hamilton apps
by SAFEWARE

Hamilton Apps Politique de sécurité

Hamilton Smart Workplace Management Solutions

T 33 (0) 1 55 34 95 55
E contact@safeware.fr

A 32 Bis Boulevard Haussmann
75009 Paris, France

W www.hamiltonapps.com

Table des matières

Introduction 4
1. Objectif 4
2. Cible 5
3. Termes et notions 5

Définition de politique 5
1. Périmétre 5
2. Date d'application 5
3. Disposition transitoire 6
4. Formation du personnel à cette politique 6
5. Conduite et évolution des politiques 6
6. Mise en œuvre de la politique par les équipes informatiques et de développement 7
7. Mise en place de procédures au sein de l'entreprise 7
8. Suivi de la mise en œuvre de la politique 8
9. Gestion des incidents et gestion des crises 8

Objectifs et règles 9
1. Organisation de la sécurité des systèmes d'information 9
2. Ressources humaines 10
   2.1 Utilisateurs 10
   2.2 Postes de responsabilité du personnel 10
   2.3 Personnel non-permanent 10
3. Maintenir les exigences de sécurité 11
   3.1 Intégration des besoins de sécurité dans les projets 11
   3.2 Intégration continue de la politique de sécurité 11
   3.3 Table de surveillance 11
4. Utiliser des produits de qualité et certifiés 11
5. Clauses contractuelles de sécurité 11
   5.1 Clauses contractuelles de sécurité 11
   5.2 Suivi et inspection des provisions 12
   5.3 Analyse de risque 12
   5.4 Hébergement de données 12
6. Accès spécifiques 12
7. Sécurisation des infrastructures 12
   7.1 Intégrité physique de l'infrastructure 12
   7.2 Application du concept de défense en profondeur 13
   7.3 Infrastructure de sauvegarde et de stockage 13
8. Protection des données sensibles 13

9. Surveillance et configuration des ressources informatiques 13
9.1 Suivi des manipulations du système 13
9.2 Configuration des ressources informatiques 13
9.3 Documentation de configuration 13
10. Contrôle d'accès et autorisations 13
10.1 Contrôle d'accès logique 14
10.2 Processus d'authentification 14
10.3 Gestion des identifiants et authentificateurs 14
10.4 Gestion des authentificateurs administratifs 14
11. Administration et protection des informations 15
11.1 Administration des systèmes 15
11.2 Contrôle à distance 15
11.3 Administration des domaines 15
11.4 Protection contre les programmes malveillants 16

Introduction

1. Objectif

La politique de sécurité de Hamilton Apps contribue à:

- Assurer la continuité de l'exécution de toutes les solutions Hamilton Apps, que ce soit sur site ou en offre de « Software as a Service ».
- Prévenir les fuites de données et protéger l'accès aux données sensibles et personnelles.
- Renforcer la confiance des entreprises extérieures dans notre capacité à nous adapter aux menaces de sécurité.

Le présent document définit les mesures de sécurité qui concernent les technologies de l'information et les systèmes à l'intérieur des applications Hamilton Apps. Il suit 10 principes stratégiques, comme suit:

- P1. En cas de besoin, l'entreprise demande des services à des prestataires externes de confiance et certifiés.
- P2. Tous les systèmes d'information doivent recevoir des analyses de risques permettant des mesures de sécurité préventives et des actions de réponse aux dernières menaces de sécurité. Ces analyses font partie d'un protocole d'amélioration continue de la sécurité de tous les systèmes et doivent couvrir toute leur durée de vie.
- P3. Tous les moyens humains, techniques et financiers pour assurer la sécurité des systèmes d'information doivent être planifiés, quantifiés et identifiés.
- P4. Tous les employés doivent utiliser des méthodes d'authentification fortes pour garantir un accès contrôlé et restrictif aux systèmes d'information et aux données.
- P5. Toutes les opérations administratives et de gestion exploitées sur des systèmes d'information doivent être enregistrées et traçables.
- P6. La protection des systèmes d'information nécessite l'application stricte des mesures telles qu'elles sont décrites dans le présent document.
- P7. Chaque employé, en tant qu'utilisateur d'un système d'informations, doit être informé de ses autorisations et interdictions d'accès aux données et doit être sensibilisé à la cyber-sécurité. Toutes les mesures techniques de sécurité doivent être connues de tous à l'intérieur de l'entreprise.
- P8. Tous les administrateurs d'un système d'informations doivent appliquer strictement, après avoir reçu une formation spécialisée, des règles élémentaires de manipulation de données confidentielles.
- P9. Tous les produits et services acquis par l'entreprise doivent être évalués et certifiés par le responsable de l'information afin d'assurer la sécurité de tous les systèmes d'information de l'entreprise.
- P10. Toutes les données considérées comme sensibles, en raison de leurs besoins de confidentialité, d'intégrité ou de disponibilité, doivent être hébergées à l'intérieur de l'Union européenne et de préférence à l'intérieur du territoire national des clients.

