NORTON ROSE FULBRIGHT

Norme de sécurité de l'information à l'intention des fournisseurs

Juillet 2025

Politique et gestion de la sécurité de l'information

1.1 Le fournisseur doit établir et maintenir un programme de sécurité de l'information qui comprend des politiques et des procédures en matière de sécurité de l'information qui conviennent à l'ampleur des activités et à la sensibilité de l'information traitée pour le compte de Norton Rose Fulbright.

1.2 Le programme de sécurité de l'information du fournisseur doit comprendre des mesures organisationnelles et techniques adéquates conformes aux pratiques exemplaires du secteur afin de protéger l'information contre une destruction accidentelle ou illégale, la perte, une modification, une divulgation ou un accès non autorisé, et fournir un niveau de sécurité qui convient au risque représenté par le traitement et la nature de l'information à protéger.

1.3 Les politiques de sécurité de l'information du fournisseur doivent être révisées, mises à jour et approuvées périodiquement par la direction du fournisseur. Le fournisseur doit communiquer par écrit les exigences en matière de sécurité de l'information à tous les membres de son personnel qui prennent part aux services fournis à Norton Rose Fulbright.

Points de contact

2.1 Si le fournisseur doit communiquer avec Norton Rose Fulbright à propos de la sécurité de l'information, comme il est indiqué dans la présente norme, les coordonnées du centre de service TI mondial de Norton Rose Fulbright sont les suivantes : téléphone : +44 (0) 207 444 5555; courriel : 5555@nortonrosefulbright.com.

2.2 Le fournisseur doit désigner une personne qui agira comme point de contact unique et permanent de Norton Rose Fulbright afin de traiter des questions touchant l'utilisation et la sécurité de l'information confidentielle de Norton Rose Fulbright.

Relations avec des tiers

3.1 Le fournisseur doit aviser Norton Rose Fulbright avant de transférer, de sous-traiter ou d'impartir à un tiers la totalité ou une partie de ses obligations de fournir les services, et cet avis doit comprendre le nom et l'adresse du tiers fournisseur.

3.2 Le fournisseur doit exiger de tous ses tiers fournisseurs qui hébergent, consultent ou traitent l'information confidentielle de Norton Rose Fulbright qu'ils mettent en œuvre des mesures de sécurité conformes à la présente norme. Le fournisseur doit établir des processus pour vérifier si tous les tiers fournisseurs qui ont accès à l'information confidentielle de Norton Rose Fulbright sont gérés de façon à limiter les risques pour Norton Rose Fulbright. Les tiers fournisseurs doivent faire l'objet d'une vérification périodique par le fournisseur et d'une évaluation des risques de sécurité de l'information.

3.3 Sous réserve de toute autre obligation que le fournisseur peut avoir ou de toute autre demande que Norton Rose Fulbright peut faire, le fournisseur est pleinement responsable de la totalité des travaux, des services, des contenus, des dessins, des documents et des actes écrits, des manquements, des omissions, des défauts et/ou de la négligence ou de la défaillance de l'un ou l'autre de ses tiers fournisseurs, comme s'il s'agissait de l'acte, du manquement, de l'omission, du défaut, de la négligence ou de la défaillance du fournisseur.

3.4 Si le fournisseur propose d'utiliser un environnement en nuage pour traiter ou stocker l'information confidentielle de Norton Rose Fulbright, le fournisseur doit utiliser uniquement un environnement en nuage privé ou dédié qui chiffre l'information au repos et la stocke conformément aux modalités de la présente entente, y compris sans limitation le paragraphe 5.2 de la présente norme.

Conservation, retour et destruction de l'information

4.1 Le fournisseur ne doit conserver l'information confidentielle de Norton Rose Fulbright que pendant la durée précisée par Norton Rose Fulbright ou selon ce qui est nécessaire pour fournir les services, sauf si les lois ou règlements applicables exigent une période de conservation plus longue.

4.2 Sur demande de Norton Rose Fulbright, le fournisseur doit :

i. Détruire l'information confidentielle de Norton Rose Fulbright placée sous son contrôle;

ii. Fournir une confirmation selon laquelle l'information confidentielle de Norton Rose Fulbright a été détruite de manière irréversible.

