Charte d'utilisation du SI pour les utilisateurs non administrateurs

En tant qu'utilisateur du SI, je m'engage à :

1. Ne pas utiliser de logiciels ou périphériques non autorisés.
2. Protéger mes identifiants et mots de passe.
3. Verrouiller mon poste de travail lorsque je m'absente.
4. Ne pas stocker de données sensibles sur des supports amovibles non sécurisés.
5. Ne pas installer de logiciels sans l'autorisation de la DSI.
6. Utiliser les ressources informatiques uniquement à des fins professionnelles.
7. Signaler immédiatement toute anomalie ou incident de sécurité.
8. Respecter la politique de sécurité de l'entreprise lors de l'utilisation d'Internet et de la messagerie.
9. Ne pas divulguer d'informations confidentielles de l'entreprise.
10. Respecter les règles de bon usage et de sécurité des systèmes d'information.

Tableau récapitulatif pour les utilisateurs non administrateurs

Règle	Domaine	Budget (1-5)	Contraintes	Avantages	Contrôle
1	Logiciels/ Dispositifs	2	Restriction d'usage	Protection contre malwares	Audit régulier
2	Sécurité des accès	1	Gestion des mots de passe	Réduction du risque de piratage	Vérification des pratiques
3	Postes de travail	1	Discipline personnelle	Prévention de l'accès autorisez	Contrôles inopinés
4	Gestion des données	2	Restriction des support	Protection des données	Audit de sécurité
5	Installation logiciel	2	Validation par DSI	Prévention des risque de sécurité	Suivit des installation
6	Utilisation des ressources	1	Respect des règles	Bonne gouvernance de l'IT	Surveillance de l'usage
7	Gestion des incident	1	Communication rapide	Réaction et résolution rapide	Suivi des incidents
8	Utilisation interne/email	2	Respect des directive	Réduction des risque cyber	Analyse de trafics
9	Confidentialité	3	Non-divulgation	Protection des actifs	Contrôle d'accès
10	Bon usage	1	Adhésion au politique	Cohérence et sécurité	Evaluation périodiques

Charte d'utilisation du SI pour les administrateurs du SI

En tant qu'administrateur du SI, je m'engage à :

1. Appliquer le principe de moindre privilège.
2. Maintenir une documentation à jour de toutes les configurations et procédures.
3. Réaliser des audits de sécurité régulièrement.
4. Appliquer les mises à jour de sécurité sans retard.
5. Surveiller continuellement les systèmes pour détecter toute activité anormale.
6. Sécuriser physiquement et logiquement les accès aux serveurs et autres composants critiques.
7. Former et sensibiliser les utilisateurs aux bonnes pratiques de sécurité
8. Assurer un chiffrement efficace des données sensibles.
9. Établir et tester régulièrement les procédures de sauvegarde et de restauration.
10. Utiliser des comptes d’administration uniquement pour les tâches nécessitant des droits élevés.

Tableau récapitulatif pour les administrateurs du SI :

Règle	**Domaine**	**Budget**(1-5)	**Contrainte**	**Avantages**	**Contrôle**
1	Droit d’accès	2	Limitation des droits	Réduction des risques de sécurité	Audits des droits
2	Documentation	3	Mise à jour constant	Fiabilité et référence claire	Vérification documentaire
3	Audits de sécurité	4	Régularité des audits	Prévention des failles	Rapports d'audit
4	Mises à jour	3	Application rapide	Diminution des vulnérabilités	Suivi des versions
5	Surveillance	4	Monitoring continu	Détection rapide des incidents	Révisions des journaux
6	Sécurité physique/logique	4	Mesures strictes	Protection contre accès non autorisés	Inspections de sécurité
7	Formation des utilisateurs	3	Programmation régulière	Amélioration de la culture de sécurité	Évaluation de la formation
8	Chiffrement	4	Application systématique	Confidentialité des données	Audits de chiffrement
9	Sauvegardes	5	Protocoles stricts	Récupération des données	Tests de restauration
10	Comptes d’administration	2	Usage restreint	Minimisation des risques	Vérification de l'usage