**MODÈLE DE LISTE DE VÉRIFICATION POUR LES CONTRÔLES ISO 27001**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECTION/****CATÉGORIE** | **EXIGENCE/TÂCHE** | **ATTRIBUÉ À** | **EN CONFORMITÉ ?** | **DATE DE LA DERNIÈRE MISE À JOUR** |
| ***5. Politiques de sécurité de l’information*** |
| 5.1 | Des politiques de sécurité existent. |   |   |   |
| 5.2 | Toutes les politiques sont approuvées par la direction. |   |   |   |
| 5.3 | Preuve de conformité. |   |   |   |
| ***6. Organisation de la sécurité de l’information*** |
| 6,1 | Rôles et responsabilités définies. |   |  |  |
| 6.2 | Répartition des tâches définie. |   |  |  |
| 6.3 | L’organisme ou l’autorité de vérification est contactée pour la vérification de la conformité. |   |  |  |
| 6.4 | Des contacts sont établis avec des groupes d’intérêt particuliers concernant la conformité. |   |  |  |
| 6.5 | Preuve de la sécurité de l’information dans la gestion de projet. |   |  |  |
| 6.6 | Politique pour les appareils mobiles définie. |   |  |  |
| 6.7 | Politique pour le télétravail définie. |   |  |  |
| ***Sécurité des ressources humaines*** |
| 7.1 | Une politique pour le filtrage des employés avant leur embauche est définie. |   |  |  |
| 7.2 | Une politique pour la durée et les conditions d’embauche est définie. |   |  |  |
| 7.3 | Une politique sur les responsabilités de gestion est définie.  |   |  |  |
| 7.4 | Une politique pour la sensibilisation à la sécurité de l’information, l’éducation et la formation à la sécurité de l’information est définie. |   |  |  |
| 7.5 | Une politique pour les processus disciplinaires concernant la sécurité de l’information est définie. |   |  |  |
| 7.6 | Une politique pour le licenciement ou le changement d’emploi en matière de sécurité de l’information est définie. |   |  |  |
| ***8. Gestion des actifs*** |
| 8.1 | La liste des actifs est complète. |   |  |  |
| 8.2 | Propriété totale sur la liste des actifs. |   |  |  |
| 8.3 | Une politique sur l’« utilisation acceptable » des actifs est définie ? |   |  |  |
| 8.4 | Une politique de retour des actifs est définie. |   |  |  |
| 8.5 | Une politique pour la classification des informations est définie.  |   |  |  |
| 8.6 | Une politique pour l’étiquetage des informations est définie. |   |  |  |
| 8.7 | Une politique pour la gestion des actifs est définie. |   |  |  |
| 8.8 | Une politique sur la gestion des supports amovibles est définie. |   |  |  |
| 8.9 | Une politique pour l’élimination des supports est définie. |   |  |  |
| 8.10 | Une politique pour le transfert des supports physiques est définie. |   |  |  |
| ***9. Contrôle d’accès*** |
| 9.1 | Une politique pour l’enregistrement et la désinscription des ressources utilisateur est définie. |   |  |  |
| 9.2 | Une politique pour le provisionnement de l’accès des utilisateurs est définie. |   |  |  |
| 9.3 | Une politique pour la gestion des droits d’accès privilégiés est définie. |   |  |  |
| 9.4 | Une politique sur la gestion des identifiants d’authentification  des utilisateurs est définie. |   |  |  |
| 9.5 | Une politique pour l’examen des droits d’accès des utilisateurs est définie. |   |  |  |
| 9.6 | Une politique pour la suppression ou l’ajustement des droits d’accès est définie. |   |  |  |
| 9.7 | Une politique pour l’utilisation d’informations d’authentification secrètes est définie. |   |  |  |
| 9.8 | Une politique pour les restrictions d’accès à l’information est définie. |   |  |  |
| 9.9 | Une politique pour les procédures de connexion sécurisées est définie. |   |  |  |
| 9.10 | Une politique pour les systèmes de gestion des mots de passe est définie. |   |  |  |
| 9.11 | Une politique pour l’utilisation de programmes utilitaires privilégiés est définie. |   |  |  |
| 9.12 | Une politique pour le contrôle d’accès au code source du programme est définie. |   |  |  |
| ***10. Cryptographie*** |
| 10.1 | Une politique pour l’utilisation de contrôles cryptographiques est définie. |   |  |  |
| 10.2 | Une politique pour la gestion des clés est définie. |   |  |  |
| ***11. Sécurité physique et environnementale*** |
| 11.1 | Une politique pour le périmètre de sécurité physique est définie. |   |  |  |
| 11.2 | Une politique pour les contrôles d’accès physique est définie. |   |  |  |
| 11.3 | Une politique pour la sécurisation des bureaux, des salles et des installations est définie. |   |  |  |
| 11.4 | Une politique pour la protection contre les menaces externes et environnementales est définie. |   |  |  |
| 11.5 | Une politique pour travailler dans des zones sécurisées est définie. |   |  |  |
| 11.6 | Une politique pour les zones de livraison et de chargement est définie. |   |  |  |
| 11.7 | Une politique pour l’implantation et la protection des équipements est définie. |   |  |  |
| 11.8 | Une politique pour la prise en charge des services publics est définie. |   |  |  |
| 11.9 | Une politique pour la sécurité du câblage est définie. |   |  |  |
| 11.10 | Une politique pour la maintenance de l’équipement est définie. |   |  |  |
| 11.11 | Une politique pour l’élimination des actifs est définie. |   |  |  |
