Incident Response Plan

Plan de réponse à incident / PCA / PRA

PUBLIC

v1.2 - October 2024

Table of Content

Context

- Pennylane is committed to guaranteeing the security of its data and maintaining its application in operational condition at all times. To that purpose, Pennylane maintains a series of documents related to information security, incident response, and business continuity. These documents aim to organize a swift response to incidents, prompt service restoration, and effective communication with all stakeholders.

  Pennylane s'engage à garantir la sécurité de ses données et à maintenir son application en état de fonctionnement à tout moment. À cette fin, Pennylane conserve une série de documents liés à la sécurité de l'information, à la réponse aux incidents et à la continuité des activités. Ces documents visent à organiser une réponse rapide aux incidents, une restauration rapide du service et une communication efficace avec toutes les parties prenantes.

- The incident response plan is annually reviewed and evaluated under the review of the Executive Committee and daily deployed under the control of a dedicated security team.

  Le plan de réponse à incident est revu et évalué annuellement sous le contrôle du Comité Exécutif et quotidiennement mis en œuvre par une équipe de sécurité dédiée.

- Pennylane is ISO:IEC 27001 certified and ensures that its Information Security Management System complies with the ISO 27001:2022 standard at all times and at all points, through policies and controls audited regularly internally as by independent experts.

  Pennylane est certifiée ISO:IEC 27001 et assure la conformité de son Système de Management de la Sécurité de l'Information, à tout moment et en tout point, à la norme ISO 27001:2022, grâce à des politiques et contrôles régulièrement audités en interne comme par des experts indépendants.

Certificate No 786660

Validity from 2024-09-10 to 2026-09-19 (click to check)

Plan

- This plan documents the Pennylane's standards for Incident Response, according to ISO 27001:2022 standard.

  Ce processus documente les standards de Pennylane en matière de réponse aux incidents, conformément à la norme ISO 27001:2022.

- The incident response plan applies to the entirety of Pennylane, including its employees, application, and information system. It encompasses all events that could potentially or realistically impact our information system, such as slowdowns, errors, security events, fraud or unavailability.

  Le plan de réponse à incident s'applique à l'intégralité de Pennylane, ses salariés, son application et son système d'information. Il concerne tous les événements pouvant avoir un impact potentiel ou réel sur notre système d'information (ralentissements, erreurs, événements de sécurité, fraude, indisponibilité, etc.).

Roles and responsibilities

- The roles and responsibilities of the people involved in the incident management process are defined.

  Les rôles et responsabilités des personnes impliquées dans le processus de gestion des incidents sont définis.

  - The Incident leader acts as a single source of truth and ensures that everyone is focused on the highest priority issues.

    Le responsable de l'incident fait office de source unique de vérité et veille à ce que tout le monde se concentre sur les questions les plus prioritaires.

  - The Communications Leader documents the timeline and communicates updates to stakeholders.

    Le responsable de la communication documente le fil des événements et communique les mises à jour aux parties prenantes.

- Contributors are domain experts or designated owners of a component or service, who evaluate and fix issues.

  Les contributeurs sont des experts du domaine ou des propriétaires désignés d'un composant ou d'un service, qui évaluent et résolvent les problèmes.

- Internal stakeholders are regularly trained internally and have the right level of knowledge required for their roles in incident response.

  Les responsables internes sont régulièrement formés en interne et disposent du bon niveau de connaissance nécessaire à leurs fonctions dans le cadre de la réponse à incident.

Report

- Pennylane deploys technical and human resources to ensure the internal or external reporting of any actual or suspected event that could have an impact on the security of our information system.

  Pennylane dispose de moyens techniques et humains internes et externes afin d'assurer la remontée tout événement avéré ou suspecté pouvant avoir un impact sur la sécurité de notre système d'information.

- Events may be reported internally, automatically as on demand, via real-time channels shared by all employees.

  Les évènements peuvent être remontés en interne, automatiquement comme à la demande, via des canaux en temps réel partagés par tous les employés.

- Each security event is reported internally using the communication channels defined in our policy and is escalated if necessary.

  Chaque événement de sécurité est remonté en interne selon les canaux de communication définis dans notre politique et font l'objet d'une escalade en cas besoin.

Assessment

- All events that could have an impact on the information system are assessed using a criticality level of service, based on the services priority matrix reviewed annually.

  Tous les évènements pouvant impacter le système d'information sont évalués selon le niveau de criticité défini par une matrice de priorité des services revue annuellement.

- Our internal SLA's are used to determine the criticality level of each incident and the mandatory resources required to ensure a rapid and effective response.

  Nos SLA internes permettent de déterminer pour chaque évènement le niveau de criticité de l'incident et les ressources obligatoires afin d'assurer une réponse rapide et efficace.

Detection measures

- Pennylane deploys a set of strict processes and controls to guarantee the confidentiality, integrity and availability of its customers' data, as well as to deal with incidents in these areas. Pennylane is capable of detecting an attack, analyzing it and, in the event of partial or total compromise, reverting to a previous state and removing any takeover artifacts.

