Exigences de sécurité pour les fournisseurs d’Alludo

Table des matières

Introduction

Ce document présente les pratiques des sociétés du groupe Alludo (désignées collectivement « Alludo ») en matière de sécurité de l'information, de continuité des activités et de confidentialité, ainsi que le programme d'évaluation des mesures de sécurité et de continuité des fournisseurs d'Alludo. Les processus, procédures, exigences et obligations mentionnés dans le présent document sont collectivement appelés les « Normes Alludo ».

Le présent **document Exigences de sécurité pour les fournisseurs** informe les fournisseurs de biens et de services (les « fournisseurs ») des attentes en matière de sécurité, de continuité des activités et de confidentialité dont Alludo les tient responsables lorsqu'ils fournissent des services. Les fournisseurs doivent respecter ces exigences en mettant en œuvre les meilleures pratiques de l'industrie et leurs politiques de sécurité d'entreprise. Alludo ne sera pas responsable des problèmes

rencontrés par les fournisseurs, y compris la perte de données ou les dommages matériels, quelle qu'en soit la cause.

En cas d'incohérence entre ce document et un accord écrit, les termes de l'accord écrit prévaudront. Les fournisseurs doivent également se conformer à toutes les exigences réglementaires locales, nationales ou régionales. En cas de conflit entre le présent document et les réglementations applicables, les fournisseurs doivent en informer Alludo et proposer d'autres contrôles pour maintenir des normes équivalentes en matière de sécurité, de continuité des activités ou de confidentialité.

Présentation des exigences de sécurité pour les fournisseurs

Alludo a la responsabilité de protéger ses informations confidentielles et à diffusion restreinte contre tout accès ou toute divulgation non autorisés. Pour ce faire, Alludo applique les Normes Alludo, des normes internes de sécurité de l'information, de continuité des activités et de confidentialité, afin de garantir la protection de ces informations confidentielles et à diffusion restreinte et la disponibilité permanente des services fournis par Alludo. Pour garantir la conformité d'Alludo aux normes internes et aux exigences réglementaires relatives à la sécurité de l'information et à la continuité des activités, Alludo exige que ses fournisseurs adhèrent aux Normes Alludo décrites dans le présent document.

De même, dans la mesure où un fournisseur délègue ou sous-traite une partie de ses obligations en vertu de son accord avec Alludo, ou engage un autre fournisseur pour fournir des services directement ou indirectement à Alludo, le fournisseur doit exiger de cet autre fournisseur qu'il mette en œuvre et administre un programme et un plan de protection des informations conformes aux normes d'Alludo. Alludo s'engage à travailler raisonnablement avec ses fournisseurs pour les aider à respecter les exigences de conformité relatives aux Normes Alludo. L'applicabilité de ces Normes Alludo à un fournisseur donné variera en fonction du type de services et de produits fournis par ce fournisseur à Alludo.

Contrôle des accès et des identités

Le fournisseur doit assurer ce qui suit :

1. **Contrôle des accès et gestion des utilisateurs :**
   - 1.1. Une politique documentée de contrôle des accès est en place et revue au moins une fois par an.
   - 1.2. Les rôles, autorisations et droits d'accès des utilisateurs sont définis et documentés.
   - 1.3. Des processus standard pour l'arrivée et le départ d'utilisateurs sont en place, y compris la tenue de registres des approbations pertinentes.
   - 1.4. L'accès aux composants de l'infrastructure informatique est accordé selon le principe du moindre privilège et géré par des outils de gestion des identités (par exemple, Active Directory, OKTA ou similaire).

1.5. L'accès individuel aux systèmes, aux ressources réseau et aux autres ressources informatiques est officiellement approuvé et contrôlé par des identifiants uniques et des mots de passe individuels.
1.6. La séparation des tâches est maintenue lors de la création/modification des identifiants et de l'attribution des privilèges.

2. Politiques relatives aux mots de passe et à l'authentification :

2.1. Les utilisateurs sont tenus de modifier leur mot de passe lors de leur première connexion.
2.2. Les mots de passe répondent aux exigences des normes du secteur, notamment en matière de longueur, d'expiration, de complexité, d'historique des mots de passe, de tentatives infructueuses, de durée de verrouillage du compte, d'ancienneté du mot de passe et de modification lors de la première connexion.
2.3. Des mécanismes sécurisés sont utilisés pour fournir les mots de passe des utilisateurs et valider leur identité avant de réinitialiser les mots de passe.
2.4. Les systèmes qui ne prennent pas en charge l'authentification IdP ou qui doivent être conçus de manière autonome sont configurés pour appliquer une authentification forte, au moins équivalente à la configuration définie dans les politiques centrales de contrôle des mots de passe et des accès.
2.5. Tous les systèmes et applications sont configurés pour utiliser des procédures de connexion sécurisées via des mécanismes approuvés de gestion des identités et des accès.
2.6. Les systèmes et applications sont configurés pour que les sessions inactives expirent afin d'empêcher tout accès non autorisé.

