Plan Assurance Sécurité

Application de gestion d'actifs en ligne Hector

Mise à jour le 4 janvier 2023 par Joey Montambeault

hector

Tables des matières

Plan Assurance Sécurité **1**
Tables des matières 2
1. Révisions du document 2
Diffusion 2
2. Introduction **2**
Objet 2
Périmètre 2
Les équipes 3
Documents de référence 3
3. Enjeux et objectifs 5
Enjeux 5
4. La gestion des risques 6
5. Politique de Sécurité du Système d'Information 7
6. Organisation de la sécurité de l'information 8
Organisation 8
Veille 8
Gestion des risques dans les projets 8
7. La sécurité des ressources humaines 8
Embauche 8
Confidentialité 9
Sensibilisation à la sécurité 9
Compétences et formation 9
Départ 9
8. Gestion des actifs 9
Inventaire et identification des actifs 9
Gestion des supports amovibles 10
Mise au rebut des actifs 10
9. Contrôle d'accès 10
Politique de mot de passe 10
Gestion des droits d'accès 11
Revue des droits d'accès 11
10. Cryptographie 12
Transfert de données 12
Chiffrement 12
Certificats 12

Postes nomades 12
11. Sécurité physique et environnementale 12
Localisation 12
Certifications des centre de données 12
12. Sécurité liée à l'exploitation 12
Procédures d'exploitation 12
Logiciels malveillants 12
Sauvegardes 13
Tests de restauration 14
Supervision 14
Gestion des mises à jour système 15
Gestion des mises à jour des applications 15
13. Sécurité des communications 15
Architecture technique 15
Pare-feu 15
Détection d'intrusion 15
14. Acquisition, développement et maintenance des SI 16
Politique de développement 16
15. Relation avec les fournisseurs 16
16. Gestion des incidents liés à la sécurité de l'information 17
Incidents de sécurité 17
Gestion de crise 18
17. Gestion de la conformité 18

1. Révisions du document

Date de publication	Auteur
27/10/2021	J. Montambeault
11/12/2022	M. Vigier

Diffusion

Document diffusé auprès des clients de Hector Inc.

2. Introduction

Objet

Le Plan Assurance Sécurité, noté PAS dans la suite de ce document, permet de décrire les engagements pris par Hector Inc. en termes de sécurité des données et applications hébergées sur sa plateforme d'hébergement avec son fournisseur Vultr. Holdings et Microsoft Azure.

Périmètre

Le PAS s'applique à tous les services fournis aux clients, ce sont principalement :

- L'application de gestion d'actifs, développées par Hector (en mode SaaS)
- L'API (Application Programming Interface)
- L'Application Mobile disponible sur App Store et Google Play Store
- La sauvegarde externalisée (mode SaaS)
- Le Plan de Reprise d'Activité (PRA)
- L'hébergement de serveurs et d'applications

Les équipes

Hector et son équipe sont chargés de la fourniture des services hébergés et des applications en mode SaaS aux clients. Cette équipe est composée de personnels permanents. Les principales activités de cette équipe sont les suivantes :

- Gérer et faire évoluer la plateforme d'hébergement.
- Mettre en production les solutions d'hébergement et l'accès aux applications SaaS vendues aux clients.
- Assurer l'exploitation et l'administration des services.
- Assurer l'assistance technique auprès des clients

Documents de référence

CGS : Conditions Générales de Service
Et les conditions particulières, qui peuvent être

- Les Conditions Particulières d'Hébergement
- Les Conditions Particulières de Service SaaS
- Les Conditions Particulières de Service

L'ensemble de ces documents est disponible sur le site hectorassetmanager.com/fr/

Les réglementations relatives à la Protection des Données Personnelles :

- Loi n°78- 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2018-493 du 20 juin 2018.
- Le Règlement Général sur la Protection des Données (RGPD)

3. Enjeux et objectifs

Enjeux

La sécurité de la plateforme d'hébergement et du Système d'Information de Hector est une composante essentielle de la protection des intérêts propres de la société Hector, ainsi que celle de ses clients.

Il est donc impératif qu'une Politique de Sécurité du Système d'Information soit mise en œuvre, et qu'elle prenne en compte les principaux risques encourus et identifiés :

- Risque d'indisponibilité des informations et applications, et des systèmes les traitant.
- Risque de divulgation, ou perte de confidentialité, accidentelle ou volontaire des informations fournies par nos clients et pour lesquelles nous agissons en tant que sous-traitant.
- Risque d'altération, ou perte d'intégrité, qui pourrait amener à une perte d'information pour nos clients.