  Pennylane déploie un ensemble de processus et de contrôles stricts afin de garantir la confidentialité, l'intégrité et la disponibilité des données de ses clients, comme pour faire face à des incidents dans ces domaines. Ainsi, Pennylane est capable de détecter une attaque, d'analyser cette dernière et en cas de compromission partielle ou totale, de revenir à un état précédent et de supprimer tout artéfact de prise de contrôle.

- Pennylane deploys a set of automatic controls on data access (ACL), on their integrity (application encryption ensuring protection against injection), generating either automatic alerts reviewed by engineers or data inconsistencies creating application errors reviewed by technical teams.

Pennylane déploie un ensemble de contrôles automatiques sur l'accès aux données (ACL), sur leur intégrité (chiffrement applicatif garantissant une protection contre l'injection), générant soit des alertes automatiques revues par des ingénieurs ou des inconsistances de données créant des erreurs applicatives revues par les équipes techniques.

Incident response

- Pennylane maintains a set of runbooks, ensuring that the key and essential steps are followed in order to guarantee an effective and appropriate response to incidents, thereby reducing the number of incidents and providing a faster response. The runbooks are reviewed at least once a year, as well as after each incident, in order to contribute to the continuous improvement of our process.

  Pennylane maintient un set de runbooks permettant de s'assurer que les étapes clés et essentielles sont suivies afin de garantir une réponse efficace et adaptée aux incidents en cours permettant ainsi de réduire le nombre d'incident et fournir une réponse plus rapide. Les runbooks sont revus annuellement a minima, ainsi qu'après chaque incident afin de concourir au processus d'amélioration continue de notre processus.

- Pennylane is capable of redeploying the complete application infrastructure (Infrastructure As A Code - IaaC). This, coupled with our ability to redeploy in a few minutes on our primary data center as well as on the secondary data centers distant from the primary, allows us to erase any attack while preserving our redundancy and availability capabilities intact. In addition, all data is continuously backed up, allowing for the restoration at any time of data dating back at least 5 minutes. The recovery time from a backup is 1 hour. The full recovery process is verified twice a year to improve its performance.

  Pennylane est capable de redéployer l'infrastructure complète de l'application (Infrastructure As A Code - IaaC). Ceci a pour effet, couplé à notre capacité à redéployer en quelques minutes sur notre data center primaire comme sur les data centers secondaires distants du primaire, d'effacer toute attaque en conservant intactes nos capacités de redondance et de disponibilité. En outre, toutes les données sont sauvegardées en permanence, ce qui permet de restaurer à tout moment des données datant d'au moins 5 minutes. Le temps de récupération d'une sauvegarde est de 1 heure.

Le processus de récupération complète est vérifié deux fois par an pour en améliorer les performances.

- The logs tracking the attacks remain consultable and protected on two distinct environments. These logs will thus precisely identify the cause of the attacks and therefore possibly take necessary measures, such as blocking the IPs of the attacker, blocking the attacked / attack accounts, renewing infrastructure and application secrets, correcting any vulnerabilities discovered.

  Les logs retraçant les attaques restent consultables et protégés sur deux environnements distincts. Ces logs permettront ainsi d'identifier précisément la cause des attaques et donc éventuellement de prendre les mesures nécessaires, comme bloquer les IPs de l'attaquant, bloquer les comptes attaqués / d'attaque, de renouveler les secrets d'infrastructure et applicatifs, de corriger les éventuelles vulnérabilités découvertes.

- For each incident, a post-mortem is drawn up to provide a better understanding of the root-causes of the incident and the measures implemented in response. These post-mortems are used to maintain logs of events that may affect our information system.

  Lors de chaque incident, un post-mortem est rédigé afin de mieux comprendre les root-causes à l'origine de l'incident ainsi que les mesures mises en œuvre pour y répondre. Ces post-mortem constituent ainsi le maintien des journaux des évènements pouvant affecter notre système d'information.

Communication

- Each incident is communicated internally via the communication channels defined in our policy.

  Chaque incident est communiqué en interne via les canaux de communication définis dans notre politique.

- External communication is promptly carried out for incidents that have had an impact on customers and partners, in accordance with Pennylane's contractual commitments and in compliance with our internal policies. A dedicated status page can be reached at https://status.pennylane.com/.

  Pennylane communique sans délai concernant les incidents ayant eu un impact pour ses clients et partenaires, en fonction des engagements contractuels pris par Pennylane et en conformité avec nos politiques internes. Une page de statut dédiée peut être accédée à l'adresse suivante : https://status.pennylane.com/.

Security Whitepaper

- Pennylane, ISO 27001 certified, is committed to the security of its customers' data, thanks to a series of technical and organizational measures and controls, detailed in our Security Whitepaper.

  Pennylane, certifiée ISO 27001, est engagée pour la sécurité des données de ses clients, grâce à une série de mesures et contrôles techniques comme organisationnels, détaillés dans notre Security Whitepaper.

Contact

Guillaume Gohin - Head of Information Security

guillaume.gohin@pennylane.com

security@pennylane.com