2. Cible

Le directeur de l'information (CIO) d'Hamilton Apps, les équipes QA et IT et les fournisseurs tiers sont directement concernés par la politique déclarée dans ce document.

Les directeurs informatiques et les équipes informatiques des clients et prospects de Hamilton Apps sont vivement invités à se prévaloir de cette politique.

3. Termes et notions

Logiciel sur site (On-prem) : logiciel installé et exécuté sur des ordinateurs dans les locaux de la personne ou de l'organisation utilisant le logiciel, plutôt que dans une installation distante telle qu'une batterie de serveurs ou un cloud.

Logiciel en tant que service (SaaS) : modèle de licence et de livraison de logiciels dans lequel le logiciel est concédé sous licence et hébergé de manière centralisée.

Systèmes d'information (SI) : système composé d'ordinateurs qui traitent ou interprètent les informations, généralement en exécutant des bases de données informatisées.

Définition de la politique

1. Périmètre

Cette politique de sécurité s'applique à tous les systèmes d'information (SI) de l'entreprise :

- Systèmes et outils internes.
- Infrastructure SaaS et logiciel de Hamilton Apps.
- Logiciel sur site (l'infrastructure est la responsabilité du client).

Cette politique concerne toutes les sociétés ou personnes physiques faisant partie de ces SI, indépendamment de leur statut interne ou externe (prestataires tiers), et leurs salariés.

Les mesures et processus définis à l'intérieur du présent document établissent une base minimale qui peut être largement appliquée. Pour certaines applications, cette base ne doit pas être considérée comme suffisante, mais plutôt comme une condition préalable à une nouvelle extension des mesures de sécurité.

2. Date d'application

Cette politique entre en vigueur le jour de sa publication.

3. Disposition transitoire

La politique d'application doit être mise en œuvre selon les règles suivantes :

- Les solutions Software as a Service (SaaS) doivent être conformes lors du lancement de la phase de pré-production.
- Les solutions sur site (On-Prem) doivent être conformes lors du lancement de la phase de production.
- Les solutions sur site d'anciens contrats doivent être conformes lors de la mise à jour vers une version d'un produit émise après la publication de cette politique.
- Tout développement tiers doit être conforme à cette politique et validé par le directeur de l'information de Hamilton Apps, avant d'être intégré dans les solutions de pré-production et de production.

4. Formation du personnel à cette politique

Hamilton Apps formera son personnel à la nouvelle politique. Ils recevront des informations sur la cyber-sécurité, la sécurité informatique (sécurité informatique) et recevront des instructions afin de respecter les règles de sécurité.

Le personnel chargé de l'application des mesures de sécurité informatique reçoit une formation appropriée correspondant à ses tâches et à ses besoins.

5. Conduite et évolution des politiques

La politique actuelle évoluera avec le temps. Il peut être revisité notamment afin de prendre en compte :

- Évolution des menaces et retours d'expérience sur la gestion des incidents.
- Résultats des analyses de risques et mesures prises après les inspections.
- Évolution du droit et de la technologie de la protection des données.

Les évolutions susmentionnées de la politique seront menées par le directeur de l'information (CIO) et l'équipe de sécurité informatique.

Ils ont pour principaux objectifs de :

- Suivre la mise en œuvre de la présente politique.
- Suggérer des mises à jour.
- Proposer des documents et procédures complémentaires pour faciliter ou préciser la mise en œuvre de cette politique.
- Suivre l'évolution de la documentation technique et s'assurer que la politique a bien été prise en compte.

6. Mise en œuvre de la politique par les équipes informatiques et de développement

Le DSI et l'équipe de sécurité informatique assurent l'autorité nécessaire vis-à-vis des équipes informatiques et de développement pour garantir la bonne mise en œuvre de la politique.