Échange, transfert et stockage de l'information

5.1 Le fournisseur doit protéger toute l'information confidentielle de Norton Rose Fulbright en transit et stockée, y compris :

i. Encoder toute l'information confidentielle de Norton Rose Fulbright qui demeure dans les systèmes, les serveurs, les supports d'enregistrement et les supports de sauvegarde placés sous le contrôle du fournisseur, y compris l'information confidentielle de Norton Rose Fulbright qui demeure dans les systèmes et les serveurs d'un tiers à qui le fournisseur a confié le traitement ou le stockage des données électroniques en sous-traitance;

ii. Utiliser l'encodage au moment de transférer l'information confidentielle de Norton Rose Fulbright et dans les communications entre le fournisseur et Norton Rose Fulbright ou entre le fournisseur et un tiers à qui le fournisseur a confié le traitement ou le stockage des données électroniques en sous-traitance. Les systèmes du fournisseur utilisés pour les services de messagerie électronique ou les services Web doivent être configurés pour encoder automatiquement les communications entre le fournisseur et Norton Rose Fulbright à l'aide du protocole Transport Layer Security (TLS);

iii. Si l'information confidentielle de Norton Rose Fulbright venait à être transférée sur un support amovible ou un appareil électronique mobile, comme un téléphone intelligent, une tablette ou un ordinateur portable, appliquer, surveiller et maintenir l'encodage et les outils de prévention des fuites de l'information.

5.2 Le fournisseur :

i. Doit maintenir une séparation physique ou logique entre l'information confidentielle de Norton Rose Fulbright et l'information appartenant à d'autres parties, comme d'autres clients du fournisseur, afin d'éviter que des tiers malveillants ou corrompus affectent le service;

ii. Ne doit héberger, stocker, consulter ou traiter l'information confidentielle qu'aux endroits convenus ou à partir de ceux-ci;

iii. Ne doit pas, sans le consentement écrit préalable de Norton Rose Fulbright, changer l'endroit où l'information confidentielle de Norton Rose Fulbright est hébergée, stockée, consultée ou traitée ou autrement divulguer ou transférer l'information confidentielle de Norton Rose Fulbright à une personne ou une entité qui se trouve à l'extérieur d'un endroit convenu.

Gestion du contrôle d'accès logique

6.1 Le fournisseur doit être doté de contrôles d'accès logique conçus pour gérer l'accès à l'information et aux fonctions du système selon le principe du moindre privilège et de la nécessité justifiée, y compris :

i. Déterminer et documenter les comptes et les types d'utilisateurs administratifs et d'utilisatrices administratives ainsi que leur niveau d'accès; révoquer les comptes lorsqu'ils ne sont plus nécessaires; et, de plus, changer rapidement les mots de passe s'ils sont susceptibles d'avoir été portés à la connaissance d'une autre personne ou d'être autrement compromis;

ii. Authentifier l'accès à l'information, maintenir les comptes d'utilisateur ou d'utilisatrice et les comptes privilégiés en conformité avec les normes sectorielles et commerciales raisonnables et passer en revue régulièrement les privilèges d'accès à l'information et révoquer les accès lorsqu'ils ne sont plus nécessaires;

iii. Sécuriser les accès privilégiés à l'aide de méthodes d'authentification robustes;

iv. Protéger l'ensemble des mots de passe, des phrases de chiffrement et des NIP des utilisateurs et utilisatrices en mémoire à l'aide de solutions d'encodage unidirectionnel et sécuriser les accès privilégiés à l'aide de méthodes d'authentification robustes;

v. Rexiger une authentification à deux facteurs pour l'accès à distance aux actifs informationnels contrôlés par le fournisseur.

Sécurité des ressources humaines

7.1 Contrôle de sécurité du personnel

Une vérification des antécédents doit être effectuée pour l'ensemble des membres du personnel du fournisseur qui ont accès à l'information confidentielle de Norton Rose Fulbright. Cette vérification doit comprendre au moins une vérification de l'identité, une vérification des diplômes ou autres compétences déclarées, une vérification de dossier criminel, des vérifications financières et une vérification des attestations et permis pertinents, lorsque la loi le permet.

