Iso 27001 Report

Question	Answer	Conclusion	Recommendation
Existe-t-il un comité de sécurité du système d'information ?	non	Absence de comité de sécurité du SI.	Il convient de désigner un comité ou une structure regroupant l'ensemble des responsables de sécurité.
Existe-il un RSSI dans la société, avec une fiche de poste, ainsi qu'une délégation formelle mentionnant ses attributions et ses moyens d'actions ?	oui	------	------
Les informations confidentielles à protéger sont elles identifiées ?	non	Absence de L'identification des informations confidentielles	Il est conseillé d'identifié les informations confidentielles
* La société a-t-elle identifié les risques liés aux types d'accès possible pour les tiers externes	oui	------	------
Existe-t-il un propriétaire pour chaque actif ?	non	Manque d'un responsable pour chaque ressource.	Définir pour chaque actif un propriétaire qui assume la responsabilité du développement, de la maintenance, de l'exploitation, de l'utilisation et de la sécurité de cet actif.
Les actifs sont –elles classifiés en termes de sensibilités de criticité et de valeurs ?	oui	------	------
Existe-il des règles d'utilisation des biens et des services d'information ?	non	L'inexistence des règles d'utilisation des biens et des services d'information	Les actifs doivent être classifiées selon leur importance basée sur les 3 axes : besoin en terme de disponibilité, confidentialité et intégrité
Toutes « les fiche poste » contiennent-elles des détails sur les rôles et responsabilités des acteurs en matière de sécurité ?	oui	------	------

Les employés suivent-t-ils une formation et une sensibilisation régulière aux risque et mesure de protection relatifs au traitement de l'information ?	non	Absence d'un programme de sensibilisation du personnel aux risques d'accident, d'erreur et de malveillance relatifs au traitement de l'information.	Il est recommandé d'améliorer le programme de sensibilisation pour tout le personnel de la société
Les employés suivent-t-ils une formation et une sensibilisation régulière aux risque et mesure de protection relatifs au traitement de l'information ?	oui	------	------
La société a-t-elle établi un périmètre de sécurité et déterminé clairement des zones de sécurité en fonction de la sensibilisation des informations et des infrastructures ?	non	Périmètre de sécurité n'est pas définie : absence des zones de sécurité.	Il est recommandé d'établir un périmètre de sécurité pour la société selon la sensibilité des informations et des infrastructures. Ainsi il est recommandé de définir des zones de sécurité présentant des besoins différents de protection en fonction des risques identifiés
Existe-t-il une documentation liée à la sécurité physique et environnementale ?	oui	------	------
Les postes informatiques et réseaux sensibles sont-ils secourus en cas de rupture de l'alimentation électrique normale ?	non	Pas de test de vérification en cas de coupure de courant ou d'incendie. Absence de protection de la salle serveur.	Il est recommandé que la direction de l'entreprise prend décision de changer l'emplacement de la salle serveur dans des zones sécurisées et surtout l'isoler de telle façon réduire la possibilité d'intrusions interdites à cette salle sensible
Des procédures d'exploitation des systèmes d'information en production sont-elles définies ?	oui	------	------
Y a-t-il un responsable pour la gestion de communication et d'exploitation.	oui	------	------
Les processus d'alerte en cas d'infection virale et de réparation sont- ils formalisés et mis en œuvre ?	oui	------	------
L'accès au système est il			

contrôlé par un dispositif d'identification et d'authentification ?	oui	------	------
Des mesures sont-elles été prises pour renforcer l'authentification lors des connexions distantes (utilisation de tokens, de techniques cryptographique…) ?	non	Il n'existe pas des bonnes pratiques concernant la protection des mots de passe.	Il est recommandé d'utiliser des mesures pour renforcer l'authentification lors des connexions distantes.
L'authentification de l'utilisateur est–elle obligatoire pour toute connexion à un terminal ou à un PC de la société ?	oui	------	------
* Existe-t-il des procédures de contrôle pour les logiciels développés en sous-traitance ?	non	Absence des procédures de contrôle pour les logiciels développés en sous-traitance.	Mettre en place des procédures pour contrôler l'installation du logiciel sur les systèmes d' exploitation.
Existe-t-il un comité de sécurité du système d'information ?	non	Absence de comité de sécurité du SI.	Il convient de désigner un comité ou une structure regroupant l'ensemble des responsables de sécurité.
Existe-il un RSSI dans la société, avec une fiche de poste, ainsi qu'une délégation formelle mentionnant ses attributions et ses moyens d'actions ?	oui	------	------
Les informations confidentielles à protéger sont elles identifiées ?	non	Absence de L'identification des informations confidentielles	Il est conseillé d'identifié les informations confidentielles
* La société a-t-elle identifié les risques liés aux types d'accès possible pour les tiers externes	oui	------	------
Existe-t-il un propriétaire pour chaque actif ?	non	Manque d'un responsable pour chaque ressource.	Définir pour chaque actif un propriétaire qui assume la responsabilité du développement, de la maintenance, de l'exploitation, de l'utilisation et de la sécurité de cet actif.
Les actifs sont –elles classifiés en termes de	oui	------	------