Ils ont pour mission de :

- Élaborer des méthodes de protection pour protéger les systèmes d'information et s'assurer que ces méthodes sont appliquées.
- Inspecter les systèmes d'information de l'entreprise.
- Maintenir continuellement à jour un rapport sur la situation de tous les systèmes d'information concernant la sécurité et la mise en œuvre de la politique.
- Mettre en place un processus de surveillance de tous les réseaux d'entreprise, afin de pouvoir réagir rapidement et efficacement à une éventuelle cyberattaque.
- Communique régulièrement avec des tiers et des fournisseurs de services afin de détecter les failles de sécurité potentielles et de pouvoir les contrer et déployer des correctifs de sécurité rapides.

Les équipes de développement, IT et QA devront également collaborer efficacement autour des mesures de sécurité, leur mission sera de :

- Organiser et mettre en œuvre des capacités opérationnelles de détection des problèmes, de collecte de commentaires et de gestion des incidents.
- Assurer l'amélioration des flux d'informations avec l'équipe de sécurité informatique.

7. Mise en place de procédures au sein de l'entreprise

L'entreprise doit mettre en place un processus de gestion des risques pour tous ses systèmes d'information. Cette démarche doit permettre une meilleure maîtrise des SI en mettant en place des mesures de protection en fonction des enjeux stratégiques et des risques encourus.

Cette gestion s'appuie sur un processus continu d'identification, d'appréciation et de traitement des failles de sécurité. Ce processus doit également garantir des réponses de sécurité appropriées. Le choix de ces mesures se fait alors que les actions et leur coût sont conformes à la réduction des risques. Le DSI et l'équipe de sécurité informatique doivent toujours être consultés sur les choix stratégiques de sécurité.

L'entreprise doit:

- Toujours avoir une organisation qui permet le respect de la présente politique.
- Établir un inventaire complet et exhaustif de tous ses systèmes d'information et évaluer la sensibilité de leurs informations.
- Instruit les analyses de risques de ses systèmes d'information et rassemble les ressources nécessaires aux mesures de sécurité.
- Instruit des campagnes et formations de motivation et de sensibilisation autour de la sécurité des systèmes d'information et fournit une communication claire sur les sanctions possibles pour non-respect des chartes et des règles d'utilisation des SI (y compris les actions en justice).
- Établir un contrôle régulier de l'accès aux systèmes d'information et ordonner des manœuvres correctives.
- Établir des processus qui garantissent une bonne gestion des alertes, des incidents de sécurité et des situations d'urgence.

L'entreprise doit adapter les mesures de cette politique lorsque cela est nécessaire et justifié. Des documents techniques et un plan d'action pluriannuel décrivant les étapes successives de la mise en œuvre de la politique doivent également être établis.

Déroger aux règles et mesures décrites dans la présente politique doit toujours être fait après approbation des DSI et des équipes de sécurité informatique.

Un rapport annuel est établi par l'entreprise, qui comprend:

- Évolution et mise à jour de la cartographie des systèmes d'information.
- Indicateurs globaux permettant d'évaluer la maturité de la sécurité des systèmes d'information.
- Progrès dans l'organisation et la mise en œuvre de la présente politique.
- Un résumé de toutes les mesures prises pour se conformer à la présente politique.
- Un résumé de tous les incidents de sécurité majeurs (éventuellement accompagné d'une description des réponses prises aux incidents).
- Un résumé des tests effectués avec le rapport de leurs résultats.

8. Suivi de la mise en œuvre de la politique

La cohérence des procédures de sécurité et de la présente politique est de la responsabilité du CIO et de l'équipe de sécurité informatique.

La conformité avec la présente politique et les pratiques de sécurité recommandées doivent être sous la supervision du CIO et être évaluée régulièrement par le personnel compétent.

Hormis des évaluations régulières, des actions de contrôle peuvent être effectuées à la suite d'incidents de sécurité majeurs, ou suite à une forte suspicion de non-conformité. Dans ces cas, le CIO remplit un rapport qui sera présenté lors de l'évaluation annuelle.

9. Gestion des incidents et gestion des crises

La rapidité des cyber-attaques oblige à maintenir une veille, une réaction et une coordination renforcées des différents acteurs. Afin de rétablir le bon fonctionnement de toutes les activités dans les plus brefs délais, une stratégie de réponse aux incidents doit être établie et suivie.