| 11.12 | Une politique pour la sécurité de l’équipement et des actifs hors des locaux est définie. |   |  |  |
| 11.13 | Élimination ou réutilisation sécurisées de l’équipement. |   |  |  |
| 11.14 | Une politique pour l’équipement utilisateur laissé sans surveillance est définie. |   |  |  |
| 11.15 | Une politique pour un bureau et un écran inutilisés est définie. |   |  |  |
| ***12. Sécurité liée à l’exploitation*** |
| 12.1 | Une politique pour les procédures d’exploitation documentées est définie. |   |  |  |
| 12.2 | Une politique sur la gestion du changement est définie. |   |  |  |
| 12.3 | Une politique sur la gestion de la capacité est définie. |   |  |  |
| 12.4 | Une politique pour la séparation des environnements de développement, de test et d’exploitation est définie. |   |  |  |
| 12.5 | Une politique pour les contrôles contre les logiciels malveillants est définie. |   |  |  |
| 12.6 | Une politique pour la sauvegarde des systèmes est définie. |   |  |  |
| 12.7 | Une politique pour la sauvegarde des informations est définie. |   |  |  |
| 12.8 | Une politique pour la journalisation des événements est définie. |   |  |  |
| 12.9 | Une politique pour la protection des des informations de journalisation est définie. |   |  |  |
| 12.10 | Une politique pour les journaux des administrateurs et des opérateurs est définie. |   |  |  |
| 12.11 | Une politique pour la synchronisation des horloges est définie. |   |  |  |
| 12.12 | Une politique pour l’installation de logiciels sur les systèmes opérationnels est définie. |   |  |  |
| 12.13 | Une politique pour la gestion des vulnérabilités techniques est définie. |   |  |  |
| 12.14 | Une politique sur les restrictions à l’installation de logiciels est définie. |   |  |  |
| 12.15 | Une politique pour le contrôle de l’audit des systèmes d’information est définie. |   |  |  |
| ***13. Sécurité des communications*** |
| 13.1 | Une politique pour les contrôles réseau est définie. |   |  |  |
| 13.2 | Une politique pour la sécurité des services réseau est définie. |   |  |  |
| 13.3 | Une politique pour la ségrégation dans les réseaux est définie. |   |  |  |
| 13.4 | Une politique pour les politiques et procédures de transfert d’informations est définie. |   |  |  |
| 13.5 | Une politique pour les accords sur le transfert d’informations est définie. |   |  |  |
| 13.6 | Une politique pour la messagerie électronique est définie. |   |  |  |
| 13.7 | Une politique pour les accords de confidentialité ou de non-divulgation est définie. |   |  |  |
| 13.8 | Une politique pour l’acquisition, le développement et la maintenance des systèmes est définie. |   |  |  |
| ***14. Acquisition, développement et maintenance des systèmes*** |
| 14.1 | Une politique définie pour l’analyse et la spécification des exigences en matière de sécurité des informations est définie. |   |  |  |
| 14.2 | Une politique pour la sécurisation des services d’application sur les réseaux publics est définie. |   |  |  |
| 14.3 | Une politique pour la protection des transactions de services d’application est définie. |   |  |  |
| ***15. Relations avec les fournisseurs*** |
| 15.1 | Une politique sur les relations avec les fournisseurs est définie. |   |  |  |
| ***16. Gestion des incidents liés à la sécurité de l’information*** |
| 16.1 | Une politique sur la gestion de la sécurité de l’information est définie. |   |  |  |
| ***17. Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité*** |
| 17.1 | Une politique pour les licenciements est définie. |   |  |  |
| ***18. Conformité*** |
| 18.1 | Une politique pour l’identification des lois applicables et des exigences contractuelles est définie. |   |  |  |
| 18.2 | Une politique pour les droits de propriété intellectuelle est définie. |   |  |  |
| 18.3 | Une politique pour la protection des enregistrements est définie. |   |  |  |
| 18.4 | Une politique pour la vie privée et la protection des informations personnellement identifiables est définie. |   |  |  |
| 18.5 | Une politique pour la régulation du contrôle cryptographique est définie. |   |  |  |
| 18.6 | Une politique pour la conformité aux politiques et normes de sécurité est définie. |   |  |  |
| 18.7 | Une politique pour l’examen de la conformité technique est définie. |   |  |  |

**EXCLUSION DE RESPONSABILITÉ**

Tous les articles, modèles ou informations proposés par Smartsheet sur le site web sont fournis à titre de référence uniquement. Bien que nous nous efforcions de maintenir les informations à jour et exactes, nous ne faisons aucune déclaration, ni n’offrons aucune garantie, de quelque nature que ce soit, expresse ou implicite, quant à l’exhaustivité, l’exactitude, la fiabilité, la pertinence ou la disponibilité du site web, ou des informations, articles, modèles ou graphiques liés, contenus sur le site. Toute la confiance que vous accordez à ces informations relève de votre propre responsabilité, à vos propres risques.

Ce modèle n’est fourni qu’à titre d’exemple. Ce modèle ne saurait en aucun cas être considéré comme des conseils juridiques ou de conformité. Les utilisateurs de ce modèle doivent déterminer les informations nécessaires dont ils ont besoin pour atteindre leurs objectifs.