Tableau de traitement des risques implémenté du [date] au [date]

Actifs / Menaces / Vulnérabilités						*Valeurs avant le traitement*		
N.	**Nom de l'actif**	**Propriétaire de l'actif**	**Menace**	**Vulnérabilité**	**Propriétaire du risque**	**Impact**	**Vraisemblance**	**Risque**
1	*logiciel d'application*	*responsable informatique*	*erreurs d'application*	*absence de contrôle des données d'entrée et de sortie*	*responsable informatique*	*3*	*3*	*3*
2	*moyens de communication*	*responsable informatique*	*rupture des relations contractuelles*	*absence ou mauvaise application de l'audit interne*	*responsable informatique*	*3*	*3*	*3*
3	*logiciel d'application*	*responsable informatique*	*erreurs d'application*	*connexions de réseau public non protégées*	*responsable informatique*	*3*	*3*	*3*
4	*bureaux*	*responsable des installations*	*interruption de l'alimentation électrique*	*site sensible aux catastrophes naturelles*	*responsable des installations*	*3*	*3*	*3*
5	*moyens de communication*	*responsable informatique*	*défaillance des équipements*	*site sensible aux fuites d'eau*	*responsable informatique*	*3*	*3*	*3*

Traitement des Risques		*Valeurs après le traitement*		
Sélection des options	[illegible]	[illegible]	[illegible]	**Risque**
2. Transfert des risques à un tiers	[illegible]	[illegible]	[illegible]	*2*
1. Sélection des mesures	[illegible]	[illegible]	[illegible]	*2*
2. Transfert des risques à un tiers	[illegible]	[illegible]	[illegible]	*2*
1. Sélection des mesures	[illegible]	[illegible]	[illegible]	*2*
1. Sélection des mesures	[illegible]	[illegible]	[illegible]	*1*
				0
				0
				0
				0
				0
				0
				0
				0
				0

Options de traitement des risques

1. Sélection des mesures
2. Transfert des risques à un tiers
3. Prévention des risques
4. Acceptation des risques

Mesures conformément à l'Annexe A de la norme ISO/IEC 27001

A.5.1 Politiques de sécurité de l'information
A.5.2 Fonctions et responsabilités liées à la sécurité de l'information
A.5.3 Cloisonnement des tâches
A.5.4 Responsabilités de la direction
A.5.5 Relations avec les autorités
A.5.6 Relations avec des groupes de travail spécialisés
A.5.7 Renseignements sur les menaces
A.5.8 Sécurité de l'information dans la gestion de projet
A.5.9 Inventaire des informations et d'autres actifs associés
A.5.10 Utilisation acceptable des informations et d'autres actifs associés
A.5.11 Restitution des actifs
A.5.12 Classification des informations
A.5.13 Marquage des informations
A.5.14 Transfert des informations
A.5.15 Contrôle d'accès
A.5.16 Gestion de l'identification
A.5.17 Informations d'authentification
A.5.18 Droits d'accès
A.5.19 Sécurité de l'information dans les relations avec les fournisseurs
A.5.20 Traitement de la sécurité de l'information dans les accords conclus avec les fournisseurs
A.5.21 Gestion de la sécurité de l'information dans les chaînes d'approvisionnement des TIC
A.5.22 Gestion du contrôle, de l'examen et des modifications des services des fournisseurs
A.5.23 Sécurité de l'information pour l'utilisation des services cloud
A.5.24 Planification et élaboration de la gestion des incidents liés à la sécurité de l'information
A.5.25 Evaluation des évènements liés à la sécurité de l'information et prise de décision
A.5.26 Réponses aux incidents liés à la sécurité de l'information
A.5.27 Tirer des enseignements des incidents liés à la sécurité de l'information
A.5.28 Collecte de preuves
A.5.29 Sécurité de l'information pendant les perturbations
A.5.30 Préparation des TIC à la continuité des activités
A.5.31 Exigences légales, réglementaires et contractuelles
A.5.32 Droits de propriété intellectuelle
A.5.33 Protection des enregistrements
A.5.34 Protection de la vie privée et des données à caractère personnel
A.5.35 Examen indépendant de la sécurité de l'information
A.5.36 Conformité avec les politiques, les règles et les normes de sécurité de l'information
A.5.37 Procédures d'exploitation consignées
A.6.1 Evaluation préalable
A.6.2 Termes et conditions d'embauche
A.6.3 Sensibilisation et formation à la sécurité de l'information
A.6.4 Procédure disciplinaire
A.6.5 Responsabilités après la résiliation ou la modification du contrat de travail
A.6.6 Accords de confidentialité ou de non-divulgation
A.6.7 Travail à distance
A.6.8 Signalement des événements liés à la sécurité de l'information
A.7.1 Périmètre de sécurité physique
A.7.2 Accueil physique
A.7.3 Sécurisation des bureaux, des salles et des équipements

A.7.4 Contrôle de sécurité physique
A.7.5 Protection contre les menaces physiques et environnementales
A.7.6 Travail dans les zones sécurisées
A.7.7 Bureau propre et écran vide
A.7.8 Emplacement et protection des équipements
A.7.9 Sécurité des actifs hors des locaux
A.7.10 Supports de stockage
A.7.11 Services généraux
A.7.12 Sécurité du câblage
A.7.13 Maintenance des équipements
A.7.14 Elimination ou réutilisation sécurisée des équipements
A.8.1 Périphériques de point d'extrémité utilisateur
A.8.2 Droits d'accès à privilèges
A.8.3 Restriction d'accès à l'information
A.8.4 Accès au code source
A.8.5 Authentification sécurisée
A.8.6 Gestion des capacités
A.8.7 Protection contre les logiciels malveillants
A.8.8 Gestion des vulnérabilités techniques
A.8.9 Gestion des configurations
A.8.10 Suppression des informations
A.8.11 Masquage des données
A.8.12 Prévention aux fuites de données
A.8.13 Sauvegarde des informations
A.8.14 Redondance des moyens de traitement de l'information
A.8.15 Connexion
A.8.16 Contrôle des activités
A.8.17 Synchronisation des horloges
A.8.18 Utilisation de programmes utilitaires à privilèges
A.8.19 Installation de logiciels sur des systèmes en exploitation
A.8.20 Sécurité des réseaux
A.8.21 Sécurité des services de réseau
A.8.22 Cloisonnement des réseaux
A.8.23 Filtrage Web
A.8.24 Utilisation des mesures cryptographiques
A.8.25 Cycle de vie du développement sécurisé
A.8.26 Exigences de sécurité des applications
A.8.27 Architecture du système sécurisé et principes d'ingénierie
A.8.28 Codage sécurisé
A.8.29 Tests de sécurité en cours de développement et d'acceptation
A.8.30 Développement externalisé
A.8.31 Séparation des environnements de développement, de test et d'exploitation
A.8.32 Gestion du changement
A.8.33 Informations de test
A.8.34 Protection des systèmes d'information au cours des tests d'audit