Jamespot.

Plan Assurance Sécurité Jamespot (V1.1)

Sommaire

Introduction

Jamespot documente un Plan d'Assurance Sécurité (« PAS ») pour décrire comment il adresse les exigences de Sécurité, en décrivant les solutions mises en œuvre.

Le PAS définit notamment les procédures internes utilisées pour respecter les mesures de sécurité, ainsi que les procédures de gestion des incidents de sécurité.

Liste des versions

Version	Date	Description	Auteur(s)
V1.0	13/11/2016	Plan Assurance Sécurité	Paul Giraudon
V1.1	10/09/2020	Mise à jour du template de présentation. Mise à jour des sous-traitants.	Paul Giraudon

Glossaire

Nom	Définition
CS	Correspondant Sécurité
PAS	Plan d'Assurance Sécurité
RSSI	Responsable de la sécurité des systèmes d'information
Informations	Les Données de quelque nature que ce soit communiquées et/ou mises à disposition par le client dans le cadre d'un projet
Écosystème	Plateforme Jamespot https://ecosysteme.jamespot.pro utilisée pour communiquer entre Jamespot et ses clients

Organisation et animation de la Sécurité

Chaque Client désigne les Administrateurs de sa plateforme. Ces Administrateurs sont dès lors en contact avec le Support Jamespot. Ils seront membres des différents canaux de remontées d'information de l'équipe CSM de Jamespot, et recevrons par ces canaux les informations de sécurité générales, communes à tous les clients de Jamespot.

Pour les cas de projets accompagnés spécifiquement, les clients se verront désigner un contact unique qui centralise les informations du projet, que ce soit au niveau fonctionnel ou sécurité : le chef de projet Jamespot.

Ce contact sera le lien privilégié pour traiter les aspects Sécurité spécifiques au projet, il sera donc le CS du client.

Responsabilités de Jamespot

Jamespot a la responsabilité durant toute la durée du projet d'assurer la sécurité et la confidentialité des Informations qui sont mises à disposition par ses Clients.

Le CS rend compte des procédures opérationnelles de Sécurité prévues au PAS.

Engagement de confidentialité

Les supports informatiques, documents, Informations, données... fournis par le Client restent la propriété du Client.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel.

Conformément à l'article 35 de la Loi Informatique et Libertés, Jamespot s'engage à prendre toutes précautions utiles afin de préserver la sécurité des Données à caractère personnel et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Jamespot s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- Ne prendre aucune copie des documents et supports d'Informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation dans le cadre du projet, sans l'accord du Client ;
- Ne pas utiliser les documents et Informations traités à des fins autres que celles du projet ;
- Ne pas divulguer ces documents ou Informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du projet ;
- Prendre toutes mesures de sécurité, pour assurer la conservation et l'intégrité des documents et Informations traités pendant la durée du projet ;
- Et en fin de projet, procéder à la destruction des Informations du Client et à rendre au Client les Informations lui appartenant.

Réversibilité

Jamespot s'engage à fournir au Client les Informations gérées par ses plateformes, et à garantir, lors du transfert, la sécurité des données qui lui ont été confiées, conformément à ses obligations.

En cas d'arrêt des prestations confiées, l'ensemble des Informations sera restitué.
La réversibilité se fait via Dump SQL sécurisé de toutes les données (profils, groupes, publications, commentaires et base documentaire) vers le serveur au choix du Client par copie sftp ou ftps.

Sécurité physique

L'ensemble des données est hébergé par OVHcloud qui s'assure de la sécurité physique des systèmes.

Jamespot s'assure que l'ensemble des Informations du périmètre du projet sont localisées et hébergées en Union Européenne [SR Jitsi est un service hébergé hors de l'union européenne]

Sécurité d'exploitation

Procédures liées à l'exploitation

Durant la période d'abonnement au service, la plateforme SaaS Jamespot sera amenée à évoluer fonctionnellement. En effet, de manière régulière, de nouvelles fonctions sont ajoutées et profitent donc à l'ensemble de la communauté des clients de Jamespot.
Ces nouvelles fonctions sont en général mises à disposition gratuitement dans le cadre de la facturation annuelle de l'abonnement à la plateforme :

- soit de manière mineure par évolution des interfaces existantes,
- soit sous forme de nouvelles applications, que chaque administrateur de plateforme est libre de déployer ou non.

