**MODÈLE LISTE DE CONTRÔLE DES DIRECTIVES
ISO 27002 POUR LA SÉCURITÉ DE L’INFORMATION**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **NUMÉRO CONTRÔLE ISO 27001** | **RANG** | **PRIORITÉ** | **RESPONSABLE** | **DATE ATTRIBUÉE** | **DATE D’ÉCHÉANCE** | **EN CONFORMITÉ ?** | **STATUT** | **NOTES** |
| **5. Gestion des politiques de sécurité** |
| 5.1 - La direction a fourni une orientation et un soutien en matière de conformité ?   |  |   |  |   |   |   |  |   |
| **6. Gestion de la sécurité de l’entreprise** |
| 6.1 - Un groupe de travail sur la sécurité interne de l’information a-t-il été créé ?  |   |   |   |   |   |   |  |   |
| 6.2 - Mesures en place pour protéger les appareils mobiles et le réseau de l’organisation ?   |   |   |   |   |   |   |  |   |
| **7. Gestion de la sécurité du personnel** |
| 7.1 - Politique établie pour vérifier la sécurité avant l’emploi ? |   |   |   |   |   |   |  |   |
| 7.2 - Politique établie pour la sécurité pendant la durée de l’emploi ?  |   |   |   |   |   |   |  |   |
| 7.3 - Politique établie pour la sécurité lors de la résiliation ?  |   |   |   |   |   |   |  |   |
| **8. Gestion des ressources organisationnelles** |
| 8.1 - Politique établie pour les actifs de l’entreprise ?  |   |   |   |   |   |   |  |   |
| 8.2 - Politique établie pour la méthode de classification des informations ?  |   |   |   |   |   |   |  |   |
| 8.3 - Politique établie pour le contrôle des supports physiques ?  |   |   |   |   |   |   |  |   |
| **9. Gestion de l’accès aux informations** |
| 9.1 - Politique établie pour la gestion de l’accès à l’information pour les exigences de l’entreprise ?  |   |   |   |   |   |   |  |   |
| 9.2 - Politique établie pour la gestion des droits d’accès de tous les utilisateurs ?  |   |   |   |   |   |   |  |   |
| 9.3 - Politique établie pour l’authentification des utilisateurs ?  |   |   |   |   |   |   |  |   |
| 9.4 - Politique établie pour contrôler l’accès aux systèmes ?  |   |   |   |   |   |   |  |   |
| **10. Gestion des politiques de cryptographie** |
| 10.1 - Politique établie pour le contrôle de l’utilisation des contrôles et clés cryptographiques ?  |   |   |   |   |   |   |  |   |
| **11. Gestion de la sécurité physique** |
| 11.1 - Politique établie pour la gestion de la sécurité physique ?   |   |   |   |   |   |   |  |   |
| 11.2 - Politique établie pour protéger l’équipement de l’organisation ?  |   |   |   |   |   |   |  |   |
| **12. Gestion opérationnelle de la sécurité** |
| 12.1 - Politique établie pour les procédures et responsabilités de gestion opérationnelle de la sécurité ?  |   |   |   |   |   |   |  |   |
| 12.2 - Politique établie pour protéger l’organisation de logiciels malveillants ?   |   |   |   |   |   |   |  |   |
| 12.3 - Politique établie pour créer régulièrement des copies de sauvegarde ?  |   |   |   |   |   |   |  |   |
| 12.4 - Politique établie pour l’utilisation des journaux pour enregistrer les événements de sécurité ?  |   |   |   |   |   |   |  |   |
| 12.5 - Politique établie pour contrôler les logiciels opérationnels de l’organisation ?  |   |   |   |   |   |   |  |   |
| 12.6 - Politique établie pour traiter les vulnérabilités techniques de l’organisation ?  |   |   |   |   |   |   |  |   |
| 12.7 - Politique en place pour réduire l’impact des activités de vérification ?  |   |   |   |   |   |   |  |   |
| **13. Gestion de la sécurité des réseaux** |
| 13.1 - Politique établie pour protéger les réseaux et les installations ?  |   |   |   |   |   |   |  |   |
| 13.2 - Politique établie pour protéger les transferts de renseignements ?  |   |   |   |   |   |   |  |   |
| **14. Gestion de la sécurité du système** |
| 14.1 - Politique établie pour assurer la sécurité des parties inhérentes des systèmes d’information ?  |   |   |   |   |   |   |  |   |
| 14.2 - Politique établie pour protéger et contrôler les activités de développement de système ?  |   |   |   |   |   |   |  |   |
| 14.3 - Politique établie pour la sauvegarde des données utilisées à des fins de test du système ?   |   |   |   |   |   |   |  |   |
| **15. Gestion de la relation avec les fournisseurs** |
| 15.1 - Politique établie pour conclure des accords de sécurité avec les fournisseurs ?  |   |   |   |   |   |   |  |   |
| 15.2 - Politique établie pour gérer la sécurité et les livraisons de services des fournisseurs ?  |   |   |   |   |   |   |  |   |
| **16. Gestion des incidents liés à la sécurité** |
| 16.1 - Politique établie pour identifier et répondre aux incidents de sécurité de l’information ?  |   |   |   |   |   |   |  |   |
| **17. Gestion de la continuité de la sécurité** |
| 17.1 - Politique établie pour la mise en place de contrôles de la continuité de la sécurité de l’information ?  |   |   |   |   |   |   |  |   |
| 17.2 - Politique établie pour les constructions de redondance pour les installations de traitement d’informations ?  |   |   |   |   |   |   |  |   |
| **18. Gestion de la conformité en matière de sécurité** |
| 18.1 - Politique établie pour la conformité aux exigences légales en matière de sécurité ?  |   |   |   |   |   |   |  |   |
| 18.2 - Politique établie pour l’exécution des examens de conformité en matière de sécurité ?  |   |   |   |   |   |   |  |   |

**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.