7.2 Formation du personnel

Le fournisseur doit s'assurer que l'ensemble des membres du personnel du fournisseur qui ont accès à l'information confidentielle de Norton Rose Fulbright suivent une séance de sensibilisation à la sécurité de l'information et obtiennent des mises à jour fréquentes sur les politiques et procédures du fournisseur, selon ce qui est pertinent pour leurs fonctions.

Sécurité physique et environnementale

8.1 Le fournisseur doit veiller à ce que des mesures de protection appropriées soient en place afin d'assurer ce qui suit :

i. Protéger physiquement les installations où l'information confidentielle de Norton Rose Fulbright est consultée, stockée, traitée ou détruite à l'aide de systèmes de sécurité conformes aux normes sectorielles et des contrôles d'entrée, comme des cartes d'accès, des murs et des bureaux d'accueil avec personnel; protéger le matériel utilisé par le fournisseur pour le stockage, le traitement ou la destruction de l'information confidentielle de Norton Rose Fulbright contre les pannes de courant et autres défaillances causées par un bris des services connexes;

ii. Enregistrer l'accès aux installations et maintenir ces registres de manière sécuritaire; valider l'identité, escorter et superviser les personnes en visite ou invitées en tout temps lorsqu'elles sont dans les locaux.

Administration des systèmes et sécurité du réseau

Le fournisseur doit avoir des procédures et des contrôles opérationnels qui visent à s'assurer que la technologie et les systèmes d'information sont configurés et maintenus selon les politiques et normes internes prescrites et conformément aux pratiques exemplaires applicables. Plus précisément, le fournisseur doit mettre en œuvre et maintenir les contrôles de sécurité énumérés dans cet article, au besoin :

9.1 Protection contre les maliciels et les accès malveillants

i. Installer des mécanismes de protection contre les maliciels sur les systèmes contrôlés par le fournisseur et les configurer pour qu'ils recherchent et téléchargent automatiquement les mises à jour (au moins quotidiennement) et effectuent une recherche de virus continue. La détection des maliciels et des menaces doit être mise à jour de façon continue et les correctifs logiciels fournis par les fournisseurs de logiciels doivent être téléchargés et déployés en temps opportun.

ii. Mettre en place des contrôles pour filtrer et bloquer du contenu malveillant ou inapproprié et déployer des capacités avancées de gestion des menaces continues pour protéger les systèmes de stockage ou de traitement de l'information.

9.2 Sécurité du réseau

i. Configurer les appareils du réseau, y compris les routeurs et les commutateurs, selon les normes de verrouillage approuvées. Régir et superviser les changements aux contrôles de sécurité du réseau à l'aide de normes de gestion des changements.

ii. Déployer et maintenir des pare-feu, des zones de réseau segmentées, des systèmes de détection des intrusions et des systèmes de prévention des intrusions conçus pour protéger les systèmes contre les intrusions ou limiter la portée ou la réussite d'attaques ou de tentatives d'accès non autorisé à l'information.

iii. Établir des restrictions à l'égard des ports, des protocoles et des adresses IP qui limitent au minimum prescrit les flux entrants et sortants du réseau. Tous les flux entrants doivent être acheminés vers des destinations précises et autorisées.

iv. Effectuer des analyses régulières des applications, des systèmes d'exploitation et des infrastructures technologiques liées aux services pour analyser la vulnérabilité de la sécurité et résoudre les problèmes en temps opportun.

9.3 Maintenance des systèmes

i. Adopter et suivre des procédures de correction pour les applications, les systèmes d'exploitation et les infrastructures technologiques afin de réduire les vulnérabilités et de se protéger contre les menaces nouvelles et actuelles à la sécurité en temps opportun.

ii. Adopter et suivre des procédures pour maintenir des versions des applications, des systèmes d'exploitation et des infrastructures technologiques qui sont soutenues par leurs fabricants respectifs et pour convenablement mettre hors service les applications, systèmes d'exploitation et infrastructures technologiques avant qu'ils n'atteignent la date de fin de vie utile fixée par le fabricant.