Les objectifs de mise en œuvre de la Politique de Sécurité du Système d'Information sont :

- Améliorer et formaliser la gestion de la sécurité de la plateforme d'hébergement.
- Prévoir l'extension des services actuels en proposant des services hébergés dans des Cloud publics, par exemple l'offre Azure de Microsoft, qui sont déjà certifiés ISO 27001.
- Étendre les bonnes pratiques à tous les services proposés par Hector.
- S'assurer du respect par Hector de ses obligations légales en ce qui concerne la gestion des Données Personnelles (Loi Informatique et Libertés, RGPD), et être en mesure de le démontrer auprès des clients auprès desquels Hector intervient en tant que sous-traitant.
- Créer une culture de la sécurité auprès des équipes d'Hector, et de ses clients.

4. La gestion des risques

La direction générale de Hector souhaite que les risques de sécurité de l'Information qui pourraient conduire à une rupture de services inacceptable pour les clients soient gérés de manière continue.

La sélection du fournisseur Vultr pour l'hébergement des données des clients a été faite à la suite d'une analyse approfondie des fournisseurs de services, de la certification de leurs centres de données, d'avoir des centres de données à plusieurs emplacements géographiques, et une culture de sécurité exceptionnelle.

Cette analyse de risques a donné lieu à un plan d'actions d'évolution des mesures de sécurité mises en œuvre.

5. Politique de Sécurité du Système d'Information

Afin de répondre à ses obligations réglementaires, d'améliorer ses processus pour y intégrer en permanence l'aspect sécurité de l'information, et ainsi améliorer les pratiques de l'ensemble des équipes techniques, Hector Inc met à jour sa Politique de Sécurité (PSSI) de façon annuelle.

Cette politique a été mise en place en 2019 et est révisée régulièrement. Elle se base sur les normes de sécurité ISO 27001 et ISO 27002, et est totalement intégrée dans l'entreprise.

Un Délégué à la Protection des Données (DPO dans la suite du document) a été nommé. Il est également le responsable qualité et la sécurité de l'entreprise. Il a pour missions de s'assurer que la PSSI répond aux obligations légales sur la Protection des Données Personnelles.

La PSSI est diffusée à l'ensemble des personnes concernées, et Hector inc. met en œuvre les formations et informations nécessaires à sa compréhension, sa bonne mise en œuvre et son respect.

La PSSI est un document interne à Hector Inc. et confidentiel. Le Plan Assurance Sécurité (PAS) reprend les informations de la PSSI, communicables aux clients, pouvant ainsi faciliter sa lecture et sa compréhension.

6. Organisation de la sécurité de l'information

Organisation

Chaque salarié possède une fiche de poste qui décrit ses missions, son positionnement au sein de l'organisation de Hector Inc, ses principales activités, et les savoir-faire et savoir-être qu'il doit maîtriser pour mener à bien ses missions.

La sécurité est pilotée :

- Au niveau stratégique au minimum une fois par an lors d'une revue de direction dédiée à la sécurité par le comité de direction de l'entreprise.
- Au niveau opérationnel lors d'une revue mensuelle.

Les chefs de service sont les responsables du respect par leurs équipes de la PSSI mise en place. Ils sont aidés dans cette mission par le comité de direction.

Veille

Hector Inc a qualifié des fournisseurs dans le domaine de la sécurité, et participe régulièrement à des manifestations sur les évolutions dans les domaines réglementaires, techniques, organisationnels et sur les produits.

Gestion des risques dans les projets

La méthodologie projet élaborée par Hector Inc, impose la prise en compte de la notion de risques dans tout nouveau projet.

Mobilité et télétravail

L'accès au Système d'Information de Hector Inc. peut être effectué uniquement avec des matériels appartenant à la société, même au domicile des collaborateurs.

7. La sécurité des ressources humaines

Embauche

Un projet « arrivée » formalisé permet de structurer l'intégration de tout nouveau collaborateur. Les droits d'accès aux informations et aux applications peuvent évoluer selon le statut de l'intégration (durée minimale de présence, période d'essai terminée, …).

Confidentialité

Tout collaborateur signe une clause de confidentialité dans son contrat de travail.

Tout collaborateur a pris connaissance de la charte informatique, l'a signée et s'est engagé à la respecter et à la faire respecter. Cette charte fait également référence aux obligations de confidentialité, et définit les règles de bon usage des ressources informatiques et numériques mises à disposition.

Sensibilisation à la sécurité

Le projet « arrivée » de tout nouveau collaborateur prévoit une sensibilisation à la sécurité. Des sessions de sensibilisation sont organisées de façon annuelle, en présentiel ou sous forme de webinar.

Compétences et formation

La gestion des compétences permet à Hector Inc d'identifier les besoins de formation.

