Politique de sécurité de Poka

Date d'entrée en vigueur : 2 septembre 2021

1. Applicabilité

L'objectif de la politique de sécurité de Poka est de définir les activités associées à la fourniture de services de sécurité qui protègent les systèmes d'information, les réseaux, les données, les bases de données et les autres actifs en relation avec les services logiciels. Tous les termes qui ne sont pas définis dans le présent document ont la signification qui leur est donnée dans le document Conditions générales de service pour les Clients.

2. Ressources humaines

2.1 **Vérification des antécédents.** : tous les candidats potentiels à l'emploi doivent passer avec succès une vérification standard des antécédents dans le cadre du processus d'embauche de Poka.

2.2 **Politiques.** : Tous les employés et le personnel contractuel de Poka sont tenus de signer les politiques internes pour la gestion des données du client, y compris la sécurité, la confidentialité et l'intégrité des données.

2.3 **Contrats de travail.** : Les contrats de travail de Poka comprennent des obligations standard de confidentialité et de non-divulgation pour les employés.

2.4 **Formation.** : Poka fournit à tous ses employés une formation obligatoire et annuelle sur la sécurité de l'information, mise à jour de temps en temps pour couvrir les nouvelles menaces de sécurité, les développements techniques ou les exigences légales applicables.

3. Modèle de fourniture des services logiciels

3.1 Les Services du Logiciel sont fournis sur la base d'une maintenance, de mises à jour et de corrections de bogues qui sont publiées ou déployées de manière continue. La nature automatisée de la livraison des services logiciels et de l'infrastructure, d'infrastructure, combinée à des versions fréquentes, exige que la sécurité soit intégrée dans le cycle de développement de Poka, y compris, mais sans s'y limiter, les pratiques suivantes en matière de sécurité, de confidentialité et d'assurance qualité identification des exigences, revue des exigences, revues de conception, contrôles de développement (ex. statique, revues de code), tests automatisés et manuels, analyses de vulnérabilité automatisées, gestion des changements et contrôles du déploiement.

4. Cryptage des données

4.1 Poka utilise les derniers protocoles et suites de chiffrement recommandés pour crypter les données en transit. Les données du client sont cryptées en transit à l'aide du protocole TLS (Transport Layer Security) 1.2/1.3 et cryptées au repos à l'aide du protocole AES 256 bits, l'un des algorithmes de chiffrement par blocs les plus puissants de l'industrie.

4.2 Poka suit de près l'évolution du paysage cryptographique afin de mettre à jour les services logiciels pour répondre aux nouvelles faiblesses dès qu'elles apparaissent pour répondre à celles-ci au fur et à

mesure qu'elles sont découvertes et mettre en œuvre les meilleures pratiques au fur et à mesure qu'elles évoluent et en tenant compte des besoins de compatibilité.

4.3 Poka impose le cryptage complet du disque pour tous les appareils de l'entreprise.

5. Isolement en contexte d’environnement d'applications partagé

5.1 Afin de garantir l'isolation des données, chaque Client dispose d'une instance dédiée, d'une base de données distincte et de magasins de données pour l'application des Services du Logiciel.

6. Modèles d'identité et authentification des utilisateurs abonnés

6.1 Le Client peut intégrer les Services du Logiciel aux répertoires d'identifiants de l'entreprise en utilisant le Markup Langage SAML v2 (Security Assertion Markup Language) pour conserver le contrôle total du processus d'authentification. Le client peut aussi automatiquement provisionner et déprovisionner les utilisateurs abonnés à l'aide du système Poka de gestion des identités multi-domaines (SCIM) - un standard ouvert utilisé par les fournisseurs d'identité et les services de Single Sign-On (SSO) pour gérer les comptes utilisateurs à travers les fournisseurs de services logiciels.

Le client peut également gérer les comptes des utilisateurs abonnés directement dans l'application de services logiciels. Les informations d'identification ne sont jamais stockées dans un format lisible par l'homme. Poka utilise un algorithme de hachage unidirectionnel sécurisé avec du salage (*salt*).

6.2 L'accès à l'instance du Client est régi par les rôles et les droits d'accès configurés par les administrateurs Poka désignés par le Client.

7. Pare-feu logique

7.1 Le Client peut choisir de restreindre l'accès à une plage d'IP spécifique afin que son instance ne soit accessible que dans les lieux physiques désignés et à travers leur VPN. Poka supporte également une politique d'accès par utilisateur abonné qui leur permet de se connecter en dehors des emplacements physiques désignés par le client.
Le Client peut également restreindre les pays à partir desquels ils sont autorisés à accéder à l'instance en utilisant la fonction de contrôle d'accès par géolocalisation IP de Poka.

