HRWize en relation avec Moorepay

HRWize s'engage à fournir le plus haut niveau de service, de sécurité et d'assurance à ses clients. Pour plus de clarté sur la solidité de la plateforme et des services offerts, la relation entre HRWize et Moorepay (acquéreur de NaturalHR) est décrite ci-dessous.

HRWize est une entreprise canadienne qui met en œuvre et fournit une version en marque blanche de la plate-forme Moorepay, l'un des principaux fournisseurs de solutions de gestion des ressources humaines et de la paie basé au Royaume-Uni. Grâce à ce partenariat stratégique, HRWize bénéficie de toutes les capacités techniques et de sécurité de la plateforme Moorepay, tout en fournissant un support et des services localisés et bilingues aux organisations canadiennes.

Moorepay (en tant que fournisseur de la plateforme) et HRWize (en tant que fournisseur de services) maintiennent des certifications indépendantes selon ISO/IEC 27001, la norme internationale pour les systèmes de gestion de la sécurité de l'information. Cette double certification garantit que non seulement la plateforme sous-jacente, mais aussi les pratiques opérationnelles et les processus de prestation de services de HRWize répondent aux normes de sécurité les plus élevées.

Pour plus de transparence, le Moorepay Assurance Pack décrit le cadre de sécurité, les processus et les certifications en place pour protéger les données des clients. Les clients sont invités à demander des copies des certificats ISO 27001 respectifs ou toute autre information supplémentaire nécessaire à leurs processus d'assurance.

Ce document, ainsi que l'engagement permanent en faveur de la sécurité et de l'excellence des services, est destiné à assurer une confiance totale en HRWize en tant que partenaire technologique des ressources humaines.

Document 1 - Introduction au Moorepay Assurance Pack

Introduction

Chez Moorepay, l'information est notre métier et la sécurité de vos données est primordiale. Nous comprenons les obligations qui vous incombent pour assurer la sécurité des données qui nous sont confiées et nous nous engageons à travailler avec vous pour vous fournir les garanties dont vous avez besoin.

Lors de l'évaluation des risques d'un fournisseur ou des activités annuelles de diligence raisonnable liées à la sécurité de l'information, les organisations ont traditionnellement utilisé des questionnaires pour recueillir des informations. Les résultats obtenus par

cette approche manquent souvent du contexte nécessaire pour comprendre pleinement la posture de sécurité d'un fournisseur et, en fin de compte, ne fournissent pas les connaissances requises pour mener à bien les activités de diligence raisonnable à l'égard du fournisseur.

Le Moorepay Assurance Pack (MAP) est une compilation de documents et d'artefacts conçus pour offrir à nos clients un aperçu plus approfondi des pratiques de sécurité de Moorepay.

Le MAP comprend des attestations et des certificats indépendants, ainsi qu'une documentation décrivant les technologies, les processus et les contrôles que nous avons déployés pour protéger vos données et répondre aux exigences légales, réglementaires et contractuelles associées au traitement des données.

Contenu du MAP

Les documents et artefacts suivants sont inclus dans le MAP.

Système de gestion de la sécurité de l'information

Le système de gestion de la sécurité de l'information (SGSI) est un cadre de politiques et de procédures intégrant les contrôles administratifs, techniques et physiques déployés par Moorepay pour garantir le maintien de la confidentialité, de l'intégrité et de la disponibilité des données.

Le présent document du MAP vise à offrir un résumé concis de ces politiques, procédures et contrôles.

Aperçu de la protection des données

Une activité essentielle au sein de Moorepay est la nécessité de recueillir et de traiter des données personnelles sur les employés de nos clients, et ce conformément aux lois applicables en matière de protection des données et/ou de la vie privée des pays dans lesquels nous opérons.

Le règlement général sur la protection des données (RGPD) est utilisé comme norme de bonnes pratiques dans les pays où il n'existe pas de loi ou de règlement équivalent en matière de protection des données et/ou de la vie privée.

La législation locale peut nécessiter une mise en œuvre spécifique des politiques et des pratiques afin de s'aligner sur les exigences légales locales. Pour les opérations basées

au Royaume-Uni, Moorepay s'aligne sur le Règlement général sur la protection des données (RGPD).

Ce document MAP vise à consolider les informations pertinentes sur la mise en œuvre des pratiques et des politiques adoptées par Moorepay pour assurer le traitement sécurisé des données en avec les lois et les règlements applicables, comme indiqué ci-dessus.