9.4 Sécurité des postes de travail du fournisseur et des appareils des utilisateurs et utilisatrices

i. Déployer et maintenir des mesures de contrôle sur les postes de travail et les appareils des utilisateurs et utilisatrices sous le contrôle du fournisseur, y compris les appareils de communication mobiles et les appareils de stockage portatifs, afin de prévenir l'accès non autorisé, la fuite, la modification ou la destruction non autorisée de l'information.

9.5 Sauvegardes

i. Créer, encoder, maintenir et stocker de façon sécuritaire des sauvegardes quotidiennes de l'information confidentielle de Norton Rose Fulbright stockée dans les systèmes contrôlés par le fournisseur et toute application ou information de configuration nécessaire pour fournir les services, et tester régulièrement les copies de sauvegarde de l'information confidentielle de Norton Rose Fulbright.

ii. Mettre en œuvre une procédure de traitement des copies de sauvegarde afin de prévenir le vol ou la perte de l'information confidentielle de Norton Rose Fulbright, prendre des mesures adéquates pour protéger les copies de sauvegarde alors qu'elles sont en transit et garder des copies de sauvegarde de l'information confidentielle de Norton Rose Fulbright dans un endroit sûr et contrôlé, conformément aux directives de Norton Rose Fulbright, le cas échéant.

9.6 Résilience des services

i. Mettre en œuvre des plans de reprise et de poursuite des activités décrivant les procédures à appliquer pour s'assurer que les services se poursuivent si un événement venait à diminuer ou à interrompre la capacité du fournisseur de rendre les services ou de maintenir les niveaux de services convenus.

ii. En cas de catastrophe ou d'urgence, s'assurer que des mesures de reprise suffisantes à l'interne ainsi qu'à l'externe sont en place pour appuyer les plans de poursuite et de reprise des activités.

iii. Tester régulièrement (au moins une fois par année) son plan de poursuite et de reprise des activités qui assurera la poursuite des services, et mettre en œuvre les mesures correctives jugées nécessaires après le test.

iv. Protéger les services qui hébergent ou traitent l'information confidentielle de Norton Rose Fulbright contre les attaques par déni de services en mettant en œuvre des solutions visant à réduire ce type de situation.

Enregistrement et surveillance

10.1 Le fournisseur doit :

i. Mettre en place des mesures pour l'enregistrement des activités en lien avec les services et les infrastructures, y compris les activités liées à l'accès ou à une tentative d'accès, pour appuyer les enquêtes sur des incidents de sécurité soupçonnés ou des activités malveillantes;

ii. Assigner des identifiants uniques à l'ensemble des utilisateurs et utilisatrices des applications pour chaque application;

iii. Tenir des registres pour les applications aux fins de l'enregistrement et de l'horodatage, pour l'ensemble des utilisateurs et utilisatrices des applications, les tentatives de connexion réussies et non réussies et les actes exécutés par chaque utilisateur ou utilisatrice;

iv. Protéger les registres contre un accès ou des modifications non autorisés, et conserver ces registres pendant au moins six mois. Les registres ne doivent pas être supprimés ou écrasés pendant cette période, sauf si les données ont d'abord été transférées dans un registre central (p. ex. SIEM) afin d'y être conservées;

v. À la demande de Norton Rose Fulbright, rendre accessible à Norton Rose Fulbright tout registre qui pourrait l'aider à contrôler l'accès à l'information confidentielle de Norton Rose Fulbright.

Sécurité en matière de développement d'applications et de sites Web

11.1 Dans la mesure applicable, le fournisseur doit :

i. Établir des règles pour le développement de logiciels et de systèmes et les appliquer au développement au sein de son entreprise. La sécurité de l'information doit être conçue et intégrée dans le cycle de vie du développement de systèmes d'information;

ii. Suivre les pratiques sectorielles reconnues en matière de développement sûr dans toutes les activités de développement de codes logiciels, y compris les procédures de mise en œuvre pour protéger les codes sources des programmes et les données des essais et pour valider l'entrée, le traitement interne et la sortie des données dans les applications;

iii. Effectuer des évaluations de sécurité des applications accessibles par Internet avant le déploiement et de façon continue par la suite;

iv. Développer des applications accessibles par Internet fondées sur des lignes directrices sécuritaires en matière de codage, comme celles que l'on trouve dans le guide intitulé *Open Web Application Security Project (OWASP) Development Guide.*