Tous les acteurs concernés (clients, utilisateurs, gestionnaires d'applications, gestionnaires d'infrastructure...) doivent signaler toutes les anomalies et événements qui affectent ou peuvent affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité d'un système d'information. Ces incidents doivent ensuite être rapidement signalés à l'équipe de sécurité informatique pour une réponse rapide.

Une alerte est une action d'information qui implique la prise de conscience des acteurs concernés qu'une anomalie technique ou fonctionnelle concernant la sécurité des systèmes d'information a été détectée et doit être traitée. Cela implique également que les mesures doivent être vérifiées. Ces alertes provenaient de la veille continue de l'équipe de sécurité informatique. Des alertes importantes sont signalées au CIO qui est chargé de les traiter en demandant une action de réponse.

Une urgence de sécurité survient lorsqu'une alerte ou un incident sur un ou plusieurs systèmes d'information crée un dysfonctionnement majeur des applications Hamilton et / ou des activités de ses clients. Une situation de cette nature nécessite une grande réactivité et une coordination planifiée des acteurs concernés. C'est pourquoi il est impératif pour l'entreprise d'avoir et de suivre un planning de continuité d'activité (correspondant aux « PRA » et « PCA » français).

Objectifs et règles

Les 10 orientations stratégiques introduites dans la première partie du présent document sont traduites en une liste d'objectifs à atteindre et les procédures correspondantes pour chaque situation.

1. Organisation de la sécurité des systèmes d'information

Mise en place d'une organisation adaptée garantissant des réponses préventives et efficaces aux failles de sécurité.

Security contacts

DIDIERJEAN Yannick
Production director / CIO
yannick.didierjean@safeware.fr

BOUFERRACHE Belkacem
Application security
belkacem.bouferrache@safeware.fr

MAHFOUD Foad
Infrastructure security
foad.mahfoud@safeware.fr

Le graphique organisationnel ci-dessus est ici à titre de référence et peut changer sans préavis.

Une organisation dédiée à la sécurité des systèmes d'information est implantée au sein de l'entreprise. L'organisation prend la forme d'une équipe d'experts en sécurité informatique placée sous la tutelle du CIO. Ils établissent des processus de protection, définissent les responsabilités internes et définissent les directives et règles de sécurité pour le développement d'applications.

Les membres de l'organisation de sécurité sont clairement identifiés et connus de tous les membres de l'entreprise. Ils sont le point de référence de l'entreprise en termes de sécurité dans leur zone spécifiée.

Les responsabilités internes en matière de sécurité sont portées par l'équipe de sécurité informatique au sein de laquelle des personnes peuvent être désignées comme responsables de domaines spécifiques. La répartition des responsabilités au sein de l'équipe est définie par le CIO.

Du point de vue externe, tiers ou client, la sécurité est sous la seule responsabilité du DSI.

L'équipe de sécurité planifie des actions pour mettre en œuvre la présente politique et rend régulièrement compte au CIO des progrès de la mise en œuvre. Il tient également à jour la documentation technique de sécurité, et l'approuve par le CIO, ce qui permet de préciser la mise en œuvre de la présente politique sur son périmètre d'application.

2. Ressources humaines

S'assurer que les employé de l'entreprise connaissent leurs droits concernant les systémes d'information et leurs données.

3.2.1 Utilisateurs

Une charte d'utilisation des systèmes d'information, qui rappelle les bonnes pratiques en matière de sécurité et définit les droits et usages concernant les données de l'entreprise et du client, est élaborée par l'équipe sécurité informatique et communiquée à l'ensemble des collaborateurs. Cette charte doit être juridiquement contraignante et, si possible, intégrée dans le règlement intérieur de l'entreprise. Les salariés non permanents (stagiaires, intérimaires, prestataires externes...) sont informés de leurs droits concernant l'utilisation des systèmes d'information de l'entreprise.

3.2.2 Postes de responsabilité du personnel

Une attention particulière doit être portée lors du recrutement de personnel qui traitera des données sensibles et privées et pourra jouer un rôle dans la mise en œuvre de la présente politique de sécurité au sein de l'entreprise. Le personnel de l'équipe de sécurité informatique doit avoir suivi une formation spécifique à la sécurité des systèmes d'information. Les administrateurs de systèmes d'information doivent être régulièrement sensibilisés aux obligations de leur fonction et doivent respecter ces exigences de sécurité dans l'exercice de leurs fonctions.