Continuité des activités

Le document "Business Continuity MAP" vise à donner un aperçu de la planification de la continuité des activités de Moorepay et à fournir une illustration de haut niveau :

- l'engagement des dirigeants
- l'approche de la planification et de l'évaluation de la continuité des activités
- la garantie associée
- les analyses d'impact
- aperçu des tests

Aperçu de la sécurité des applications

Le plan d'action comprend une documentation qui décrit les dispositifs de sécurité conçus dans les produits propriétaires de Moorepay (tel que MoorepayHR/HRWize), ainsi que des informations sur les contrôles de sécurité déployés dans l'infrastructure sous-jacente et la sécurité physique en place dans les centres de données.

Votre MAP comprendra des informations sur les demandes spécifiques à votre prestation de services.

Aperçu de la sécurité du portail Moorepay

Moorepay Portal est notre plateforme numérique interentreprises disponible pour les clients de Moorepay, offrant une destination unique et sécurisée pour que les clients puissent s'engager avec nos équipes et nos processus.

La documentation MAP décrit les dispositifs de sécurité intégrés au produit.

Certification

Des copies des certificats suivants peuvent être fournies sur demande, là où les accords de confidentialité et de non-divulgation requis sont en place :

- ISO 27001:2013
- Cyber Essentials

Résultats des tests de pénétration

Moorepay passe des contrats avec des tiers indépendants pour effectuer les opérations suivantes :

- Tests de pénétration de l'infrastructure deux fois par an
- Tests de pénétration des applications avant publication

Les informations suivantes sont disponibles sur demande, là où les accords de confidentialité et de non-divulgation requis sont en place :

- Rapport de synthèse d'une tierce partie, fournissant une vue d'ensemble indépendante de la portée des tests ainsi que du nombre et de la gravité des vulnérabilités détectées.
- Attestation de remédiation produite en interne, fournissant une description de chaque vulnérabilité détectée ainsi que le plan de remédiation associé et la date d'achèvement prévue.

Document 2 - Système de gestion de la sécurité de l'information de Moorepay

Introduction

Ce document fait partie du Moorepay Assurance Pack (MAP) et doit être consulté avec tous les autres documents et artefacts inclus dans le MAP afin d'obtenir une compréhension globale des pratiques de sécurité de Moorepay.

Le système de gestion de la sécurité de l'information (SGSI) de Moorepay est un cadre de politiques et de procédures intégrant les contrôles administratifs, techniques et physiques déployés par l'organisation pour garantir à tout moment la confidentialité, l'intégrité et la disponibilité des données qui nous sont confiées.

Le présent document vise à décrire ces politiques et procédures afin de vous donner l'assurance que les bonnes pratiques sont respectées et que vos informations sont sécurisées.

Les mesures de sécurité prescrites par le SGSI intègrent les domaines de sécurité clés suivants :

Gestion des risques

Politiques de sécurité de l'information

- Organisation de la sécurité de l'information
- Sécurité des ressources humaines

Gestion des actifs

- Gestion des identités et des accès
- Cryptographie
- Sécurité physique
- Sécurité des opérations
- Sécurité des communications
- Acquisition, développement et maintenance des systèmes
- Sécurité des fournisseurs
- Gestion des incidents de sécurité

Continuité des activités et reprise après sinistre

Conformité

Pour chaque domaine clé, il existe un sous-ensemble d'exigences en matière de contrôle de sécurité et, dans le cadre de ces sous-ensembles, nous avons décrit les mesures mises en œuvre pour garantir la sécurité de vos données, en termes de politiques imposant les contrôles et de pratiques déployées pour atteindre les objectifs de ces politiques.

Gestion des risques

Évaluation des risques en matière de sécurité de l'information

La mise en œuvre de la stratégie de l'entreprise en matière de risques liés à la sécurité de l'information repose sur des méthodes formelles et reproductibles d'évaluation, de gestion et d'acceptation des risques.

Les actifs critiques sont classés par catégories pour l'évaluation des risques (par exemple, les fournisseurs, l'infrastructure informatique, les centres de données), et les

menaces, vulnérabilités et impacts associés sont pris en compte. Il s'agit d'une évaluation générale pour chaque catégorie d'actifs critiques.