8. Sauvegardes et reprise après sinistre

8.1 Les données du client sont stockées de manière redondante à plusieurs endroits dans les centres de données de l'hébergeur de Poka afin d'en assurer la disponibilité. Les données du client sont sauvegardées toutes les heures et répliquées en temps quasi réel dans la région secondaire désignée d'Amazon AWS. Les sauvegardes sont effectuées sans impact sur la disponibilité des données du client. Les opérations et l'infrastructure informatique de Poka peuvent donc être facilement récupérées et restaurées lorsque cela est nécessaire. Poka teste régulièrement ses mesures de reprise après sinistre afin de garantir une résolution adéquate d'un sinistre majeur.

9. Protection et journalisation du réseau

9.1 L'infrastructure informatique de Poka utilise une variété de contrôles pour assurer la protection et l'isolation des environnements, serveurs, conteneurs logiciels, sous-réseaux tels que le pare-feu logique, le

pare-feu d'application web, pare-feu logique, pare-feu d'application web, équilibreurs de charge d'application, etc. afin de garantir que seul le trafic autorisé provenant d'Internet ou du réseau de l'entreprise entre les serveurs est autorisé. Les journaux sont générés et analysés pour les événements de sécurité par le biais d'un logiciel de surveillance automatisé géré par l'équipe sécurité de Poka.

10. Gestion des vulnérabilités

10.1 Poka effectue des scans automatiques de vulnérabilité sur son environnement de production et remédie à toute découverte présentant un risque pour l'infrastructure informatique de Poka. De plus, des tests de pénétration dans l'environnement de production de Poka sont effectués chaque année par une tierce partie qualifiée.

11. Infrastructure d'hébergement

11.1 Poka utilise Amazon Web Services pour l'hébergement de toutes les instances du Client. Pour plus d'informations sur leur programme de certification et de conformité, veuillez visiter le site AWS Security et le site AWS Compliance.

12. Conformité

Poka détient les certifications de sécurité et de conformité suivantes pour les services logiciels :

12.1 **SOC 2 Type II.** Poka est conforme au Service Organization Controls (SOC 2) Type 2 de l'AICPA, un standard de l'industrie pour les attestations de sécurité des fournisseurs de logiciel service. Le rapport SOC 2 Type 2 confirme que le programme de sécurité de l'information et l'environnement de contrôle de Poka sont conformes aux critères de services de confiance développés et maintenus par l'AICPA. Le rapport couvre les contrôles que Poka a mis en place tant d'un point de vue organisationnel que technique, et comprend la gestion de l'accès, le cryptage, les modifications de code et le déploiement, la surveillance, la gestion des vulnérabilités, la gestion des incidents, la gestion des risques, la gestion des ressources humaines, la gestion des fournisseurs, etc. Le rapport SOC 2 Type 2 de Poka est disponible sur demande.

12.2 **Réponse de Poka au questionnaire du Cloud Security Alliance.** La Cloud Security Alliance (CSA) est une organisation à but non lucratif dirigée par une large coalition de praticiens de l'industrie, de sociétés et d'autres parties prenantes importantes. Elle se consacre à la définition des meilleures pratiques afin de garantir un environnement infonuagique plus sûr et d'aider les clients potentiels à prendre des décisions éclairées lors de la sélection d'un fournisseur de services en nuage. Le Security, Trust, and Assurance Registry (CSA STAR) et le questionnaire (CAIQ) v3.0.1 fournit un ensemble complet de questions que les organisations peuvent utiliser pour évaluer les processus de sécurité, de confidentialité et de conformité des fournisseurs de services. L'équipe de sécurité de Poka a compilé les réponses aux 294 questions du questionnaire. Ce document peut être consulté et téléchargeable ici et constitue une ressource précieuse pour comprendre comment Poka répond et dépasse les exigences énoncées par la CSA.

12.3 **Programme canadien des marchandises contrôlées.** Le Programme des marchandises contrôlées (PMC) a été lancé en avril 2001 afin de renforcer et de coordonner davantage les contrôles commerciaux de défense avec les États-Unis. Il s'agit d'un programme de conformité qui réglemente l'accès aux marchandises et technologies contrôlées, y compris les articles contrôlés par ITAR au Canada. Depuis 2017, Poka est enregistré (CGP #20710) et se conforme aux exigences du Règlement canadien sur les marchandises contrôlées et de la Loi sur la production de défense qui exige de mener des évaluations de

sécurité du personnel, de se préparer aux inspections, de développer des plans de sécurité et de signaler les brèches de sécurité.

12.4 **Traitement des données.** Poka se conforme aux lois de l'Union européenne sur la protection des données en ce qui concerne les mécanismes de transfert international de données. Dans cette mesure, l'accord de traitement des données (DPA) de Poka couvre le transfert des données du client.
en vertu du règlement (UE) 2016/679 du Parlement européen (RGPD).

12.5 **Gestion des violations de données et des incidents.** En cas de violation de la sécurité, Poka informera rapidement le Client de tout accès non autorisé aux Données du Client. Poka dispose d'un processus de gestion des incidents pour gérer l'ensemble du cycle de vie d'une violation de sécurité.