11.2 L'information confidentielle de Norton Rose Fulbright ne doit pas être utilisée dans des environnements de développement ou d'essai du fournisseur sans le consentement préalable de Norton Rose Fulbright. Si l'information confidentielle de Norton Rose Fulbright doit être utilisée à des fins d'essai, le fournisseur doit s'assurer d'avoir en place des processus pour effectuer les contrôles suivants :

i. Établir un mécanisme de suppression de contenu sensible (masquage de données) et rendre les données anonymes;

ii. Supprimer de façon sûre les données des environnements de développement ou d'essai à la fin des essais.

11.3 Sauf indication contraire dans l'entente et dans la mesure permise, le fournisseur ne doit pas, sans le consentement préalable écrit de Norton Rose Fulbright, faire ce qui suit :

i. Utiliser l'information confidentielle de Norton Rose Fulbright pour entraîner ou calibrer tout service d'IA générative ou modèle associé, y compris des technologies d'apprentissage automatique, y faire des requêtes et y téléverser ou y verser d'une quelconque autre manière des renseignements; ni

ii. Utiliser toute exigence relative aux données ou à l'information à des fins autres que la prestation des services, y compris ne pas fusionner ces données ou cette information avec le bassin de données générales d'un fournisseur.

Gestion et notification des failles de sécurité

12.1 Le fournisseur doit mettre en œuvre et maintenir une procédure de gestion des incidents liés à la sécurité de l'information (couvrant la perte de disponibilité, d'intégrité ou de confidentialité de l'information). Cette procédure doit comprendre le signalement, le diagnostic, le traitement selon le niveau de gravité, la prise en charge à un échelon supérieur et la procédure de communication, la documentation et le suivi ainsi que les comptes-rendus de l'incident. Le fournisseur passera en revue périodiquement sa procédure de gestion des incidents liés à la sécurité de l'information.

12.2 Lorsqu'il découvre un incident lié à la sécurité qui affecte la confidentialité, l'intégrité ou la disponibilité de l'information confidentielle de Norton Rose Fulbright, le fournisseur doit :

i. Dans les meilleurs délais et dans les quarante-huit (48) heures suivant la détection de l'incident lié à la sécurité, le signaler à Norton Rose Fulbright à l'aide des coordonnées de la personne-ressource indiquées dans la présente norme; le délai est réduit à vingt-quatre (24) heures s'il est établi que la confidentialité, l'intégrité ou la disponibilité de l'information confidentielle de Norton Rose Fulbright n'a pas été compromise de façon importante;

ii. Collaborer entièrement avec Norton Rose Fulbright en fournissant toute l'information pertinente concernant l'incident lié à la sécurité en temps opportun;

iii. Collaborer entièrement avec Norton Rose Fulbright en déterminant la cause à la source de l'incident lié à la sécurité, en y remédiant et en faisant les notifications requises par la loi applicable.

Conformité et droits d'examen de la sécurité

13.1 **Conformité réglementaire :** Le fournisseur doit se conformer à toutes les exigences qui lui ont été communiquées par Norton Rose Fulbright et qui sont imposées à Norton Rose Fulbright par des entités gouvernementales ou des organismes de réglementation. Norton Rose Fulbright s'attend à ce que le fournisseur lui fournisse les documents nécessaires pour étayer les audits de Norton Rose Fulbright, à sa demande.

13.2 **Audits de tiers indépendants :** Le fournisseur doit avoir recours périodiquement à une tierce société de sécurité indépendante pour auditer et tester ses contrôles de sécurité de l'information. Le fournisseur doit mettre en œuvre un processus pour supprimer tout risque ou résoudre tout problème détecté pendant ces audits.

Sur demande, le fournisseur fournira des preuves de ces résultats d'audit et des mesures prises pour corriger tout défaut détecté.