3.2.3 Personnel non-permanent

Les règles et exigences de la présente politique s'appliquent à tout le personnel non permanent lorsqu'ils interagissent avec les systèmes d'information, quel que soit leur statut. Les dispositions contractuelles préexistantes devraient être modifiées si nécessaire et si possible. Tout personnel non permanent devrait également être affecté à un supervisé par un employé qualifié, afin d'assurer le respect de la présente politique.

3. Maintenir les exigences de sécurité

Adaptez dynamiquement les mesures de protection, pendant la durée de vie des systémes d'information.

3.1 Intégration des besoins de sécurité dans les projets

La sécurité des systèmes d'information doit être prise en compte à toutes les étapes d'un projet informatique. Il doit être contrôlé et certifié par l'équipe de sécurité informatique, de la conception et de la spécification à la fin de son service.

3.2 Intégration continue de la politique de sécurité

La sécurité des systèmes d'information est traitée régulièrement par des méthodes courantes de développement propre. Les procédures écrites définissent les actions élémentaires à appliquer et à maintenir lors des phases de conception, d'évolution et de déclassement.

3.3 Table de surveillance

Une table de surveillance doit être maintenue et mise à jour régulièrement par l'équipe de sécurité informatique. Cette table de suivi donne une visibilité au CIO et au conseil d'administration de l'entreprise sur l'évolution de la sécurité à travers les projets et la structure de l'entreprise. Sur un plan stratégique, ce tableau de suivi permet à l'entreprise de disposer d'éléments factuels pour définir et allouer un budget à la sécurité informatique. Au niveau de la gestion de projet, cette carte permet de définir et de suivre des objectifs opérationnels et de détecter d'éventuels retards dans l'intégration des mesures de sécurité.

4. Utiliser des produits de qualité et certifiés

Utiliser des produits dont la sécurité a été évaluée et certifiée par le CIO.

Tous les produits et outils utilisés par l'entreprise doivent être choisis en tenant compte de leur qualification de sécurité (labels, certifications) et doivent être approuvés par le CIO après évaluation de leur efficacité en termes de sécurité.

5. Clauses contractuelles de sécurité

S'assurer que les fournisseurs tiers sont conformes aux exigences de la politique de sécurité de l'entreprise.

5.1 Clauses contractuelles de sécurité

Tout approvisionnement provenant de fournisseurs externes et tiers doit être encadré par des conditions contractuelles de sécurité. Ces conditions précisent les chartes et mesures de sécurité que le prestataire doit respecter dans le cadre de ses activités.

5.2 Suivi et inspection des provisions

Pour maintenir un haut niveau de sécurité informatique, une double vérification est toujours nécessaire comme suit:

- Le premier au cours du processus de conception et de mise en œuvre, le chef de projet doit périodiquement enquêter sur les actions du prestataire et s'assurer qu'il est conforme au cahier des charges.
- La seconde, réalisée par l'équipe de sécurité informatique, consiste à enquêter sur la spécification des exigences du contrat, à superviser les tests de sécurité et à vérifier l'intégrité des actions correctives du prestataire puis à évaluer le niveau de sécurité globale du produit en production.

5.3 Analyse de risque

Une analyse des risques est effectuée avant tout processus d'externalisation. Cela permet de définir des objectifs de sécurité et des mesures appropriées. Tous les objectifs de sécurité sont formalisés afin que l'entreprise et le fournisseur puissent convenir d'un niveau de sécurité à atteindre qui sera inclus dans le contrat.

5.4 Hébergement de données

Toutes les données sensibles ou clientes sont hébergées à l'intérieur du territoire de l'Union européenne, et de préférence sur le territoire national. Les seules exceptions sont sur demande directe du client, ou si le client est basé en dehors de l'Union européenne, auquel cas la décision d'hébergement hors du territoire de l'Union européenne doit être approuvée par le CIO.

6. Accès spécifiques

Assurer l'intégrité en empêchant l'accès non supervisé qui peut compromettre la sécurité des systèmes d'information.

Un accès spécifique aux systèmes d'information de l'entreprise ne peut être accordé que s'il existe une dérogation détaillée et justifiée. Elle doit être réalisée sous contrôle interne et dans un environnement restreint. En cas de système d'information lié au client, l'accès ne peut être accordé sans le consentement exprès du client.