L'identification du risque [de sécurité] peut également se faire à partir d'un certain nombre d'activités, telles que :

- les incidents et les faiblesses en matière de sécurité.
- les conclusions des évaluations et des audits internes ou externes en matière de [sécurité].
- les nouveaux projets ou les changements importants apportés aux projets existants. (tous les projets visant à traiter des informations confidentielles ou restreintes font l'objet d'une évaluation de l'impact sur la vie privée).
- la mise en œuvre de nouveaux produits ou services.
- la désignation d'un nouveau fournisseur. (l'évaluation des risques est réalisée avant d'accorder des droits d'accès à des tiers et doit inclure une évaluation de l'impact sur la vie privée lorsque des informations personnelles doivent être stockées, traitées ou transmises).
- une évaluation des menaces potentielles pesant sur les activités et les intérêts de l'entreprise.
- les modifications de la législation affectant les activités et les intérêts de l'entreprise.

Il incombe à tous les employés de Moorepay d'identifier et de rapporter tout risque dans leur domaine de responsabilité au propriétaire du risque désigné. Pour les risques liés à la sécurité, ils informeront le responsable de la sécurité et/ou les membres de l'équipe de sécurité qui les aideront à évaluer les risques.

Les risques de sécurité identifiés sont examinés dans le cadre d'une révision régulière de la gestion du SGSI et, lorsque cela s'avère nécessaire, une évaluation formelle des risques est entreprise par le gestionnaire de la sécurité.

L'évaluation des risques est documentée et soumise au RSSI pour examen.

Les risques sont calculés en utilisant une échelle de 1 à 5 pour l'impact (concernant la confidentialité, l'intégrité et la disponibilité des actifs/ressources d'information) multiplié par une échelle de 1 à 5 pour la vulnérabilité et une échelle de 1 à 3 pour la probabilité.

Des notes de risque sont établies pour le risque brut (non contrôlé) et le risque net (en tenant compte des contrôles actuellement déployés et de l'effet qu'ils ont sur la réduction des risques).

Traitement des risques liés à la sécurité de l'information

Pour chaque risque identifié, un plan de traitement des risques est formulé et formellement approuvé par le propriétaire du risque (généralement un membre de l'équipe de direction élargie).

Les options de traitement du risque sont sélectionnées sur la base de diverses considérations et comprennent les options suivantes :

- réduire - le niveau de risque est ramené à un niveau acceptable par l'introduction de contrôles
- conserver (accepter) - la décision est prise de conserver le risque sous sa forme actuelle
- éviter - la condition à l'origine du risque est évitée
- transfert - le risque est transféré à un tiers

Politique de sécurité de l'information

Orientation du gestionnaire en matière de sécurité de l'information

L'objectif de ce sous-ensemble de contrôles est de fournir une orientation et un soutien au gestionnaire en matière de sécurité de l'information, conformément aux exigences de l'entreprise et aux lois et règlements pertinents.

Politiques de sécurité de l'information

Moorepay dispose d'une politique documentée de gestion de la sécurité de l'information qui définit l'approche de l'organisation pour gérer ses objectifs en matière de sécurité de l'information.

Cette politique définit l'engagement stratégique de Moorepay en matière de gestion de la sécurité de l'information :

- garantit le maintien de la qualité du service
- répondre aux obligations contractuelles, légales et réglementaires de l'organisation
- répond aux besoins et aux attentes des clients et des autres parties intéressées.

La politique garantit que la gestion de la sécurité de l'information est traitée comme une partie intégrante des activités de gestion et qu'elle est poursuivie de la même manière et avec la même vigueur que les autres objectifs gestionnaires.

Les principaux objectifs de la politique de gestion de la sécurité de l'information sont les suivants :

- protéger les actifs informationnels de Moorepay et de ses clients contre toutes les menaces, qu'elles soient internes ou externes, délibérées ou accidentelles.
- minimiser les risques de dommages en cherchant à prévenir les incidents de sécurité et à réduire leur impact potentiel.

Le champ d'application de la politique de gestion de la sécurité de l'information englobe toutes les formes de sécurité de l'information liées aux actifs de l'entreprise, aux actifs de traitement de l'information, aux activités commerciales et aux informations confiées à Moorepay par ses clients sous toutes leurs formes, y compris les données stockées sur des ordinateurs, transmises par des réseaux, enregistrées sur papier ou conservées sur d'autres dispositifs de stockage.

