Lyyti Sécurité des informations

Un haut niveau de sécurité des informations est primordial pour nous.

Garder un haut niveau de sécurité des informations est primordial pour Lyyti. Quand vous nous faites confiance avec vos données événementielles, vous pouvez être assuré de leur sécurité.
Nous nous engageons à 100 % à respecter des normes de sécurité strictes grâce à plusieurs niveaux de protection.
Avec Lyyti, vous avez tous les outils nécessaires pour gérer les données de vos participants en toute sécurité.

L'Information Security Management System (ISMS) de Lyyti est conforme à la norme ISO/IEC 27001, englobant une gamme complète de mesures de sécurité. Ces mesures comprennent des contrôles, des politiques, des lignes directrices, des plans et des procédures, tous conçus pour protéger tous les aspects de nos opérations.

Lyyti traite les données exclusivement sur le territoire de l'UE, dans le strict respect du RGPD (2016/679). Les locaux de Lyyti ont été conçus et équipés pour respecter des règles de sécurité strictes.

Une équipe opérationnelle veille constamment au bon fonctionnement de Lyyti. L'équipe est présente 24h/24 et 7j/7, tous les jours de l'année.

Nous surveillons en permanence les environnements Lyyti pour identifier et corriger rapidement les vulnérabilités potentielles.

Tous les sous-traitants Lyyti sont soigneusement sélectionnés pour répondre à nos normes de sécurité strictes. Chaque sous-traitant est audité chaque année pour garantir sa conformité et une liste de ces partenaires est disponible sur le site web de Lyyti.

Le système de sauvegarde de Lyyti est robuste et englobe quatre niveaux opérationnels distincts et géographiquement séparés pour renforcer la sécurité.

Notre programme de sécurité du personnel exige que tous les employés suivent une formation annuelle sur la sécurité et la protection des données, garantissant ainsi que notre équipe maîtrise le maintien des normes les plus élevées en matière de sécurité des informations.

Le programme de sécurité Lyyti

La sécurité de l'entreprise englobe tous les aspects des opérations de l'entreprise. Les opérations de sécurité protègent les valeurs fondamentales de Lyyti, notamment les personnes, les données, la réputation, les biens, les actifs et l'environnement. L'une des principales responsabilités de la sécurité d'entreprise est d'améliorer la compétitivité de l'entreprise en garantissant la confidentialité, l'intégrité et la disponibilité de toutes les informations traitées.

Sécurité Physique

Les bureaux Lyyti sont équipés de serrures électroniques, de caméras de surveillance et de systèmes d'alarme antivol modernes et sont surveillés 24h/24 et 7j/7 par une société de sécurité externe. Chaque employé est tenu d'utiliser une clé électronique personnelle pour accéder au bureau. Tous les événements d'accès sont enregistrés, surveillés et peuvent être audités si nécessaire.

Le fournisseur d'hébergement des produits Lyyti adhère à plusieurs normes de sécurité reconnues par l'industrie, telles que ISO 9001, SOC 1 Type II, SOC 2 Type II, ISO 27001, ISO 22301 et PCI-DSS. Une liste complète des certifications du fournisseur d'hébergement peut être trouvée ici : https://upcloud.com/data-centres.

Classification des Données

Lyyti utilise un modèle de classification des données à trois niveaux. Les critères de classification des données dans ces niveaux, ainsi que les lignes directrices pour la gestion de chaque niveau de classification, sont décrits dans notre politique de sécurité. Les employés reçoivent régulièrement une formation sur ces procédures afin de garantir une bonne gestion des données.

Sécurité des terminaux

Tous les appareils électroniques accédant aux données de l'entreprise sont émis par l'entreprise et ont été renforcés de manière documentée. Ces appareils sont protégés contre différents types d'attaques par une solution XDR, surveillée 24h/24 et 7j/7. Lyyti utilise une solution MDM pour le contrôle des politiques et les corrections de ses terminaux, garantissant que tous les appareils sont sécurisés et chiffrés. Les utilisateurs sont tenus de signaler toute anomalie rencontrée lors de l'utilisation des appareils de l'entreprise.

La Politique d'Utilisation de Lyyti décrit l'acceptation de l'utilisation des ressources informatiques de l'entreprise et des actifs émis par l'entreprise et inclut le processus en cas de violation de la politique.

Formations de Sécurité

Tous les nouveaux employés doivent suivre une formation sur la sécurité et la confidentialité et réussir un examen dès leur premier jour de travail. Le contenu de la formation est périodiquement mis à jour et tout le personnel doit réussir ces mises à jour et réussir les examens correspondants dans les délais impartis, normalement au moins une fois par an. Les résultats de ces examens sont soigneusement surveillés et enregistrés à des fins de responsabilité.

Les développeurs sont formés chaque année aux pratiques de développement de logiciels sécurisés.

Cryptage des Données

Tous les appareils émis par l'entreprise sont cryptés. Les données clients sont toujours traitées sous forme cryptée, tant au repos qu'en transit.

Rôles de Sécurité dans l'Entreprise

Tous les rôles liés à la sécurité sont décrits sur les pages internes de l'entreprise Lyyti. Les canaux de communication sécurisés de l'entreprise incluent les coordonnées des titulaires du rôle de sécurité.

