renseignements personnels.

Dans le cas où le présent Avis est fourni à un.e Utilisateur ou utilisatrice autorisé.e dans une langue autre que l'anglais, toute divergence, tout conflit ou touteincohérence entre les deux versions linguistiques seront résolus comme indiqué dans l'ADP pertinent.

Quel que soit l'emplacement, les outils et processus de surveillance sont régulièrement déployés par la Société sur les systèmes et appareils électroniques de la Société dans la mesure où cela n'est pas interdit par les lois ou règlements locaux. Toutes les activités de surveillance qui ont lieu sur les systèmes et appareils électroniques de la Société sont menées conformément au présent Avis.

Tous les Renseignements personnels recueillis dans le cadre des processus de surveillance seront traités conformément à l'ADP pertinent émis de temps à autre. Le traitement des Renseignements personnels s'effectue à l'aide d'outils manuels et électroniques.

Le présent Avis fait référence à des parties clés des politiques pertinentes de la Société, mais ne contient pas toutes les politiques et exigences de la Société applicables à l'utilisation des communications électroniques et d'Internet. Les Utilisateurs ou utilisatrices autorisé.e.s sont tenu.e.s de se conformer aux exigences indiquées dans le Code de conduite de la Société, le Guide des communications électroniques et les

---

[3] L'Avis de surveillance de la sécurité de l'information (ASSI) était auparavant intitulé l'Avis de surveillance de la cybersécurité (ASC) et peut également être désigné comme tel dans d'autres documents de l'entreprise

[4] Conformément au Code de conduite, les utilisateurs ou utilisatrices autorisé.e.s ont le droit d'utiliser à des fins personnelles des appareils et des applications gérés par l'entreprise, l'Internet et les courriels pour les communications personnelles. L'utilisation des ressources peut être surveillée et inspectée pour maintenir l'intégrité des systèmes (par ex., surveillance de l'introduction de logiciels malveillants ou de transmissions de données inappropriées) et éviter les activités qui peuvent entraîner la responsabilité ou le risque de l'entreprise.

documents de la Politique mondiale sur la sécurité de l'information, ainsi qu'à toute autre norme applicable émise par la Société de temps à autre. Tous les termes en majuscules utilisés, mais non définis dans le présent Avis, ont le sens qui leur est attribué dans les documents de la Politique mondiale sur la sécurité de l'information de la Société.

Les communications de certains membres du personnel réglementé de la Société sont assujetties à des exigences de supervision détaillées supplémentaires et nous rappelons aux Utilisateurs ou utilisatrices autorisé.e.s de consulter les politiques et procédures pertinentes pour leur secteur d'activité pour obtenir de plus amples renseignements.

Toutes les Communications électroniques, y compris les courriels (chiffrés et non chiffrés) et les connexions à Internet et aux sites Web intranet utilisant les ressources informatiques ou réseau de la Société, sont la propriété de la Société et peuvent faire l'objet d'une surveillance.

Sous réserve des lois applicables, cela comprend, sans s'y limiter :

- **Mener des activités de surveillance sans donner de préavis (« surveillance secrète »), dans des circonstances où il est autorisé à le faire (par exemple, lorsqu'il existe des soupçons d'exfiltration de données, d'activités délictueuses ou d'autres activités illégales, d'une violation des politiques mondiales de conformité ou de sécurité de l'information de la Société ou d'une violation de toute autre obligation due à la Société);**
- **La surveillance et/ou le blocage des courriels entrants et sortants et d'autres messages indiqués comme personnels ou privés ou autrement de nature personnelle lorsqu'il existe un soupçon que ces courriels et leur contenu ou leurs pièces jointes contreviennent ou viole la loi applicable ou aux politiques de conformité ou de sécurité mondiale de l'information de la Société ou à toute autre obligation due à la Société.**

COLLECTE DE RENSEIGNEMENTS PERSONNELS ET MOTIFS D'UTILISATION

Certaines activités de surveillance des systèmes et appareils électroniques de la Société sont pratiquées dans l'ensemble de la Société aux fins énoncées à l'Annexe A du présent Avis.

Les catégories de Renseignements personnels que la Société peut traiter tout en effectuant la surveillance décrite dans le présent Avis et les motifs juridiques de ce traitement (y compris le consentement, le cas échéant) sont tels qu'ils sont énoncés dans l'ADP pertinent.

RENSEIGNEMENTS PERSONNELS DE NATURE DÉLICATE

La Société peut recueillir et traiter certaines catégories spéciales de Renseignements personnels, y compris les Renseignements personnels sensibles, comme indiqué dans l'ADP pertinent dans le cadre de la conduite des activités décrites dans le présent Avis.

Les activités de surveillance mondiale de la sécurité de l'information ne surveillent pas activement les Renseignements personnels sensibles, mais certains Renseignements personnels sensibles peuvent inévitablement être divulgués pendant la surveillance d'autres types de données.

