RioTinto

# EXIGENCES DE CYBERSÉCURITÉ DE RIO TINTO POUR LES FOURNISSEURS

Les fournisseurs doivent s'assurer que leurs technologies de l'information et autres systèmes d'affaires répondent aux exigences suivantes lorsqu'ils offrent leurs prestations au Groupe Rio Tinto ou qu'ils interagissent avec les systèmes des technologies de l'information (TI) ou des technologies industrielles et opérationnelles (I&OT) du Groupe.

## 1. GÉNÉRALITÉS

Le fournisseur doit s'assurer que tous les systèmes technologiques utilisés ou les services rendus par le fournisseur, ou encore la modification importante de systèmes ou de services existants, n'exposent pas Rio Tinto à un risque important en matière de cybersécurité. Rio Tinto détermine à son entière discrétion ce qui constitue un risque important.

## 2. ÉVALUATION DES RISQUES POUR LA CYBERSÉCURITÉ

Le fournisseur doit réaliser une évaluation des risques pour la cybersécurité, la consigner et la fournir, sur demande, à Rio Tinto. Cette évaluation doit :

(a) évaluer les systèmes du fournisseur et tous les systèmes de tiers utilisés pour la prestation;
(b) définir les principales mesures techniques et de conformité nécessaires pour garantir le maintien de la confidentialité, de l'intégrité et de la disponibilité des informations;
(c) veiller à ce que les mesures de contrôle appliquées soient proportionnelles au risque défini.

Cette exigence peut ne pas s'appliquer si le fournisseur présente des attestations de gouvernance en matière de cybersécurité à jour et pertinentes, comme la certification ISO/IEC 27001 ou un rapport SSAE18/ISAE3402 SOC 2 Type II, délivrées par un tiers indépendant et dûment qualifié couvrant les systèmes pertinents utilisés pour la prestation. Rio Tinto se réserve le droit de demander des preuves supplémentaires ou des attestations d'un tiers, à sa discrétion.

## 3. CONTRÔLE D'ACCÈS

### 3.1 ACCÈS AUX SYSTÈMES DE RIO TINTO

Dans la mesure où le fournisseur a besoin d'accéder aux systèmes technologiques de Rio Tinto dans le cadre de la prestation, il doit s'assurer de ce qui suit :

(a) L'accès est fourni par Rio Tinto au moyen du fournisseur d'identité de Rio Tinto.
(b) L'accès est strictement limité au personnel du fournisseur qui en a besoin pour accomplir des tâches liées aux prestations.
(c) L'accès n'est accordé que durant la période nécessaire à la prestation des services. Le fournisseur doit rapidement aviser Rio Tinto lorsque l'accès n'est plus nécessaire afin qu'il puisse être révoqué, même si la période d'accès initiale n'est pas encore expirée.
(d) Chaque identité d'utilisateur nécessitant l'accès aux systèmes de Rio Tinto est liée à une personne identifiable de manière unique.
(e) Tous les utilisateurs, appareils et autres identités sont authentifiés sur le réseau de Rio Tinto à l'aide d'une authentification multifactorielle (MFA).

### 3.2 ACCÈS À DISTANCE AUX ACTIFS DU FOURNISSEUR SITUÉS SUR LE RÉSEAU DE RIO TINTO

Dans la mesure où le fournisseur a besoin d'accéder à ses propres systèmes technologiques fournis dans le cadre de la prestation et que ces systèmes situés dans l'environnement réseau de Rio Tinto, le fournisseur doit s'assurer que :

(a) les solutions d'accès à distance utilisées pour accéder aux réseaux de Rio Tinto sont préapprouvées et gérées par Rio Tinto;
(b) l'accès n'est accordé qu'aux parties autorisées pour des raisons professionnelles valables;
(c) l'accès est contrôlé continuellement, réexaminé périodiquement et révoqué rapidement lorsqu'il n'est plus nécessaire;
(d) les contrôles techniques minimaux requis pour assurer la sécurité de l'accès à distance sont appliqués, conformément aux spécifications de Rio Tinto.

## 4. SÉCURITÉ DU RÉSEAU

Lorsqu'il accède aux réseaux de Rio Tinto, le fournisseur doit prendre toutes les mesures nécessaires pour garantir le maintien de la sécurité du réseau de Rio Tinto, notamment :

(a) Veiller à ce que les réseaux du fournisseur soient bien séparés des réseaux de Rio Tinto.
(b) Appliquer des ensembles de règles à la passerelle entre les zones du réseau pour contrôler et filtrer le trafic afin d'assurer une ségrégation et une segmentation efficaces du réseau[1]. La passerelle doit être préapprouvée et gérée par Rio Tinto.
(c) Adopter une approche de « refus par défaut », n'autorisant que le trafic explicitement défini entre les zones, les règles d'autorisation précisant la source IP, la destination IP et le port TCP/UDP. Ne pas utiliser de règle qui autorise toutes les sources et destinations ou tous les types de service ou de protocole.