3. Gestion des accès privilégiés :

3.1. L'accès privilégié aux ressources est limité à des rôles d'utilisateurs définis et approuvé par le personnel autorisé.
3.2. Les comptes d'utilisateurs privilégiés sont configurés pour utiliser l'authentification à plusieurs facteurs.
3.3. Les privilèges qui ne sont plus nécessaires sont immédiatement révoqués.
3.4. L'utilisation des identifiants d'administrateur est limitée à des circonstances précises, telles que le dépannage, et les utilisateurs effectuent les opérations quotidiennes avec les identifiants les moins privilégiés.
3.5. L'accès aux infrastructures, systèmes, périphériques réseau et applications informatiques critiques (par exemple, accès à distance, serveurs critiques, périphériques réseau) est protégé par une authentification à plusieurs facteurs.

4. Suivi et révision des accès :

4.1. Des révisions périodiques des droits d'accès sont effectuées et les exceptions identifiées sont traitées rapidement.
4.2. Un rapprochement de tous les identifiants d'utilisateur (y compris le domaine, les applications, les périphériques réseau, les systèmes informatiques, les intergiciels, les bases de données, etc.) est effectué au maximum une fois par an, et des mesures correctives immédiates sont prises pour toute anomalie identifiée.

5. Gestion des tiers et des fournisseurs :

5.1. L'accès des fournisseurs tiers aux réseaux et systèmes est strictement contrôlé, sur la base du besoin avéré et d'une approbation formelle.

5.2. Les identifiants par défaut fournis par les fournisseurs sont modifiés avant la mise en production des systèmes, des applications, des périphériques réseau ou d'autres dispositifs de l'infrastructure informatique.

6. Considérations particulières en matière d'accès :

6.1. Les identifiants génériques et partagés ne sont pas utilisés, sauf si cela est formellement justifié et approuvé par la direction générale, avec des mécanismes permettant de suivre leur utilisation et de remonter jusqu'aux individus.

6.2. Tous les accès en mode administrateur sans console sont chiffrés à l'aide d'algorithmes de chiffrement approuvés par l'industrie, et les protocoles non sécurisés (par exemple, telnet/ftp) sont interdits pour les accès en mode administrateur sans console.

Gestion des ressources

Le fournisseur doit assurer ce qui suit :

7. Gestion des ressources et des stocks :

7.1. Des inventaires complets des ressources sont tenus à jour, et contiennent des informations essentielles telles que le nom du propriétaire, ses coordonnées et l'emplacement.

7.2. Les registres des ressources informatiques, y compris le matériel, les systèmes d'exploitation, les applications et les bases de données, sont régulièrement mis à jour et vérifiés pour garantir leur exactitude.

7.3. Des procédures de gestion des ressources et des contrôles de configuration sont établis et maintenus pour gérer la disponibilité des ressources critiques et les configurations des réseaux et des systèmes d'information vitaux.

8. Classification et identification des informations :

8.1. Une politique de classification des informations, accompagnée de procédures et de directives, est mise en place. Toutes les ressources sont identifiées conformément aux instructions établies, et les informations sont classées et protégées en fonction de niveaux de classification définis.

9. Manipulation des ressources :

9.1. Les directives de gestion des ressources pour une manipulation correcte sont conservées et communiquées à tous les employés et sous-traitants concernés.

9.2. Des procédures documentées sont en place pour protéger les ressources d'information, identifier les ressources à éliminer et assurer l'élimination sécurisée de ces ressources.

9.3. Des processus sont établis pour garantir que les ressources allouées sont rapidement restituées à l'équipe de gestion des ressources correspondante en cas de résiliation ou de cessation d'emploi, de contrat ou d'accord.

10. Gestion des appareils mobiles et des supports amovibles :

10.1. Des politiques et procédures de contrôle des appareils mobiles (y compris les appareils apportés par les employés) utilisés pour stocker, transmettre ou traiter des informations professionnelles sont mises en œuvre. Des mesures de protection adéquates sont requises

avant d'autoriser les appareils mobiles à accéder aux informations et ressources professionnelles.

10.2. L'utilisation de dispositifs de stockage de masse amovibles doit être chiffrée pour garantir la sécurité des données.