13.3 **Droit d'effectuer un audit :** Le fournisseur doit tenir des registres complets, précis et à jour pertinents concernant l'exécution de ses obligations aux termes de l'entente et les conserver pendant six ans à compter de la résiliation ou de l'expiration de l'entente. Sans limiter les dispositions des paragraphes précédents de la présente norme,

en tant qu'entité réglementée, Norton Rose Fulbright peut exiger des droits d'accès pour Norton Rose Fulbright et ses auditeurs (p. ex. les ordres professionnels ou les organismes d'application de la loi auxquels Norton Rose Fulbright est assujetti) afin d'exécuter les audits en rapport avec l'entente. Le fournisseur déploiera des efforts raisonnables pour assurer l'accès aux locaux, au personnel, au matériel et à d'autres supports, selon ce qui peut être raisonnablement requis aux fins de ces tâches. Ces dispositions en matière de registre et de droit d'audit subsisteront à la résiliation de la présente entente.

Définitions applicables à la présente norme

Endroits convenus désigne le territoire où Norton Rose Fulbright est établi (et s'il s'agit de l'Angleterre, les endroits convenus se trouvent au Royaume-Uni et dans l'Espace économique européen) et/ou tout autre territoire convenu par Norton Rose Fulbright, conformément aux modalités de la présente entente, ou, s'ils ne sont pas précisés dans l'entente, les endroits convenus par écrit par Norton Rose Fulbright.

Entente désigne l'entente entre Norton Rose Fulbright et le fournisseur à laquelle la présente norme est annexée ou, s'il n'y a pas d'entente, la présente norme.

Entités Norton Rose Fulbright désigne le Verein de Norton Rose Fulbright, les cabinets membres, à l'occasion, du Verein de Norton Rose Fulbright (qui, à la date de la présente entente, comprennent Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada S.E.N.C.R.L., s.r.l., Norton Rose Fulbright South Africa Inc., Norton Rose Fulbright US LLP) et Norton Rose Fulbright Development Holdings Limited, Norton Rose Fulbright Australia Services Pty Ltd, Jaramer Pty Ltd, TNB & Partners, Services OR LP/SEC, une société en commandite établie au Canada, Ascendant Legal LLC, Shanghai Pacific Legal et, dans tous les cas les membres de leur groupe respectif, les personnes ayant un lien avec chacune d'entre elles ou leurs filiales respectives de temps à autre, et tout renvoi au terme entité Norton Rose Fulbright désignera l'une ou l'autre de celles-ci, selon le cas.

Fournisseur désigne la personne qui fournit les services à Norton Rose Fulbright.

Information confidentielle de Norton Rose Fulbright désigne la totalité des données ou de l'information quel qu'en soit le format (y compris sous forme écrite, orale, visuelle ou électronique) obtenue par le fournisseur directement ou indirectement de Norton Rose Fulbright ou de toute autre entité Norton Rose Fulbright à tout moment, portant sur les entités Norton Rose Fulbright ou les clients, membres, associé·es, membres du personnel, entreprises, finances, actifs, activités, savoir-faire, stratégie ou affaires de l'une ou l'autre des entités Norton Rose Fulbright, selon le cas, et toute donnée ou information requise aux termes de la présente entente ou conformément à celle-ci et qui, par suite des négociations relatives à la présente entente ou de l'exercice de ses droits ou de l'exécution de ses obligations aux termes des présentes, est acquise par le fournisseur ou pour son compte aux bureaux ou autres locaux, ou par l'intermédiaire de l'accès à un système de TI, de l'une ou l'autre des entités Norton Rose Fulbright ou qu'elle provienne d'observations faites par le fournisseur ou pour son compte, y compris toute information acquise par inadvertance par le fournisseur alors qu'il se trouvait dans les locaux de Norton Rose Fulbright, que ce soit avant ou après la date de la présente entente.

Norton Rose Fulbright désigne l'entité Norton Rose Fulbright qui obtient les services.

Services a le sens qui lui est attribué dans l'entente ou, s'il n'y a pas d'entente, les biens, les travaux, les services, les fonctions que le fournisseur a convenu de fournir à Norton Rose Fulbright et les responsabilités qu'il a convenu d'assumer à l'égard de Norton Rose Fulbright, y compris les biens, travaux, services, fonctions et responsabilités accessoires raisonnablement et nécessairement requis pour l'exécution des services.