Annexe ----- au contrat n° -----

SÉCURITÉ DE L'INFORMATION / CYBERSÉCURITÉ

1 Champ d'application, but et contenu

1.1 La présente annexe s'applique à toutes les prestations fournies ou livrées par l'entreprise dans le cadre du présent contrat. L'annexe décrit les exigences minimales ainsi que les obligations de l'entreprise en matière de réduction des cyberrisques (ci-après, ce terme couvre également les risques liés à la sécurité de l'information) et complète les exigences de la législation applicable ainsi que d'autres exigences spécifiques aux clients et aux lieux d'intervention.

1.2 Dans la présente annexe, les termes «sécurité», «sûr» ou «lié à la sécurité» font référence à la protection et à la résilience face à la sécurité de l'information ou aux cyberrisques. Le domaine de la sécurité fonctionnelle (safety) n'entre pas dans le champ de la présente annexe.

2 Gestion de la sécurité

2.1 L'entreprise maintient un système de gestion de la sécurité lié à l'entreprise destiné à réduire les cyberrisques (par exemple selon ISO/CEI 27001 ou CEI 62443-2-1) qui est adapté, de par sa nature et son ampleur, à la prestation à fournir et qui correspond à l'état reconnu de la technique.

2.2 L'entreprise veille à ce que ses propres employés ainsi que les employés des sous-traitants qui participent au développement et à la fabrication des produits et des composants ou auxquels il est fait appel pour fournir des services soient sensibilisés et formés en ce qui concerne les cyberrisques, qu'ils connaissent les réglementations applicables, qu'ils aient été contrôlés de manière appropriée en ce qui concerne leur intégrité et qu'ils soient contrôlés régulièrement. Elle garantit également que ces collaborateurs utilisent leurs droits d'accès aux systèmes et aux données des CFF exclusivement pour remplir leurs obligations contractuelles.

2.3 Dans le domaine du développement de logiciels et de produits, l'entreprise met en œuvre des processus visant à réduire les cyberrisques. Ceux-ci sont fondés, en cas de traitement de données personnelles, sur les principes de «security by design» (sécurité dès la conception) et de «privacy by design» (respect de la vie privée dès la conception). L'entreprise se base sur des méthodes et des normes reconnues, telles que la norme IEC 62443-4-1 ou NIST SP 800-160.

2.4 Pour la divulgation des vulnérabilités, l'entreprise a mis en place des directives et des processus conformes à des méthodes et à des normes reconnues telles que la norme ISO/CEI 29147. Ces processus et directives définissent notamment la manière dont les vulnérabilités peuvent être signalées, comment elles sont évaluées et comment les informations sur les vulnérabilités sont communiquées à CFF SA.

2.5 L'entreprise a mis en place les processus nécessaires pour traiter les vulnérabilités, et elle se base pour ce faire sur des méthodes et des normes reconnues (par ex. ISO/IEC 30111).

3 Personne de contact pour la cybersécurité

3.1 Les parties désignent une personne de contact qui sera responsable de la coordination des accords, du contrôle du respect des exigences de laprésente annexe et des accords complémentaires.

3.2 Les parties veillent à ce que pendant la durée du projet et la période de maintenance du produit, les changements de personnes de contact soient communiqués à l'autre partie en temps utile.

3.3 L'entreprise communique un contact général pour les questions relatives à la cybersécurité, qui peut être joint même après l'expiration du contrat.

4 Incidents de sécurité

4.1 L'entreprise informe immédiatement CFF SA en cas d'incidents de sécurité importants.

4.2 La société soutient CFF SA lors d'incidents de cybersécurité en lien avec ses produits et services.

4.3 L'entreprise s'engage à assurer une journalisation (log) adéquate des systèmes et des produits afin de permettre leur intégration dans un système de surveillance central. Si les données de journalisation sont gérées par l'entreprise, celle-ci fournit à CFF SA les rapports de sécurité correspondants et veille à ce que les données de journalisation soient conservées pendant une période suffisante.

4.4 En cas d'incidents de sécurité ayant un impact pour CFF SA, tous les documents et données nécessaires sont mis à disposition pour permettre une résolution rapide de l'incident.

5 Gestion des vulnérabilités et des correctifs

5.1 L'entreprise informe CFF SA de manière proactive au sujet des vulnérabilités importantes.

5.2 Le produit ou service a la capacité de corriger les erreurs de logiciel (y compris du micrologiciel et du système d'exploitation) qui entraînent un risque de cybersécurité. Le logiciel (y compris le micrologiciel et le système d'exploitation) peut à cet effet être mis à jour de manière appropriée.

5.3 L'entreprise doit mettre à disposition un processus établi pour les mises à jour logicielles. Le processus comprend les mesures nécessaires pour garantir l'authenticité et l'intégrité des mises à jour logicielles livrées.

5.4 L'entreprise veille à ce que les mises à jour logicielles qui concernent des vulnérabilités en matière de cybersécurité soient fournies ou appliquées en temps utile.