## 5. PLAN DE RÉSILIENCE DES SERVICES ET DE REPRISE APRÈS SINISTRE

5.1 Le fournisseur doit garantir la disponibilité et la résilience de ses principaux systèmes technologiques et des données utilisées pour fournir la prestation à Rio Tinto, de manière à ce que celle-ci puisse être rétablie aussi rapidement que possible en cas de panne. Bien que les mesures mises en œuvre par le fournisseur puissent varier (p. ex. utilisation de zones de disponibilité, plans d'intervention et de reprise testés périodiquement, procédures de restauration des sauvegardes, etc.), elles doivent fournir une assurance claire et démontrable que la prestation peut être rétablie dans un délai acceptable.

5.2 Le fournisseur doit maintenir des plans de reprise après sinistre pour tous ses systèmes critiques pendant toute la durée de la fourniture des services à Rio Tinto et aussi longtemps que le nom ou la marque du fournisseur demeure publiquement associés à Rio Tinto, que les services soient ou non toujours fournis. Ces obligations s'appliquent en plus des exigences propres aux services des plans de reprise après sinistre énoncées ailleurs. Tous les plans de reprise après sinistre doivent :

i. prévoir la continuité des services essentiels, y compris les exigences en matière d'intervention et de reprise;
ii. prendre en considération les menaces et les scénarios pertinents en matière de cybersécurité;
iii. être testés périodiquement pour s'assurer que les procédures et les contrôles sont efficaces et que les systèmes et les services peuvent être rétablis dans des délais

[1] Aux fins du présent document, la « ségrégation du réseau » consiste à séparer un réseau d'autres réseaux dont le niveau de confiance est différent, tandis que la « segmentation du réseau » désigne le fait de diviser un réseau en segments de réseau plus petits ou en zones, sur la base de facteurs tels que l'autorité de gestion, le niveau de confiance, la criticité fonctionnelle et l'importance du trafic de communication nécessaire pour franchir les limites de la zone.

acceptables.

## 6. GESTION DU CHANGEMENT

6.1 Dans la mesure où cela s'applique à la prestation fournie à Rio Tinto, le fournisseur doit établir et maintenir des processus efficaces de gestion du changement, notamment en :

(a) se conformant aux processus de gestion du changement applicables de Rio Tinto;
(b) déterminant les types de changements de configuration du système d'information du fournisseur tout en évaluant explicitement l'impact potentiel sur la sécurité;
(c) consignant les décisions associées au changement de configuration des systèmes du fournisseur;
(d) conservant des enregistrements détaillés de tout changement de configuration des systèmes du fournisseur.

6.2 Sur demande, le fournisseur doit permettre à Rio Tinto d'accéder aux enregistrements des changements de configuration liés aux systèmes utilisés pour fournir la prestation.

## 7. CHIFFREMENT

Le fournisseur veille au chiffrement adéquat des informations de Rio Tinto, conformément aux meilleures pratiques de l'industrie (p. ex. NIST FIPS et SP 800, normes ISO/IEC), notamment :

(a) les informations classées par Rio Tinto comme « confidentielles » ou « hautement confidentielles » lorsqu'elles sont stockées au repos par le fournisseur;
(b) toutes les informations, quelle que soit leur classification, transmises par Internet (c.-à-d. en transit).

## 8. SUPPORTS AMOVIBLES

8.1 Les supports amovibles[2] ne doivent pas être connectés à un appareil électronique de Rio Tinto sans l'autorisation écrite préalable de l'équipe de la Cybersécurité de Rio Tinto.
8.2 Lorsque l'utilisation de supports amovibles est approuvée par l'équipe de la Cybersécurité, le fournisseur doit :
(a) restreindre l'accès aux supports amovibles aux seuls membres de son personnel qui doivent y avoir accès dans le cadre de la prestation;
(b) veiller à ce que tous les supports amovibles soient protégés en tout temps et exempts de logiciels malveillants;
(c) tenir à jour des procédures consignées pour la gestion sécuritaire des supports amovibles, qui doivent notamment :
i. préciser les types de supports approuvés;
ii. expliquer les processus de manipulation et d'élimination;
iii. décrire les contrôles techniques mis en œuvre pour assurer la conformité à ces exigences;
iv. être mises à la disposition de Rio Tinto sur demande écrite.

## 9. CESSATION DE LA RELATION

[2] Aux fins de la présente disposition, « supports amovibles » se dit de dispositifs portatifs de stockage informatique conçus pour être insérés et retirés d'un ordinateur ou d'un système, y compris les disques optiques et les clés USB.

À la fin de la relation entre Rio Tinto et le fournisseur, ce dernier doit s'assurer que :

(a) toutes les informations de Rio Tinto détenues par le fournisseur, tant dans ses propres systèmes que dans tout système tiers qu'il utilise, sont soit restituées à Rio Tinto dans un format standard,
(b) ou détruites en toute sécurité, conformément aux instructions de Rio Tinto;
(c) tout accès aux environnements de Rio Tinto du côté du fournisseur (le cas échéant), y compris tout accès accordé au personnel et aux tiers, est immédiatement révoqué, puis confirmer par écrit à Rio Tinto que cela a été fait;
(d) rendre à Rio Tinto tout élément de propriété intellectuelle qui lui appartient.