7. Sécurisation des infrastructures

Application de la protection des infrastructures avec des mécanismes physiques et des logiciels de protection à l'intérieur des Datacenters.

7.1 Intégrité physique de l'infrastructure

De manière générale, les Datacenters sont conçus pour que leurs architectures et infrastructures puissent satisfaire tous les besoins en termes de disponibilité, confidentialité, traçabilité et intégrité. Il est toujours fortement recommandé d'obtenir des garanties des prestataires de services et de s'assurer que ces services répondent aux besoins de l'entreprise.

7.2 Application du concept de défense en profondeur

Pour assurer un niveau de défense maximum, l'infrastructure doit être constituée de machines privées et dédiées, avec des séparations virtuelles et physiques. Des réseaux locaux virtuels (VLAN) appropriés et des flux d'application et d'administration strictement filtrés peuvent être utilisés.

7.3 Infrastructure de sauvegarde et de stockage

Le réseau dédié aux sauvegardes et au stockage doit être basé sur une infrastructure dédiée.

8. Protection des données sensibles

Dèfinir et ètablir des mesures de protection avancèes pour les donnèes sensibles.

Des mesures de sécurité doivent être mises en place afin de garantir la protection des informations sensibles à la fois en confidentialité et en intégrité. Les informations doivent être utilisées dans un réseau sécurisé et, dans certains cas, renforcées à l'aide d'un chiffrement localisé.

9. Surveillance et configuration des ressources informatiques

Resserrer les contrôles et les configurations des ressources informatiques et surveiller les opérations effectuées sur celles-ci.

9.1 Suivi des manipulations du système

Toute maintenance effectuée sur un système ou des ressources informatiques doit être suivie par les services de sécurité informatique et doit être accessible au CIO pendant une période minimale d'un an.

9.2 Configuration des ressources informatiques

Les systèmes d'exploitation et les applications doivent être installés, configurés et mis à jour en suivant leur documentation et les protocoles recommandés et sous la supervision du DSI en cas de besoin.

9.3 Documentation de configuration

La configuration de toutes les ressources informatiques doit être documentée et mise à jour à chaque modification notable.

10. Contrôle d'accès et autorisations

Authentifier les utilisateurs et limiter leur accès aux ressources et aux systèmes d'information avec un système d'autorisation robuste.

10.1 Contrôle d'accès logique

L'accès à toutes les ressources non publiques doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de données sensibles, un protocole d'authentification fort doit être utilisé.

En fonction du niveau de sensibilité, du besoin de distribution et des droits d'accès définis, l'utilisateur ne doit pouvoir accéder à une ressource que si l'une des deux méthodes valide la demande:

- Un accès à la ressource spécifique a été explicitement créé pour l'utilisateur.
- La ressource a un privilège de droit d'accès minimum qui est sous le niveau de privilège de l'utilisateur.

Les applications contenant des données sensibles doivent avoir une gestion affinée des droits d'accès. Les deux méthodes précédemment mentionnées ici doivent être appliquées et combinées.

10.2 Processus d'authentification

Toutes les autorisations d'accès à un système d'information ou à l'une de ses ressources doivent être basées sur une validité temporelle qui commence lorsqu'un employé rejoint l'entreprise et se termine une fois que l'employé ne fait plus partie de l'entreprise.

Un examen annuel de tous les accès valides est effectué par l'équipe de sécurité informatique, sous la supervision du CIO.

10.3 Gestion des identifiants et authentificateurs

Les informations d'authentification (mots de passe, clés privées, certificats...) doivent être considérées comme des données sensibles et sont strictement confidentielles.

Les utilisateurs ne doivent jamais stocker leurs mots de passe en texte brut (par exemple à l'intérieur d'un fichier). Les mots de passe de toutes sortes ne doivent également jamais être transmis via les réseaux sociaux ou les réseaux de communication non sécurisés.

Chaque compte d'utilisateur est créé avec un mot de passe initial aléatoire à haute complexité. Dans certains cas, un mot de passe moins complexe peut être créé, mais uniquement si son utilisation est limitée à une seule fois.

La complexité des mots de passe doit être évaluée et appliquée techniquement à l'intérieur des outils et des systèmes d'information de l'entreprise.