ACCÈS PAR LE PERSONNEL DE LA SOCIÉTÉ

L'accès aux Renseignements personnels traités en vertu du présent Avis est limité aux personnes qui en ont besoin aux fins énumérées à l'Annexe A. En plus des personnes indiquées dans l'ADP pertinent, l'accès sera accordé en cas de nécessité absolue aux membres limités du service mondial de sécurité de l'information et, au besoin, aux enquêtes internes de l'entreprise.

DIVULGATION

Les outils et processus de surveillance décrits dans le présent Avis peuvent être déployés par les équipes mondiales de sécurité de l'information de la Société et de l'une de ses sociétés affiliées et succursales, y compris celles situées aux États-Unis, au Royaume-Uni, à Singapour, à Hong Kong et en Inde, ainsi que dans le pays/région d'exploitation spécifique. Les Renseignements personnels peuvent être conservés dans la juridiction d'origine de l'Utilisateur ou utilisatrice autorisé.e et/ou dans les autres juridictions où la Société exerce ses activités.

Étant donné la nature mondiale des activités de la Société, la Société peut donc transférer vos Renseignements personnels dans des pays situés à l'extérieur de votre pays d'origine, comme indiqué dans l'ADP pertinent.

La Société peut divulguer, conformément à la loi applicable, des Renseignements personnels pertinents à l'une de ses sociétés affiliées et succursales, et elle peut traiter ces Renseignements personnels aux fins énoncées dans le présent Avis. De plus, la Société peut divulguer, conformément à la loi applicable, les Renseignements personnels pertinents à certains tiers, comme indiqué dansl'ADP pertinent.

SÉCURITÉ

La Société adopte des mesures de sécurité technique et organisationnelle adéquates pour protéger les Renseignements personnels contre des traitements non autorisés ou illégaux et/ou la perte accidentelle, l'altération, la divulgation ou l'accès, ou la destruction ou les dommages accidentels ou illégaux des Renseignements personnels.

MODALITÉS DE TRAITEMENT ET DE CONSERVATION DES DONNÉES

Dans le traitement des Renseignements personnels aux fins énoncées dans le présent Avis, la Société n'utilise pas la prise de décision automatisée sur les processus d'Utilisateur ou utilisatrice autorisé.e lorsque la décision aurait un effet juridique ou similairement significatif sur l'Utilisateur ou utilisatrice autorisé.e lors de la surveillance, comme décrit dans le présent Avis. La « prise de décision automatisée » est le processus qui consiste à prendre une décision par des moyens automatisés sans aucune intervention humaine.

Les périodes de conservation pour chaque type de données et de juridiction sont décrites dans le Calendrier mondial de conservation des documents qui se trouve sur la page de Gestion mondiale des documents sur Flagscape. Les exigences de conservation sont disponibles sur demande pour les nouveaux.elles Utilisateurs ou utilisatrices autorisé.e.s qui n'ont pas encore accès au site interne. La Société supprimera les Renseignements personnels après la période de conservation applicable.

MESURE DISCIPLINAIRE

Les Utilisateurs ou utilisatrices autorisé.e.s qui enfreignent l'une des politiques mentionnées dans le présent Avis peuvent faire l'objet d'une enquête, d'une suspension de l'accès et/ou de procédures disciplinaires (pouvant aller jusqu'à la cessation d'emploi ou des services contractuels). Les Utilisateurs ou utilisatrices autorisé.e.s qui ne sont pas des employé.e.s peuvent faire l'objet d'un renvoi devant leur employeur pour des mesures disciplinaires. Les Utilisateurs ou utilisatrices autorisé.e.s qui enfreignent les lois ou règlements applicables peuvent être renvoyés devant les autorités policières ou réglementaires conformément aux exigences légales et réglementaires. Tout contenu ou preuve identifiée par (y compris, mais sans s'y limiter) la surveillance des appels téléphoniques, des courriels et de l'utilisation d'Internet ou d'intranet (y compris les appels téléphoniques personnels, les courriels et l'utilisation d'Internet) peut être utilisé dans toute procédure disciplinaire et enquête interne ou externe. Les Utilisateurs ou utilisatrices autorisé.e.s sont tenus de coopérer aux demandes de renseignements, aux inspections, à la surveillance et à l'enregistrement des activités si elles sont formulées. Le refus de coopérer à une enquête de sécurité peut entraîner des mesures

juridiques ou disciplinaires, y compris la cessation d'emploi ou des services contractuels.

COORDONNÉES

Pour toute question ou pour obtenir de plus amples informations sur cet Avis, ou sur les activités de surveillance de la sécurité globale des informations, les Utilisateurs autorisés doivent contacter le Département de Sécurité Globale des Informations.

Vous pouvez avoir le droit de déposer une plainte auprès de l'autorité de protection des données de votre pays, pour l'applicabilité et de plus amples renseignements, consultez l'ADP pertinent.