Les chefs de services définissent les besoins de formation pour leurs équipes, ils sont transmis au service RH pour consolidation et validation d'un plan de formation annuel.

Départ

Un projet « départ » formalisé permet de structurer les actions à mener au départ de tout collaborateur, et en particulier la fermeture de ses comptes d'accès aux différentes ressources auxquelles il avait droit.

8. Gestion des actifs

Inventaire et identification des actifs

Tous les actifs des collaborateurs Hector inc, sont identifiés et inventoriés dans le système de gestion d'actifs de l'entreprise.

Gestion des supports amovibles

Aucun support amovible n'est utilisé pour l'administration et l'exploitation de la plateforme d'hébergement pour les clients. Les équipes techniques ne disposent pas de ce type de support.

Mise au rebut des actifs

Les supports physiques qui contiennent des données sont détruits physiquement avant leur mise au rebut. La seule exception est l'envoi à un constructeur d'un disque dur dans le cadre de la gestion d'un matériel sous garantie, c'est le constructeur dans ce cas qui s'engage à la destruction physique du matériel.

9. Contrôle d'accès

Politique de mot de passe

Chaque utilisateur est identifié par un identifiant unique et un mot de passe fort.

- La politique de mot de passe pour les utilisateurs des services hébergés est la suivante : Personnalisation par l'utilisateur lors de sa 1ère connexion sur l'environnement de production.
- Taille minimale : 8 caractères
- Complexité : lettre, chiffre et symbole
- Fréquence de changement : tous les 6 mois
- Pas de réutilisation des 5 derniers mots de passe
- Verrouillage après 5 tentatives infructueuses

Les mots de passe sont personnels et confidentiels, ils ne sont donc pas stockés par les équipes techniques. Si pour quelque raison que ce soit un intervenant technique a besoin de connaître le mot de passe d'un utilisateur, il sera demandé à ce dernier de le changer avant de le communiquer au technicien, et il sera obligé de le réinitialiser lors de sa connexion suivante.

Les comptes d'administration suivent les mêmes règles que celles des utilisateurs, si ce n'est que la taille minimale du mot de passe est de 16 caractères. Ces mots de passe sont stockés dans une base sécurisée et chiffrée.

Gestion des droits d'accès

Les membres permanents de l'équipe disposent de comptes d'accès en permanence. L'administration courante des environnements hébergés est réalisée par l'équipe d'Infrastructure informatique par l'intermédiaire de comptes d'administration aux droits limités. L'accès par les autres personnels techniques n'est autorisé que pour la durée d'affectation ou d'intervention prévue.

Revue des droits d'accès

Les droits d'accès d'administration à l'ensemble du Système d'Information Hector Inc. sont revus au minimum une fois par an.

10. Cryptographie

Transfert de données

Tout transfert de données vers la plateforme d'hébergement est réalisé par l'intermédiaire de liens VPN. Si des données confidentielles doivent transiter soit sur un média amovible, soit dans un mail, ces données doivent être chiffrées en respectant les règles en vigueur.

Chiffrement

Les équipes techniques utilisent un logiciel de chiffrement s'appuyant sur l'AES256.

Certificats

Les certificats utilisés par les équipes techniques proviennent d'autorités de certifications publiques et reconnues.

Postes nomades

Les disques durs des postes nomades des équipes techniques sont chiffrés.

11. Sécurité physique et environnementale

Localisation

Les centres de données d'Hector sont localisés aux emplacements suivants :

- Toronto, Canada
- New Jersey, États-Unis
- Paris, France

Certifications des centre de données

Emplacement	SOC TYPE I	SOC TYPE II	ISO 27001	PCI-DSS
Toronto	Oui	Oui	Oui	Oui
New Jersey	Oui	Oui	Oui	Oui
Paris	Oui	Oui	Oui	Oui

https://learn.microsoft.com/fr-fr/azure/compliance/
https://www.vultr.com/resources/faq/#datacenter_compliance

12. Sécurité liée à l'exploitation

Procédures d'exploitation

Hector documente pour l'ensemble de ses activités, les procédures d'exploitation sont documentées, mises à jour et régulièrement auditées.

Logiciels malveillants

Hector Inc n'a pas de réseau informatique interne. Tout le travail effectué par ses collaborateurs se fait dans la suite nuagique Google Workspace. L'accès à Google Workspace est sécurisé par les pratiques de sécurité énumérées dans la section contrôle d'accès. Chaque poste de travail est équipé d'une suite logicielle contre les logiciels malveillants. La disponibilité de mises à jour est vérifiée quotidiennement, elles sont automatiquement téléchargées et déployées sur les équipements.

