Normes de Cybersécurité pour les Fournisseurs

Section A – tous les fournisseurs

TOUS les fournisseurs doivent respecter les normes de cybersécurité détaillées ci-dessous.

1. Les fournisseurs doivent être en mesure de démontrer une culture de sensibilisation à la cybersécurité au sein de leur organisation. Cela comprend, mais sans s'y limiter :
    I. la preuve de tout enregistrement à une norme de cybersécurité reconnue (par exemple, celles détaillées dans Cyber Essentials) ;
    II. la formation des employés à la cybersécurité, comprenant un programme d'amélioration continue ;
    III. des sauvegardes robustes ; politiques de réponse aux incidents ; et plans de reprise après sinistre, etc.

2. Le phishing et les logiciels malveillants peuvent souvent provenir de fournisseurs compromis. Par conséquent, les fournisseurs doivent justifier de systèmes de cybersécurité robustes. Cela comprend :
    I. les systèmes de messagerie utilisant l'authentification multi-facteurs ou d'autres mesures de protection, par ex. DMARC ;
    II. des processus en place pour garantir une notification active dans les meilleurs délais si le fournisseur détecte que ses systèmes ont été compromis ou impliqués dans le phishing.

3. En cas de phishing ou de compromission de logiciels malveillants, provenant du fournisseur et détectés par INEOS Inovyn, il doit y avoir un parcours de remontée hiérarchique clair vers le fournisseur.

4. La fraude financière est souvent tentée par des courriels interceptés qui demandent au destinataire de modifier les coordonnées bancaires du fournisseur.
    Dans le cadre de la politique antifraude d'INEOS Inovyn, les fournisseurs doivent disposer d'un processus clairement défini par lequel ils informeraient INEOS Inovyn des changements légitimes, avec des contacts nommés qu'INEOS Inovyn utilisera pour des contrôles indépendants afin de confirmer la validité.

5. Les fournisseurs qui stockent des données liées à INEOS Inovyn doivent s'assurer que ce stockage est conforme aux exigences légales de protection des données en fonction de chaque pays, y compris :
    I. La conformité au règlement général sur la protection des données (RGPD) ou équivalent ;
    II. Les données INEOS Inovyn stockées sur des appareils portables, par ex. ordinateurs portables, doivent utiliser le cryptage complet du disque.

6. Toute méthode utilisée pour transférer des logiciels ou des données dans le cadre du travail du fournisseur doit utiliser des mécanismes convenablement sécurisés, tels que :
    I. un site sécurisé SharePoint hébergé par INEOS Inovyn ;
    II. un site de transfert de fichiers sécurisé fourni par le fournisseur et certifié par INEOS Inovyn.

7. Les dispositifs de transfert de masse tels que les clés / lecteurs USB ne doivent être utilisés que lorsqu'il n'existe aucun autre mécanisme pratique et doivent dans tous les cas être conformes aux politiques et aux contrôles d'INEOS Inovyn au moment de l'utilisation.

Section B - Fournisseurs de systèmes et de ressources devant travailler sur les systèmes INEOS Inovyn

En plus de la section A, TOUS les fournisseurs de systèmes, d'équipements et de ressources qui travailleront sur les systèmes INEOS Inovyn doivent s'assurer que les exigences supplémentaires suivantes sont respectées.

8. Les systèmes fournis et tout équipement rebadgé doivent utiliser des plateformes prises en charge par le fournisseur avec une durée de vie minimale prévue de 5 ans. Cela comprend des aspects tels que :
    I. systèmes d'exploitation (OS) ;
    II. firmware ;
    III. recours à des applications, composants et navigateurs Web tiers.

9. Les systèmes fournis doivent pouvoir être mis à jour face aux vulnérabilités futures, par exemple:
    I. application de correctifs réguliers du système d'exploitation ;
    II. application des mises à jour de version du système d'exploitation ;
    III. le fournisseur doit indiquer son processus de test et d'approbation des correctifs, par ex. durée de la phase d'approbation des fournisseurs, dispositions particulières pour les correctifs particulièrement critiques.
10. Les systèmes fournis doivent avoir la capacité de cyber protection, y compris des mesures telles que :
    I. protection antivirus de base ;
    II. protection par liste blanche des applications ;
    III. protection avancée contre les logiciels malveillants ;
    IV. protection du réseau par des dispositifs pare-feu ;
    V. le fournisseur ne doit pas être identifié par le gouvernement comme étant vulnérable en matière de cybersécurité, et donc soumis à des restrictions.

11. Si un fournisseur se voit accorder un accès à distance aux systèmes INEOS Inovyn, un tel accès doit uniquement être utilisé aux fins prévues, et uniquement aux systèmes identifiés dans le champ d'application du support, de l'accord de niveau de service (SLA), etc. :

I. toutes ces tâches doivent être convenues avec INEOS Inovyn avant d'avoir lieu et faire l'objet d'un examen régulier (par an, au minimum).

12. En cas d'accès à distance accordé à n'importe quelle partie des systèmes INEOS Inovyn, des exigences supplémentaires peuvent être requises, telles que :
    I. personnes nommées uniquement - y compris les vérifications des antécédents possibles, la preuve de formation, adjoints nommés convenus, etc.
    II. authentification de second facteur détenue par INEOS Inovyn.

13. Lorsque les fournisseurs fournissent des ressources plutôt que des systèmes à INEOS Inovyn, on s'attend à ce que toutes les ressources fonctionnent dans le respect des directives d'INEOS Inovyn pour la cybersécurité, à la fois sur nos sites ou ailleurs dans le cadre de travaux liés à INEOS Inovyn. Ces directives doivent être normalement communiquées dans le cadre du processus d'intégration d'INEOS Inovyn.

FIN DU DOCUMENT

V1. Août 2020