Description de la Politique

La politique de sécurité de l'entreprise comprend plusieurs sous-politiques et directives contrôlés, chacune étant attribué à un propriétaire désigné ayant la responsabilité principale du processus d'examen. Ces documents font l'objet d'un processus de révision annuel, ou plus si besoin. Ce système robuste garantit que les politiques et directives restent à jour et alignées sur les objectifs, les buts et les exigences statutaires de l'entreprise.

Violations de sécurité et Gestion des incidents

Lyyti maintient des processus documentés et des plans complets de gestion des incidents, assurant une surveillance continue des failles de sécurité avec des solutions sophistiquées. Tous les employés sont tenus de signaler rapidement toute violation détectée ou suspectée des politiques de sécurité de

l'information, toute tentative d'intrusion, toute violation de données, tout vol ou perte de matériel, ou tout autre événement et incident lié à la sécurité.

L'entreprise revoit régulièrement sa documentation de gestion des incidents et la rend accessible à tous les utilisateurs. La documentation décrit les protocoles de communication à suivre lors d'incidents, soulignant l'importance d'une réponse rapide pour protéger les services et les données de Lyyti.

Gestion des Risques

La gestion des risques fait partie intégrante du processus stratégique de Lyyti. Elle aide l'entreprise à atteindre ses objectifs en garantissant que les risques sont proportionnels à la capacité de risque.
Lyyti a identifié et documenté divers risques dans son registre des risques. Les risques ont été classifiés et analysés, et des plans d'action sont élaborés chaque année pour les atténuer. Le CTO, avec le PDG et l'équipe de conformité, est responsable de la formulation de la politique de gestion des risques et de l'évaluation des risques. L'équipe de direction approuve la politique de gestion des risques et revoit le processus chaque année.

Plan de Continuité des Activités (PCA) et Plan de Reprise d'Activité (PRA)

Lyyti dispose d'un Plan de Continuité des Activités (Business Continuity Plan) soutenu par un Plan de Reprise d'Activité après sinistre (Disaster Recovery Plan). Cela garantit que toutes les fonctions commerciales critiques peuvent continuer, pendant et après un incident grave. L’objectif principal du Plan de

Reprise d'Activité après sinistre est de minimiser les temps d'arrêt du système et les pertes de données. Ces documents sont régulièrement révisés pour garantir leur efficacité.

Analyses de vulnérabilité et Surveillance

Toute l'infrastructure Lyyti fait l'objet d'une surveillance opérationnelle 24h/24 et 7j/7, y compris l'infrastructure cloud, les réseaux, les points finaux et les propriétés des bureaux. Toutes les anomalies trouvées sont classées, documentées et traitées conformément aux politiques et directives.
Tous les environnements sont analysés contre les vulnérabilités en ligne, quotidiennement ou hebdomadairement, selon le système.

Tests d'Intrusions

Une société externe indépendante effectue des tests d'intrusion au moins une fois par an. Tous les résultats possibles sont documentés dans les systèmes électroniques et traités de manière appropriée.

Un résumé du dernier test d'intrusion, exécuté par Fraktal Oy en mars 2024. LINK.

Processus de Mise à Jour

Le matériel et les logiciels de production de Lyyti sont surveillés en permanence pour détecter les vulnérabilités potentielles. Les vulnérabilités classées comme « Critiques » ou « Élevées » selon le système d'évaluation de gravité CVSS v3.0 sont corrigées immédiatement, tandis que celles classées « Moyennes » ou inférieures sont corrigées dans le mois suivant la publication du correctif.

Pratiques de Sécurité des Employés et des Sous-traitants

Lyyti s'engage à maintenir les plus hauts niveaux de sécurité, en commençant par les processus d'embauche et d'intégration des employés et des sous-traitants. L'entreprise n'embauche que des personnes fiables et dignes de confiance et, de plus, chaque contrat comprend une clause de confidentialité pour protéger toute information sensible.

Pour garantir la sécurité, le personnel et les sous-traitants suivent une formation et doivent passer des évaluations avant de se voir accorder l'accès au système. L'accès est strictement réglementé en fonction des rôles professionnels, autorisant uniquement l'accès nécessaire aux données sensibles.

De plus, comme exigence de leur emploi ou de leur accord contractuel, tous les membres du personnel doivent adhérer aux politiques de sécurité de l'entreprise. Cet engagement strict envers les pratiques et politiques de sécurité aide Lyyti à protéger ses actifs, ses données et la confidentialité de ses clients.

Départ d'un Employé

Lorsqu'un employé quitte l'entreprise, un processus de départ détaillé, étape par étape, est suivi. Cela inclut, par exemple, la désactivation ou la suppression immédiate du compte utilisateur sur tous les systèmes utilisés et l'effacement des terminaux utilisés. Tous les appareils émis par l'entreprise sont répertoriés dans les registres d'actifs et sont collectés et gérés selon des procédures documentées.

Emplacement des données et sous-traitement

Toutes les données traitées par Lyyti, y compris le sous-traitement, sont traitées dans la région UE. Une liste des sous-traitants utilisés par Lyyti est disponible sur https://www.lyyti.com/en/subprocessors et tous les sous-traitants sont examinés chaque année.