La supervision et la console centralisée d'administration permettent de détecter immédiatement toute anomalie (mise à jour non déployée, infection, …).

Sauvegardes

Les données des clients des services SaaS sont sauvegardées tous les jours avec une rétention de 7 à 30 jours (ou plus longtemps) selon le plan de service.

Les serveurs virtuels des environnements hébergés sont sauvegardés tous les jours avec une rétention de 3 mois. L'ensemble des sauvegardes sont dupliquées dans chez un prestataire infonuagique différent de l'hébergeur chaque jour.

Tests de restauration

Des tests de restauration sont effectués chaque jour pour garantir qu'aucune faille ne soit introduite dans le système de sauvegarde.

Supervision

Les serveurs, moyens de communication et services sont supervisés en permanence, et des alertes sont positionnées afin que les équipes soient immédiatement informées de toute anomalie potentielle, ou de toute situation pouvant amener à une dégradation du service.

Gestion des mises à jour système

Services : les mises à jour critiques et de sécurité sont déployées lors de leur mise à disposition sur un échantillon pilote d'équipements, et elles sont ensuite déployées sur l'ensemble des environnements si aucune anomalie n'est survenue durant 1 semaine.

Gestion des mises à jour des applications

Les mises à jour critiques et de sécurité sont déployées dès leur mise à disposition dès leur validation dans un environnement de tests.

L'entreprise effectue entre 4 à 6 mises à jour de l'application par an.

13. Sécurité des communications

Architecture technique

Administration et management : un lien dédié est utilisé par les équipes techniques de Hector pour toute intervention sur la plateforme d'hébergement, l'accès à ce lien est filtré aux seules personnes habilitées par MAC adresse et adresse IP. En cas de rupture ou d'indisponibilité, l'accès est réalisé en accédant via Internet via la plateforme d'Azure et Vultr.

Pare-feu

Tous les accès à la plateforme d'hébergement et aux applications SaaS transitent par des pare-feux physiques et logiciels.

Détection d'intrusion

Tous les flux d'accès à la plateforme sont analysés afin d'identifier et bloquer les flux anormaux et les programmes malveillants.

Des tests d'intrusion sont effectués chaque mois pour détecter les vulnérabilités. Les vulnérabilités critiques sont traitées dans la journée ouvrable suivant leur détection. Les vulnérabilités sévères sont réparées dans la semaine suivant leur détection.

14. Acquisition, développement et maintenance des SI

Politique de développement

Les activités de développement sont conformes aux cycles en V ou aux méthodologies Agile qui sont utilisés par les équipes Hector.

Toute nouvelle version, que ce soit un correctif, une évolution ou une montée de version a fait l'objet de tests et de validations préalables avant mise en œuvre dans l'environnement SaaS.

Une phase de retour arrière est prévue si le moindre dysfonctionnement est constaté suite à une mise à jour.

15. Relation avec les fournisseurs

Des sous-traitants sont amenés à intervenir sur la plateforme hébergée, il peut s'agir :

- Du propriétaire des centres de données

Les relations entre ces sous-traitants et Hector répondent aux exigences liées au RGPD, et prennent en compte les aspects sécurité.

Toutes les interventions des sous-traitants sont tracées et respectent une procédure, notamment en ce qui concerne les affectations des droits d'accès.

16. Gestion des incidents liés à la sécurité de l'information

Incidents de sécurité

Chaque acteur du SI et de la plateforme d'hébergement, utilisateur ou administrateur, Hector Inc ou sous traitant, Client, est sensibilisé à l'importance de signaler tout incident réel ou suspecté. Ceci inclut le vol de moyens informatiques ou de supports de données.

Le signalement des incidents et leur enregistrement sont systématiques. Les Clients le font par l'outil de billetterie d'Hector Inc, les utilisateurs internes suivent la procédure mise en place. Cette procédure décrit les escalades et personnes à alerter selon la gravité de l'incident.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la sécurité du SI.

Un incident de type violation de Données Personnelles respecte les obligations liées au RGPD, il peut faire l'objet d'une notification aux autorités.

Gestion de crise

Le plan de gestion de crise intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur le SI ou la plateforme d'hébergement.

17. Gestion de la conformité

ISO 27001 : Les centre de données d'Hector sont certifiés selon les normes ISO 27001 et ISO 27002 pour la gestion de la sécurité, de la fourniture de services hébergés et d'application SaaS, et pour la fourniture des services auprès de tous les clients.

Données Personnelles : Le Délégué à la Protection des Données Personnelles est le garant du respect par Hector Inc de ses obligations. Il est joignable à l'adresse rgpd@hectorassetmanager.com.