11. Conformité des logiciels :

11.1. L'utilisation de logiciels sans licence ou non approuvés est interdite. Des processus sont en place pour identifier toute infraction et prendre les mesures nécessaires pour y remédier.

Opérations informatiques

Le fournisseur doit assurer ce qui suit :

12. Opérations liées aux systèmes critiques :

12.1. Des procédures d'exploitation des réseaux et systèmes d'information critiques sont établies et mises à jour, et comprennent :

12.1.1. Des processus d'approbation formels pour l'accès aux ressources informatiques.

12.1.2. Des mécanismes d'authentification robustes pour toutes les technologies (par exemple, VPN, connexion Windows).

12.1.3. La révision régulière des droits de privilège.

12.1.4. L'identification des emplacements réseau pour les technologies critiques en fonction des exigences de continuité des activités.

13. Gestion des changements :

13.1. Un processus complet de gestion des changements est mis en œuvre pour les systèmes informatiques, les applications, les bases de données et les composants réseau, garantissant :

13.1.1. La consignation, la révision, le test et l'approbation formelle de tous les changements.

13.1.2. Des plans de restauration pour les modifications potentiellement perturbatrices.

14. Divers :

14.1. Les systèmes et les composants réseau traitant des informations sensibles et confidentielles sont soumis à des contrôles de surveillance de l'intégrité des fichiers.

14.2. Tous les systèmes et composants réseau sont configurés pour utiliser des sources NTP (Network Time Protocol) autorisées afin d'assurer une synchronisation précise de l'heure.

14.3. Des processus de maintenance réguliers, proactifs et préventifs sont mis en place pour tous les systèmes, applications, périphériques réseau et machines des utilisateurs finaux critiques.

14.4. Les règles des pare-feu et des routeurs sont révisées périodiquement ou conformément aux normes de l'industrie, et les règles inutiles ou non autorisées sont rapidement supprimées.

14.5. Des contrôles sont mis en place pour maintenir l'intégrité des informations et des logiciels dans l'ensemble de l'environnement informatique.

Sécurité des ressources humaines

Le fournisseur doit assurer ce qui suit :

15. **Vérifications des antécédents :**
    15.1. Établir et maintenir des politiques et procédures pour la vérification des antécédents.
    15.2. Effectuer les vérifications d'antécédents appropriées sur les employés et les sous-traitants avant leur embauche, dans la mesure où la loi le permet, en fonction de leurs fonctions et responsabilités.
16. **Gestion des changements de personnel** :
    16.1. Mettre en place un processus de gestion des changements de personnel ou de leurs rôles et responsabilités, y compris la formation du nouveau personnel aux politiques et procédures pertinentes.
    16.2. Révoquer les droits d'accès, les badges, les équipements et autres ressources rapidement après les changements de personnel lorsqu'ils ne sont plus nécessaires ou autorisés.
17. **Application des politiques** :
    17.1. Mettre en œuvre et appliquer une procédure disciplinaire claire pour les employés qui enfreignent les politiques de sécurité.
    17.2. Garantir la mise en cause des auteurs des violations des politiques de sécurité par des mesures contractuelles appropriées. Cela inclut l'intégration de clauses pertinentes dans les contrats de travail du personnel et les accords de service des sous-traitants.

Formation à la sécurité et à la confidentialité

Le fournisseur doit assurer ce qui suit :

18. La formation à la sécurité et à la confidentialité est obligatoire pour tous les employés et sous-traitants. Cette formation doit être suivie lors de l'embauche initiale, puis annuellement ou moins fréquemment par la suite.
19. Les employés et sous-traitants ayant d'importantes responsabilités en matière de sécurité informatique suivent une formation annuelle spécialisée adaptée à leurs rôles et fonctions spécifiques en matière de sécurité.
20. La direction a accès à des outils et des systèmes qui lui permettent de suivre et de contrôler les progrès de la formation de ses employés et sous-traitants.
21. Le programme de formation et de sensibilisation de l'organisation fait l'objet de révisions et de mises à jour périodiques. Ce processus tient compte de l'évolution des besoins de l'entreprise, des changements législatifs et des leçons tirées des incidents de sécurité passés.

Sécurité des informations et gouvernance

Le fournisseur doit assurer ce qui suit :

22. **Cadre de sécurité et gouvernance :**
    22.1. Le fournisseur doit mettre en œuvre un cadre de normes de sécurité reconnu (par exemple, NIST CSF, RMF, 800-53, ISO 27001, CIS) pour la gouvernance de l'information et de la cybersécurité. Ce cadre doit inclure :

22.1.1. Des politiques et procédures complètes en matière d'information et de cybersécurité, soumises à un réexamen annuel, à une approbation formelle et à une communication à l'échelle de l'organisation.
22.1.2. Une stratégie de sécurité de l'information bien définie et alignée sur les objectifs commerciaux.
22.1.3. Des processus robustes de gouvernance et de gestion des risques, traitant spécifiquement des risques liés à l'information et à la cybersécurité.
22.1.4. Des mécanismes de conformité pour répondre aux exigences légales et réglementaires en matière d'information et de cybersécurité.