sensibilités de criticité et de valeurs ?			
Existe-il des règles d'utilisation des biens et des services d'information ?	non	L'inexistence des règles d'utilisation des biens et des services d'information	Les actifs doivent être classifiées selon leur importance basée sur les 3 axes : besoin en terme de disponibilité, confidentialité et intégrité
Toutes « les fiche poste » contiennent-elles des détails sur les rôles et responsabilités des acteurs en matière de sécurité ?	oui	------	------
Toutes « les fiche poste » contiennent-elles des détails sur les rôles et responsabilités des acteurs en matière de sécurité ?	non	Absence d'un document précisant les rôles et responsabilités du personnel.	Etablir une clause dans les contrats d'embauche ou dans le règlement intérieur, précisant l'obligation de respecter l'ensemble des règles de sécurité
Les employés suivent-t-ils une formation et une sensibilisation régulière aux risque et mesure de protection relatifs au traitement de l'information ?	oui	------	------
Les employés suivent-t-ils une formation et une sensibilisation régulière aux risque et mesure de protection relatifs au traitement de l'information ?	non	Absence d'un programme de sensibilisation du personnel aux risques d'accident, d'erreur et de malveillance relatifs au traitement de l'information.	Il est recommandé d'améliorer le programme de sensibilisation pour tout le personnel de la société
La société a-t-elle établi un périmètre de sécurité et déterminé clairement des zones de sécurité en fonction de la sensibilisation des informations et des infrastructures ?	oui	------	------
Existe-t-il une documentation liée à la sécurité physique et environnementale ?	non	Absence d'un document lié à la sécurité physique et environnementale.	Il conseiller de mettre en œuvre un document lié à la sécurité physique et environnemental
Les postes informatiques et			

réseaux sensibles sont-ils secourus en cas de rupture de l'alimentation électrique normale ?	oui	------	------
Des procédures d'exploitation des systèmes d'information en production sont-elles définies ?	non	Absence des procédures d'exploitation du système informatique en production.	Établir des procédures opérationnelles d'exploitation qui doivent être documentées, maintenues à jour, rendues disponibles à toute personne en ayant besoin et approuvées par les responsables concernés.
Y a-t-il un responsable pour la gestion de communication et d'exploitation.	oui	------	------
Les processus d'alerte en cas d'infection virale et de réparation sont- ils formalisés et mis en œuvre ?	non	Manque des processus d'alerte en cas d'infection virale et de réparation.	Définir une politique afin de lutter contre les risques d'attaque par des codes malveillants (virus, chevaux de Troie, vers,…).
L'accès au système est il contrôlé par un dispositif d'identification et d'authentification ?	oui	------	------
Des mesures sont-elles été prises pour renforcer l'authentification lors des connexions distantes (utilisation de tokens, de techniques cryptographique…) ?	non	Il n'existe pas des bonnes pratiques concernant la protection des mots de passe.	Il est recommandé d'utiliser des mesures pour renforcer l'authentification lors des connexions distantes.
L'authentification de l'utilisateur est–elle obligatoire pour toute connexion à un terminal ou à un PC de la société ?	oui	------	------
* Existe-t-il des procédures de contrôle pour les logiciels développés en sous-traitance ?	non	Absence des procédures de contrôle pour les logiciels développés en sous-traitance.	Mettre en place des procédures pour contrôler l'installation du logiciel sur les systèmes d' exploitation.