Les développements sont mis en production par un outil de développement continu, suivant les procédures de mise en production de Jamespot.

Sécurité des réseaux

L'ensemble des serveurs n'est accessible en SSH que depuis une liste fermée d'adresses IP ou le VPN de Jamespot.

L'accès aux ports HTTP et HTTPS est autorisé depuis toutes les provenances.

L'accès à la plateforme des clients peut être configurée pour s'effectuer exclusivement par HTTPS.

Sécurité du développement et de la maintenance

Des sauvegardes multiples et redondantes sont effectuées afin de garantir l'intégrité des informations.

Les modifications sont déployées après un processus de validation en mode Intégration Continue : tests unitaires, tests de scénarios utilisateurs. On utilise Jenkins pour gérer cette tâche.

L'ensemble du système est contrôlé par plusieurs outils de monitoring afin de détecter les éventuels problèmes et vulnérabilités, et d'en alerter l'équipe de développement.

Protection contre les codes malveillants

Les serveurs sont placés sous monitoring constant par deux prestataires externes, et envoient des données de production en temps réel : CPU, Entrées sorties, Mémoire, et tout dépassement de seuils définis engendrent l'envoi d'une alerte mail et/ou SMS.

Sauvegarde

Une sauvegarde journalière est effectuée et copiée à l'extérieur d'OVHcloud, vers un Datacenter de Scaleway Dedibox, et conservée 7 jours. Ces sauvegardes permettent une remise en place d'une plateforme à une date passée, dans la limite de la semaine (le coût de cette opération est en sus de l'abonnement).

Une copie hebdomadaire stockée 1 mois, et 12 copies mensuelles stockées un an sont ensuite effectuées. Les sauvegardes sont compressées et chiffrées. La base de données sauvegardé est également chiffrée.

Surveillance

Des traces sur l'ensemble des accès sont sauvegardés sur un an glissant et dès à présent consultables dans le back office de la solution

Gestion des certificats

Chaque client est responsable de fournir à Jamespot les certificats permettant la mise en œuvre des protocoles sécurisés.

Suivant les contraintes internes de chaque Client, plusieurs solutions peuvent être proposées pour mettre en place ces solutions y compris sur un sous domaine du Client.

Contrôle d'accès

Pour effectuer un contrôle d'accès strict, toute plateforme doit être déployée en mode 'fermé'. Seuls les administrateurs de la plateforme sont autorisés à créer de nouveaux comptes.

Jamespot propose de façon standard des modes d'accès externes s'appuyant sur des fournisseurs d'identités proposant l'un des protocoles suivants : OAuth2, SAML2, CAS ou LDAP.

Audits de sécurité

Jamespot doit s'assurer de faire pratiquer chaque année au moins un test de sécurité de type PenTesting BlackBox (tests sans accès fourni au préalable) / GreyBox (on fournit aux auditeurs les accès utilisateurs et administrateurs).

Jamespot s'engage à corriger les éventuelles failles remontées par ces tests dans les plus brefs délais.

Gestion des incidents liés à la sécurité

Jamespot s'engage à communiquer sur toute faille qui serait susceptible d'avoir compromis quelque information que ce soit.
La communication de ces incidents se fait dans le Groupe des Administrateurs de l'Écosystème.

Dans le cas où un problème spécifique à un client serait repéré, ce Client recevrait par l'intermédiaire de son CS la notification du problème. Un groupe de gestion de sécurité pourra être créé sur l'Écosystème afin de coordonner les efforts de Jamespot et du Client dans la gestion de l'incident.

Contactez Jamespot

Jamespot - Siège social

66 rue Marceau (Bâtiment C')

93100, Montreuil

+33 (0)1 48 58 18 01

info@jamespot.com

Jamespot - Pôle Ouest

2 Rue de la Mabilais

35000, Rennes