22.2. S'il ne respecte pas un cadre de sécurité reconnu, le fournisseur doit soumettre un rapport démontrant que son environnement a fait l'objet d'un audit.
22.2.1. Un plan de correction des problèmes identifiés, comprenant des délais prévus, doit être convenu d'un commun accord entre le fournisseur et Alludo.

23. Direction et structure organisationnelle :

23.1. Les rôles et responsabilités appropriés en matière de sécurité de l'information et de cybersécurité sont définis et mis en œuvre à l'échelle de toute l'organisation.

24. Gestion et évaluation des risques :

24.1. Un cadre formel de gestion des risques approuvé par la direction générale est en place pour :
24.1.1. Identifier les menaces internes et externes.
24.1.2. Évaluer la sensibilité des informations/données concernées.
24.1.3. Évaluer les impacts commerciaux potentiels.
24.1.4. Évaluer les menaces, les vulnérabilités et les risques correspondants.
24.1.4.1. Tous les risques et menaces identifiés sont classés par ordre de priorité, et des mesures sont prises en temps utile pour atténuer les risques en conséquence.
24.1.4.2. Des processus et/ou des outils sont mis en œuvre pour identifier les événements qui entraînent des interruptions des principaux objectifs commerciaux de l'organisation.
24.1.4.3. Le fournisseur doit immédiatement informer Alludo s'il n'est pas en mesure de remédier à ou de réduire tout risque important susceptible d'avoir un impact sur le service fourni.

25. Suivi de la conformité et des performances :

25.1. Des processus sont en place pour identifier, enregistrer et suivre toutes les exigences légales, réglementaires et contractuelles applicables à l'organisation.
25.2. Des évaluations périodiques sont effectuées pour valider le respect des obligations légales, réglementaires et contractuelles. Des registres sont tenus pour ces évaluations et les lacunes identifiées sont comblées sans retard injustifié.
25.3. Les politiques, procédures et directives sont revues au moins une fois par an et mises à jour conformément aux exigences légales, réglementaires et contractuelles.
25.4. Les indicateurs clés de performances pour les fonctions essentielles telles que l'informatique, la sécurité de l'information et la confidentialité des données, etc. sont définis, officiellement documentés, périodiquement évalués et communiqués à la direction.

Sécurité du réseau

Le fournisseur doit assurer ce qui suit :

26. Conception du réseau et architecture de sécurité :

26.1. Le réseau du fournisseur utilise des principes de « défense en profondeur », intégrant des contrôles appropriés tels que la segmentation du réseau afin de minimiser les violations de la sécurité de l'information et de la cybersécurité.

26.2. Une conception d'architecture robuste est mise en œuvre, avec une gestion efficace des identités et des configurations de système d'exploitation robustes.

26.3. La conception et la mise en œuvre du réseau font l'objet d'examens annuels afin de garantir une efficacité et une sécurité continues.

26.4. La configuration du réseau est conforme à toutes les exigences légales et réglementaires applicables.

27. Contrôle d'accès et authentification :

27.1. Les connexions réseau externes doivent être documentées, acheminées via des pare-feu, vérifiées et approuvées avant d'être établies.

27.2. L'accès au réseau sans fil nécessite une authentification, une autorisation, une segmentation et un chiffrement. Des systèmes sont en place pour détecter les points d'accès sans fil non autorisés ou les connexions non autorisées et y répondre.

27.3. L'accès à distance au réseau du fournisseur doit être approuvé et effectué par des moyens sécurisés, avec une authentification à plusieurs facteurs.

27.4. Des contrôles sont mis en place pour empêcher ou minimiser l'accès non autorisé au réseau du fournisseur.

28. Administration et gestion sécurisées :

28.1. Tout le trafic réseau lié à la gestion entre les postes de travail des administrateurs et les périphériques réseau utilise des protocoles de chiffrement et d'authentification standard.

28.2. L'accès administrateur sans console s'effectue exclusivement par des canaux chiffrés approuvés par l'industrie.

28.3. Les comptes invité sont désactivés ou supprimés, et tous les mots de passe par défaut et ceux fournis par le fournisseur sont modifiés avant le déploiement des périphériques réseau dans l'environnement de production.