10.4 Gestion des authentificateurs administratifs

Les authentificateurs de comptes génériques permettant d'accéder aux ressources des systèmes d'information doivent être verrouillés et tenus à jour, à l'intérieur d'un coffre-fort, d'un tiroir ou d'une armoire verrouillée. Tout accès à une ressource informatique doit être suivi et il doit être en mesure d'identifier la personne qui a fait la demande d'accès.

Chaque administrateur doit avoir un mot de passe très complexe qui n'est connu de personne d'autre.

Si un administrateur quitte l'entreprise, son accès personnel à tous les systèmes d'information doit être immédiatement désactivé ou supprimé. Tous les mots de passe d'administration (comptes génériques par exemple) dont il avait connaissance doivent être modifiés.

11. Administration et protection des informations

Donner aux administrateurs les outils nécessaires pour assurer la sécurité informatique.

11.1 Administration des systèmes

Les utilisateurs ne doivent jamais disposer de privilèges administratifs sans une demande et des besoins très spécifiques, auquel cas l'approbation du DSI est requise.

L'accès aux outils d'administration et aux interfaces doit être limité au personnel autorisé, suivant un processus d'autorisation strict.

Le nombre de personnes autorisées disposant de privilèges administratifs et leur identité doivent être connus et validés par le DSI. Dans le cas des systèmes d'information liés au client, la liste des administrateurs côté client est définie par eux-mêmes.

Toutes les opérations administratives sont suivies et leur auteur identifié. Cela vise à accroître la responsabilité de chaque action administrative.

Toutes les opérations administratives sur les ressources locales utilisent des protocoles de sécurité réseau. Un réseau dédié et séparé (physiquement ou logiquement) de celui de l'utilisateur est utilisé pour la manipulation de la plateforme et de l'infrastructure.

Afin d'améliorer la gestion des systèmes d'information, les administrateurs doivent avoir accès à des outils centralisés, permettant l'automatisation des tâches administratives et offrant une vue d'ensemble de tous les systèmes d'information.

11.2 Contrôle à distance

Le contrôle à distance des systèmes d'information doit être limité aux membres spécifiquement autorisés de l'équipe informatique, et uniquement sur les systèmes dont ils sont responsables. Des mesures de sécurité spécifiques autour du contrôle à distance doivent être définies et établies pour éviter les failles de sécurité.

11.3 Administration des domaines

Une politique d'administration des comptes de domaine doit être définie et documentée.

Les mots de passe des comptes de domaine doivent être soumis à une procédure stricte visant à les protéger des attaques par force brute. Une complexité minimale des mots de passe doit également être rendue obligatoire pour les utilisateurs.

La gestion des comptes doit impliquer une dénomination claire qui permet de distinguer facilement les comptes d'utilisateurs standard, les comptes administratifs (domaine, serveurs, systèmes...) et les comptes de service.

L'affiliation à des groupes administratifs tels que les ADMINISTRATEURS D'ENTREPRISE et les ADMINISTRATEURS DE DOMAINE doit être limitée à un nombre restreint d'employés et est nécessaire dans de rares cas.

La majorité des tâches administratives doivent être effectuées à partir de comptes administratifs de portée locale et non de comptes à l'échelle de l'entreprise, ou après réception d'une délégation administrative.

Les comptes de services peuvent avoir leurs mots de passe ou jetons d'accès écrits en texte brut à l'intérieur des applications ou des systèmes qui les utilisent. Afin d'assurer la réactivité en cas de rupture de confidentialité de l'un d'entre eux, ils doivent être suivis et faciles à gérer.

Les comptes de services doivent avoir des droits minimaux et restreints, selon le principe du « moindre privilège ».

Il est absolument nécessaire de désactiver immédiatement ou de supprimer les comptes obsolètes. Indépendamment de leur type (comptes utilisateurs, administratifs, services).

Pour empêcher l'utilisation des droits d'administration à portée locale d'un système à un autre, les mots de passe des administrateurs locaux doivent être différents et les connexions distantes à ces comptes système doivent être restreintes ou interdites.

11.4 Protection contre les programmes malveillants

Un logiciel de protection contre les programmes malveillants, communément appelé anti-virus, doit être installé sur tous les systèmes d'interconnexion et d'application, ainsi que sur les postes de travail de l'entreprise. Les outils logiciels de protection doivent être adaptés à ces trois catégories de systèmes et de préférence différents pour chacun d'entre eux.