6 Livraison, documentation et exploitation

6.1 Si l'entreprise fournit des produits, elle doit mettre à la disposition de CFF SA toute la documentation nécessaire à l'intégration et à l'exploitation sûres du produit. Cela comprend, par exemple, les documents d'architecture, les informations sur les algorithmes cryptographiques utilisés, le matériel de chiffrement, les comptes utilisateur et les mots de passe. La transmission des documents se fait sur des canaux ou des systèmes de stockage sécurisés.

6.2 Lors de la livraison des logiciels ou de leurs mises à jour, l'entreprise fournit les moyens nécessaires, tels que les sommes de contrôle, pour vérifier l'authenticité et l'intégrité de la livraison.

6.3 Les conditions environnementales, les réglages et les étapes de mise en service nécessaires au fonctionnement sûr du produit sont clairement indiqués dans la documentation. La documentation doit être mise à jour en tout temps pendant l'intégralité du cycle de vie du produit.

6.4 L'accès aux systèmes de CFF SA à des fins de maintenance doit toujours être déclaré et faire l'objet d'un accord conjoint. Dans la mesure du possible et si cela est économiquement judicieux, il convient d'utiliser les accès de maintenance standard de CFF SA.

7 Réception

7.1 Sauf dispositions contraires dans le contrat ou dans les CG, les règles spécifiques suivantes sont applicables en matière de réception.

7.2 Pour la réception, CFF SA peut exiger des tests de sécurité spécifiques tels qu'un test de pénétration effectué par des experts internes ou externes.

7.3 La réception a lieu à l'issue de la vérification pour autant que celle-ci ne révèle que des vulnérabilités non critiques. L'entreprise élimine immédiatement les vulnérabilités constatées et les signale à CFF SA.

7.4 Si les tests de sécurité révèlent des vulnérabilités critiques, la réception est reportée. L'entreprise élimine immédiatement les vulnérabilités constatées et invite CFF SA en temps utile à une nouvelle vérification.

7.5 Le démarrage de l'utilisation productive ne vaut pas réception, à moins que CFF SA ne l'ait confirmée par écrit.

7.6 Malgré le report de la réception, l'objet du contrat peut, d'un commun accord, être remis à CFF SA pour utilisation, l'ensemble des droits et obligations des parties étant maintenus quant à la réception et à ses effets juridiques.

8 Garantie

8.1 Les vulnérabilités des produits livrés ou des services fournis par l'entreprise constatées au moment de la réception ou par la suite sont considérées comme un défaut au sens du contrat, et les obligations de garantie correspondantes s'appliquent.

9 Droit de contrôle et d'audit des CFF

9.1 Sauf dispositions contraires dans le contrat ou dans les CG, les règles spécifiques suivantes sont applicables concernant le droit de contrôle et d'audit.

9.2 CFF SA est en droit d'exiger que le respect des obligations de l'entreprise au sens du chiffre «Gestion de la sécurité» et le respect des autres obligations essentielles soient vérifiés par un organisme indépendant. La vérification peut être effectuée par CFF SA ou par une entreprise de révision indépendante dans le cadre d'un audit. Chaque partie supporte ses propres frais engagés ou commandés. CFF SA ne peut exiger plus d'un audit de ce type par année civile sans motif justifié.

9.3 Si l'audit n'est pas effectué par CFF SA, le rapport d'audit transmis à CFF SA se limite aux informations entrant dans le cadre strict de l'étendue de l'audit et relatives

au respect par l'entreprise de ses obligations contractuelles. En cas de manquement aux obligations contractuelles, CFF SA dispose d'un droit de regard complet sur les informations pertinentes au sujet du manquement. Dans ce cas, les CFF peuvent facturer à l'entreprise leur part des coûts (y compris le cas échéant celle des entreprises mandatées) de l'inspection.

9.4 L'entreprise accorde à CFF SA et aux partenaires contractuels correspondants de CFF SA le droit de vérifier l'intégrité et la sécurité du matériel et du logiciel du produit (reverse engineering). Il ne s'agit pas là d'une violation des droits de propriété intellectuelle (DPI) de l'entreprise.

10 Sous-traitants

10.1 Sauf dispositions contraires dans le contrat ou dans les CG, les règles spécifiques suivantes sont applicables en cas de recours à des sous-traitants.

10.2 Si l'entreprise recourt à des tiers pour fournir ses prestations, y compris pour mettre à disposition des produits, elle doit intégrer entièrement la part des fournisseurs dans sa gestion de la sécurité et la présenter à la demande des CFF. Elle maintient un système approprié d'évaluation, de sélection et d'évaluation régulière des sous-traitants.

10.3 L'entreprise astreint, preuve à l'appui, les tiers auxquels elle recourt à respecter les engagements qu'elle a pris dans le cadre de la présente annexe ou garantit la cybersécurité de ses livraisons provenant de sous-traitants par ses propres moyens. Les CFF peuvent exiger de l'entreprise des preuves documentées attestant que celle-ci s'est assurée de l'efficacité du système de gestion de la sécurité des tiers auxquels elle recourt.