29. Renforcement du réseau et protection contre les menaces :

29.1. les services, applications et ports inutilisés sont désactivés afin de réduire la surface d'attaque.

29.2. Des mesures de détection et/ou de prévention des intrusions sont déployées pour les segments critiques du réseau.

29.3. Les systèmes critiques sont protégés contre les attaques par déni de service (DoS) et par déni de service distribué (DDoS).

Cryptographie

Le fournisseur doit assurer ce qui suit :

30. Une politique de cryptographie complète, ainsi que des procédures de soutien, sont mises en œuvre pour assurer la conformité avec toutes les exigences légales, réglementaires et commerciales pertinentes. Cette politique suit les meilleures pratiques de l'industrie pour garantir un cryptage sécurisé conformément aux lois et normes applicables.

31. Normes de cryptage et mise en œuvre :

31.1. Seuls les algorithmes de cryptage et les niveaux de sécurité approuvés par l'industrie sont autorisés, garantissant une protection adéquate des données dans tous les systèmes et processus.

31.2. Des solutions cryptographiques sont mises en œuvre pour protéger les informations confidentielles et restreindre l'accès aux données sensibles, y compris le chiffrement des données en transit et au repos.

31.3. Tout stockage et transmission de mot de passe est chiffré, ce qui permet de préserver la confidentialité des identifiants des utilisateurs à tout moment.

31.4. Les données Alludo en transit doivent être chiffrées (TLS 1.2 au minimum ou norme plus récente).

31.5. Les données Alludo au repos doivent être chiffrées (AES 256 bits au minimum ou norme plus récente).

Sécurité des données

Le fournisseur doit assurer ce qui suit :

32. Récupération :

32.1. **Sauvegarde et récupération des données** :

32.1.1. Des sauvegardes des données Alludo doivent être effectuées périodiquement.

32.1.2. Les sauvegardes des données Alludo doivent être conservées pendant 1 an.

32.1.3. Les sauvegardes des données d'Alludo doivent être chiffrées.

32.2. **Reprise après sinistre** :

32.2.1. Le plan de reprise d'activité après sinistre doit être testé chaque année.

33. Politique et procédure de sauvegarde :

33.1. La politique de sauvegarde et les procédures associées doivent être clairement documentées.

33.2. Les processus de restauration des sauvegardes doivent être documentés et testés à une fréquence définie.

33.3. Les preuves des tests de restauration des sauvegardes doivent être conservées.

33.4. Une copie des fichiers de sauvegarde des données critiques doit être conservée en lieu sûr.

34. Surveillance des sauvegardes :

34.1. Les journaux des sauvegardes ayant échoué (le cas échéant) doivent être surveillés par l'administrateur des sauvegardes.
34.2. Des mesures correctives doivent être prises et documentées pour les sauvegardes ayant échoué.

35. **Emplacement des données** :
35.1. Le fournisseur est tenu de veiller au respect de toutes les lois applicables en matière de protection des données et de la vie privée dans les pays où les données seront stockées.
35.2. Il doit respecter les restrictions relatives au transfert transfrontalier de données (RGPD, etc.).
35.3. Le fournisseur doit mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger les données, conformément aux lois et aux normes des pays où les données sont stockées.
35.4. Alludo se réserve le droit de contrôler les pratiques du fournisseur en matière de traitement des données afin de garantir le respect des mesures de sécurité convenues et des réglementations locales.

36. **Suppression des données** :
36.1. Des procédures de suppression sécurisée des données à la fin du contrat doivent être mises en place, garantissant le respect des lois locales en matière de conservation des données.

37. **Chiffrement intégral des disque** :
37.1. Le chiffrement intégral des disques doit être configuré pour les postes de travail et les serveurs.

38. **Classification des données :**
38.1. Une politique documentée de classification des données doit être en place.
38.2. Les données doivent être classées en fonction de leur caractère critique et sensible.
38.3. Les contrôles de sécurité correspondant à la sensibilité des données doivent être identifiés et mis en œuvre.

Communication des informations

Le fournisseur doit assurer ce qui suit :

39. **Sécurité Web** :
39.1. Un logiciel de filtrage de contenu Web est mis en place pour bloquer l'accès aux sites Web hébergeant des contenus malveillants.
39.2. Tous les systèmes et applications basés sur le Web doivent être accessibles via des mécanismes sécurisés et authentifiés.
39.3. La communication client-serveur pour les applications et les portails Web doit se faire sur des canaux cryptés.