Pour toute question concernant les lois et restrictions locales, les Utilisateurs ou utilisatrices autorisé.e.s doivent communiquer avec leur agent de conformité local, leur agent de protection des données ou leur service juridique.

MODIFICATIONS APPORTÉES AU PRÉSENT AVIS

Le présent Avis n'est pas contractuel et la Société se réserve le droit de modifier ou de retirer l'Avis à tout moment. Si la Société apporte des modifications importantes au présent Avis, elle avisera les Utilisateurs ou utilisatrices autorisé.e.s dès que raisonnablement possible en publiant de nouveau un Avis révisé et/ou en prenant d'autres mesures conformément aux lois applicables.

Documents connexes

Code de conduite

Conservation des communications électroniques – Politique d'entreprise

Documents de la Politique mondiale sur la sécurité de l'information

Prévention du harcèlement, de la discrimination et des représailles – Politique d'entreprise

Risque pour la réputation – Politique d'entreprise

Lieu de travail sans violence - Politique d'entreprise

Avis de surveillance de la sécurité de l'information - Flagscape

Pour obtenir des politiques, des normes et des lignes directrices supplémentaires, veuillez consulter la page Flagscape de la Source de la politique mondiale.

ANNEXE A

Reportez-vous à la matrice dont le lien se trouve ici pour voir les catégories de renseignements qui peuvent être recueillies à chaque fin d'utilisation, résumées ci-dessous. La matrice est disponible sur demande pour les nouveaux.elles Utilisateurs ou utilisatrices autorisé.e.s qui n'ont pas encore accès au site interne.

Les communications et les dossiers (en direct et après l'événement) que nous surveillons sur les systèmes et appareils électroniques de la Société et à partir desquels nous pouvons recueillir des Renseignements personnels comprennent, sans s'y limiter :

- Les courriels envoyés;
- Les courriels reçus;
- L'utilisation Web/Internet, FTP, HTTP, HTTPS, Telnet;
- L'utilisation de l'impression;
- Les fichiers situés sur le bureau (à l'extérieur de Mes documents), les sites de collaboration, les partages ouverts, les wikis internes;
- Les supports amovibles, les dispositifs non gérés par la Société se connectant au système de la Société;
- La messagerie instantanée;
- Les appels téléphoniques, appels VoIP, messages vocaux;
- Les journaux et registres d'accès et d'utilisation des applications;
- Les journaux et les registres d'accès et d'utilisation du système (y compris les dossiers indiquant le déroulement de l'utilisation et de la conduite);
- La numérisation/imagerie de télécopies et de documents;
- L'utilisation et le contenu des médias sociaux (externes, non liés à la Société);
- Les renseignements libres et accessibles au public;
- Les journaux de sécurité;
- Les registres clés et saisies d'écran;
- Les technologies de conférence;
- Les témoins, balises, entonnoirs et pots de miel;
- Le GPS, le suivi Wi-Fi et les données de localisation;
- Les données d'entrée des badges;
- Les messages texte envoyés et reçus.

Fins auxquelles nous pouvons recueillir, utiliser, transférer et divulguer des Renseignements personnels :

La Politique mondiale sur la sécurité de l'information est conçue pour fournir les exigences nécessaires pour permettre à la Société de préparer, de prévenir, de détecter, de réagir et se rétablir des changements croissants dans le paysage des menaces. Le Programme mondial de sécurité de l'information fournit des solutions et utilise des techniques avancées pour empêcher les menaces à la sécurité de l'information de nuire à la confiance des clients et de perturber les opérations commerciales. La Sécurité mondiale de l'information protège la Société et ses clients en utilisant un cadre axé sur les risques et les résultats.

- Préparer : Nous protégeons en mettant continuellement à jour le Programme de sécurité de

l'information, ce qui comprend le respect des lois locales ou étrangères propres à un État ou à un pays afin de mieux anticiper et identifier les menaces potentielles;

- Prévenir : Nous protégeons en restant à l'avant-garde des adversaires grâce au déploiement de contrôles préventifs pour prévenir la perte, l'utilisation abusive et l'utilisation inappropriée de renseignements confidentiels et exclusifs et réduire le nombre d'incidents;
- Détecter : Nous protégeons en limitant l'exposition par le déploiement de contrôles de détection, y compris la surveillance de pare-feu, la protection antipourriel et antivirus, et d'autres mesures de surveillance; nous surveillons continuellement tous les coéquipiers, applications, données, systèmes et réseaux de la banque;
- Atténuer : Nous protégeons en atténuant les incidents grâce à une capacité d'intervention agile et coordonnée;
- Répondre/Rétablir : Nous protégeons en améliorant la posture de sécurité grâce à de solides capacités judiciaires, d'enquêtes et de leçons apprises tout en traitant tout problème de conformité, toute demande réglementaire, toute mesure disciplinaire ou toute réclamation juridique.