40. **Sécurité du système de messagerie** :

40.1. Des contrôles de sécurité sont en place pour empêcher toute utilisation abusive du système de messagerie électronique.
40.2. Toutes les communications par message électronique doivent être transmises par des canaux cryptés.
40.3. La passerelle de messagerie est équipée de :
40.3.1. Filtres anti-hameçonnage.
40.3.2. Activer les protocoles de sécurité pour les messages électroniques (DMARC, DKIM et SPF).
40.3.3. Autres configurations nécessaires pour prévenir les menaces véhiculées par message électronique.

Développement de logiciels

Le fournisseur doit assurer ce qui suit :

41. Cycle de développement logiciel :
41.1. Un cadre de développement de logiciels et de systèmes doit être en place.
41.2. Les systèmes et les applications doivent être développés conformément aux meilleures pratiques de développement de logiciels sécurisés (par exemple, OWASP).
41.3. Le code des logiciels doit être :
41.3.1. Protégé contre toute modification non autorisée
41.3.2. Stocké de manière sécurisée
41.3.3. Soumis à des processus d'assurance qualité
41.4. Des révisions de code doivent être effectuées.

42. Test et déploiement :
42.1. Les applications doivent être soumises à des tests de sécurité et de fonctionnalité approfondis avant d'être déployées dans l'environnement de production.
42.2. Les environnements de production et de non-production doivent être séparés de manière appropriée.
42.3. La séparation des tâches entre le développement de la production et le développement de la non-production doit être maintenue.
42.4. Les données de production ne doivent pas exister dans un environnement de test.

Sécurité des applications

Le fournisseur doit assurer ce qui suit :

43. Sécurité des applications :
43.1. Des évaluations de la sécurité des applications sont effectuées pour toutes les nouvelles applications et pour toutes les applications existantes qui subissent des modifications importantes afin d'identifier les vulnérabilités de sécurité connues.
43.2. Toutes les vulnérabilités de sécurité identifiées avec un score CVSS supérieur à 4 sont neutralisées avant de déployer l'application dans l'environnement de production.

43.3. Des processus de révision du code sont mis en œuvre pour identifier et corriger le code susceptible d'introduire des vulnérabilités de sécurité.

44. Protection des applications Web :

44.1. Les applications Web destinées au public sont protégées par un pare-feu d'application Web robuste afin de prévenir les menaces externes.

Gestion des correctifs

Le fournisseur doit assurer ce qui suit :

45. Les derniers correctifs de sécurité sont appliqués aux systèmes, réseaux, applications, bases de données, etc. en temps utile et en fonction du caractère critique de la vulnérabilité traitée par le correctif. Les correctifs sont obtenus directement auprès des revendeurs OEM respectifs pour les systèmes propriétaires.

46. Tous les correctifs sont testés avant leur déploiement dans les systèmes de production et le bon fonctionnement du service corrigé est vérifié après toute activité de correction.

47. Des mesures d'atténuation appropriées sont en place si un système ne peut pas être corrigé, l'efficacité de ces mesures d'atténuation est évaluée périodiquement et les preuves correspondantes sont conservées.

Protection contre les logiciels malveillants

Le fournisseur doit assurer ce qui suit :

48. Tous les systèmes informatiques sont protégés en permanence par une solution de protection contre les logiciels malveillants qui inspecte les données entrantes en temps réel afin d'éviter les interruptions de service ou les failles de sécurité. En outre, des procédures de sensibilisation des utilisateurs sont mises en œuvre. Le système de protection contre les logiciels malveillants détecte diverses menaces, notamment les virus, les logiciels espions, les vers, les codes mobiles non autorisés, les enregistreurs de frappe, les botnets et les chevaux de Troie.

49. Les signatures de logiciels malveillants sont régulièrement mises à jour pour garantir que les systèmes sont toujours équipés des dernières définitions de menaces.

50. Le logiciel de protection contre les logiciels malveillants est configuré pour effectuer des analyses programmées et à la demande, et pour isoler ou supprimer tout fichier ou logiciel malveillant identifié.

51. Les utilisateurs finaux n'ont pas le droit ni la possibilité de désactiver la protection contre les logiciels malveillants.

Gestion des vulnérabilités

Le fournisseur doit assurer ce qui suit :

52. Processus de gestion des vulnérabilités :

52.1. Des politiques, processus et procédures établis pour une gestion complète des vulnérabilités.

52.2. Des processus pour recevoir, analyser et répondre aux vulnérabilités provenant de sources internes et externes.

53. Évaluation et correction des vulnérabilités :

53.1. Des évaluations trimestrielles des vulnérabilités de l'infrastructure informatique et des applications du fournisseur, y compris les sites de reprise après sinistre.

53.2. La correction des vulnérabilités identifiées avec un score CVSS supérieur à 4 doit être effectuée dans les délais impartis.

54. Test de pénétration :

54.1. Des tests de pénétration indépendants sont réalisés chaque année sur l'infrastructure informatique du fournisseur et sur les applications utilisées pour les services Alludo.

54.2. Les tests visent à identifier les vulnérabilités exploitables et à prévenir les atteintes à la sécurité par le biais de cyberattaques.

54.3. L'accès aux rapports de tests de pénétration/vulnérabilité pertinents est accordé à Alludo sur demande raisonnable.

Consignation et suivi

Le fournisseur doit assurer ce qui suit :

55. Les systèmes critiques, y compris les applications, sont configurés pour enregistrer les événements clés (y compris ceux liés aux accès privilégiés et à l'activité des utilisateurs) et les conserver pendant une période minimale d'un an ou conformément aux exigences réglementaires applicables.

56. Au minimum, les journaux des événements clés (le cas échéant) contiennent les éléments suivants :

56.1. Démarrage et arrêt du système.

56.2. État des services et processus critiques au démarrage et à l'arrêt.

56.3. Changements dans les paramètres de configuration, par exemple, changements dans la configuration du démarrage du système.

56.4. Connexions réussies et échecs de connexion.

56.5. Création, modification et suppression de comptes utilisateur.

56.6. Système/ressources consultés.

56.7. Identification et localisation des personnes ayant accédé aux ressources et de l'endroit d'où elles l'ont fait.

56.8. Date et horodatage.

57. Les journaux d'audit sont collectés et corrélés à partir de plusieurs sources et capteurs, puis stockés en toute sécurité et de manière inviolable pour permettre la reconstitution de tels événements.

58. Des processus de surveillance des événements consignés (de préférence en temps réel) sont mis en place pour détecter toute activité non autorisée, cibler les attaques et garantir l'examen des journaux d'événements clés.

Gestion des incidents

Le fournisseur doit assurer ce qui suit :

59. Les rôles et les processus sont clairement définis afin de garantir une réponse rapide, efficace et organisée aux incidents de sécurité de l'information et de confidentialité.

60. Les employés et les sous-traitants sont formés pour reconnaître ce qui constitue un incident de sécurité, ainsi que pour savoir comment et où signaler tout incident potentiel ou confirmé.

61. Le personnel chargé d'analyser les incidents et d'y répondre est qualifié dans le domaine et suit régulièrement des formations sur les pratiques efficaces de réponse aux incidents.

62. Un registre est tenu pour tous les incidents signalés, détaillant les mesures prises pour atténuer l'impact de l'incident et les leçons tirées de l'événement.

63. Alludo est averti dès que l'organisation a connaissance d'un incident de sécurité le concernant, et au plus tard 24 heures après sa détection.

Sécurité physique et environnementale

Le fournisseur doit assurer ce qui suit :

64. Des politiques et procédures de sécurité physique et de contrôle environnemental, conformes aux normes de l'industrie, sont mises en œuvre.

65. Les installations critiques abritant des systèmes informatiques, des applications et du personnel (par exemple, les centres de données, les sites opérationnels) sont protégées contre les accidents, les attaques et les accès non autorisés.

66. Des mesures de sécurité telles que des contrôles d'accès électroniques, la vérification de l'identité, des gardes de sécurité, la gestion des visiteurs et une surveillance par vidéosurveillance 24 heures sur 24, 7 jours sur 7, sont en place pour empêcher toute entrée non autorisée.

67. Les images de vidéosurveillance sont conservées pendant au moins 30 jours, ou plus longtemps si la réglementation l'exige.

68. L'accès aux installations est limité au personnel autorisé à des fins spécifiques et régulièrement contrôlé.

69. Les visiteurs sont accompagnés, leurs heures d'entrée et de sortie sont enregistrées et ils doivent porter un badge de visiteur à tout moment. Les cartes d'accès ou les clés sont récupérées au moment du départ.

70. Les installations critiques sont protégées contre les coupures de courant par des onduleurs (UPS) ou des générateurs afin d'assurer la continuité des opérations.

71. Une maintenance périodique est effectuée sur les équipements critiques tels que les onduleurs, les générateurs, les détecteurs de fumée, les systèmes d'extinction d'incendie et les systèmes de contrôle d'accès, et des registres sont tenus.

72. Les installations sont construites avec des matériaux ignifuges et équipées d'alarmes incendie, de détecteurs de fumée, de capteurs de température et d'inondation, ainsi que d'extincteurs pour se protéger contre les risques naturels.

73. Des mécanismes d'élimination sécurisés pour les données, tant sur support papier que sur support électronique, sont définis, utilisant des déchiqueteuses à coupe croisée pour le papier et des méthodes telles que la désinfection, la démagnétisation ou la destruction pour les supports électroniques.

74. Une politique dite du « bureau rangé » garantit une manipulation sécurisée des notes autocollantes, des documents écrits et des supports amovibles.

75. L'efficacité des contrôles physiques et environnementaux est évaluée au moins une fois par an.

Confidentialité et protection des données

Si le fournisseur ou ses sous-traitants traitent des données personnelles pour le compte d'Alludo ou des clients d'Alludo, le fournisseur doit s'assurer de ce qui suit :

76. Conformité et gouvernance en matière de protection des données :

76.1. Respecter toutes les lois applicables en matière de protection des données.

76.2. Établir un cadre de gestion de la confidentialité comprenant :

76.3. Les politiques, déclarations, avis et procédures en matière de confidentialité (révisés chaque année).

76.4. Les processus de gouvernance de la protection de la vie privée et de gestion des risques.

76.5. Respecter les exigences légales et réglementaires.

76.6. Tenir à jour les registres des activités de traitement des données à caractère personnel d'Alludo.

76.7. Définir et mettre en œuvre les rôles et responsabilités appropriés en matière de confidentialité des données :

76.8. Nommer un responsable de la protection des données (ou équivalent).

76.9. Créer une fonction spécialisée dans la protection des données.

76.10. Former un comité chargé de coordonner les activités de conformité en matière de protection des données.

77. Mesures de protection et de sécurité des données

77.1. Mettre en œuvre des mesures de protection conformes aux normes de l'industrie (par exemple, ISO/IEC 27001:2013, SOC2, etc.) pour protéger les informations d'Alludo.

77.2. Appliquer des mesures de protection supplémentaires pour les données personnelles sensibles (par exemple, le chiffrement, la pseudonymisation).

77.3. Appliquer des contrôles d'accès :

77.4. Restreindre l'accès en fonction du besoin et du principe du moindre privilège.

77.5. Retirer rapidement les droits d'accès en cas de licenciement ou de changement de poste.

77.6. Procéder à des examens périodiques des droits d'accès.

77.7. Garantir les engagements de confidentialité de l'ensemble du personnel traitant les Données à caractère personnel.

78. Gestion des droits des personnes concernées :

78.1. Aider Alludo à respecter ses obligations en matière de droits des personnes concernées.
78.2. Informer Alludo dans les 2 jours suivant la réception des demandes des personnes concernées.
78.3. Répondre aux demandes uniquement selon les instructions d'Alludo, sauf obligation légale contraire.

79. Réponse aux incidents :

79.1. Informer Alludo dans les 24 heures de toute violation de données à caractère personnel impliquant des données Alludo.

Mesures relatives aux sous-traitants

Le fournisseur doit assurer ce qui suit :

80. Ils procèdent à des évaluations annuelles des risques liés aux tiers pour tous les sous-traitants impliqués dans le traitement, la manipulation ou le stockage des données d'Alludo. Ces évaluations doivent porter sur les contrôles de sécurité des sous-traitants, les mesures de protection des données, le respect des réglementations en vigueur et la position globale en matière de risques. Les fournisseurs doivent fournir sur demande la documentation relative à ces évaluations, traiter rapidement tout risque identifié et communiquer en temps utile tout changement apporté aux sous-traitants ou toute constatation importante. Nous nous réservons le droit d'examiner les résultats des évaluations et de demander des mesures de sécurité supplémentaires si nécessaire.

Gestion de la continuité de l'activité

Le fournisseur doit assurer ce qui suit :

81. Une politique de gestion de la continuité de l'activité (Business Continuity Management, BCM) est mise en place, accompagnée de plans et de procédures détaillés. Ces documents décrivent les objectifs de l'organisation en matière de continuité de l'activité et font l'objet d'un examen et d'une approbation annuels.
82. Un cadre de test pour la gestion de la continuité de l'activité est élaboré et mis en œuvre afin d'évaluer l'efficacité des stratégies existantes en la matière.
83. Les analyses d'impact sur l'activité (Business Impact Analyses, BIA) sont réalisées au moins une fois par an ou à la suite de changements organisationnels importants.
84. Un plan de gestion de crise est établi, comprenant des dispositions spécifiques pour la préparation à une pandémie. Ce plan garantit une réponse appropriée aux situations d'urgence, en mettant l'accent sur la protection des employés, des visiteurs, de l'environnement, des biens et le maintien des opérations commerciales essentielles.
85. Le système de gestion de la continuité de l'activité (Business Continuity Management System, BCMS) fait l'objet de tests d'efficacité annuels, avec des enregistrements détaillés pour chaque test.

<Fin du document>