Cette politique fixe les objectifs de sécurité minimale pour garantir que les informations ne sont accessibles qu'aux personnes autorisées à y accéder, que les informations que nous traitons et les méthodes utilisées sont exactes et complètes et que les informations que nous traitons sont mises à la disposition de toutes les parties prenantes autorisées lorsqu'elles en ont besoin.

La politique de gestion de la sécurité de l'information est étayée par un ensemble de politiques, de normes, de guides, de processus et d'autres documents spécifiques. Un résumé de cet ensemble de politiques est disponible sur demande, sous réserve d'approbation.

Lorsque, pour une raison quelconque, une politique de sécurité de l'information de l'entreprise ou une exigence normative ne peut être respectée, une demande formelle de dérogation doit être soumise par écrit pour approbation. Le fait de ne pas obtenir l'approbation d'une exception sera considéré comme une violation de la présente politique.

Toute infraction à la politique de sécurité de l'information de Moorepay peut faire l'objet d'une enquête de sécurité formelle et peut conduire à des mesures disciplinaires à l'encontre des personnes concernées.

Toutes les politiques et normes de sécurité de Moorepay sont communiquées à tous les employés et mises à la disposition des autres parties intéressées, le cas échéant.

Examen des politiques en matière de sécurité de l'information

Toutes les politiques et normes de sécurité de l'information sont réexaminées au moins une fois par an, à moins que des changements dans les opérations commerciales, la législation, les règlements, les engagements contractuels ou les codes de pratique ne nécessitent une modification plus rapide.

Toutes les politiques et normes de sécurité de l'information sont examinées et approuvées par le responsable de la sécurité.

Pour certaines politiques, une approbation supplémentaire peut être requise de la part d'experts en la matière ou de chefs de service.

Organisation de la sécurité de l'information Organisation interne

Les contrôles suivants ont été déployés afin d'établir un cadre de gestion pour initier et contrôler la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de Moorepay.

Rôles et responsabilités en matière de sécurité de l'information

Le responsable de la sécurité de l'information (CISO) a la responsabilité globale de l'information et de la cybersécurité au sein de Moorepay, sous l'autorité du des produits et des technologies (CPTO), et avec des rapports formels au directeur général (CEO), assurant ainsi une supervision exécutive.

L'équipe de direction de la sécurité, qui rapporte au CISO, est responsable des fonctions et des services de sécurité de l'information et de cybersécurité au sein de Moorepay. Une équipe dédiée de spécialistes de la sécurité (équipe de sécurité) rapporte à l'équipe de direction pour mettre en œuvre les pratiques de sécurité de l'information et de cybersécurité.

Moorepay a également mis en place un gestionnaire de services de sécurité (MSSP) qui fournit des services de sécurité supplémentaires, tels que des services de renseignement sur les menaces, de SIEM et de SOC.

L'équipe juridique et l'équipe de conformité et d'audit sont placées sous l'autorité du directeur juridique. Les principaux rôles et responsabilités sont les suivants :

- Le PDG et l'équipe de direction ont la responsabilité globale de la stratégie de sécurité de l'information de l'entreprise.
- L'équipe chargée de la conformité est responsable de la gestion du programme de certification ISO qui fait partie des activités de conformité de l'entreprise.

- L'équipe chargée de la conformité et de la confidentialité des données veille à ce que la législation pertinente fasse l'objet d'un suivi et à ce que les gestionnaires soient informés des modifications apportées à la législation.
- Les secteurs d'activité de Moorepay ont nommé des "champions de la sécurité" pour soutenir la stratégie de l'entreprise en matière de sécurité.
- Le processus de gestion de l'ISMS, le déploiement des politiques et la sensibilisation à la sécurité.
- La sécurité des ressources humaines relève de la responsabilité de l'équipe des ressources humaines de l'entreprise et des responsables hiérarchiques. Les vérifications préalables à l'embauche sont effectuées selon la norme reconnue au niveau national. Lorsque des contrats spécifiques avec des clients nécessitent une vérification plus poussée, celle-ci est effectuée par les unités opérationnelles par l'intermédiaire des autorités compétentes.
- La formation annuelle à la conformité (ACT) est assurée par l'équipe chargée de la conformité. L'objectif est de s'assurer que tous les employés de Moorepay comprennent les politiques de l'entreprise (y compris les politiques de sécurité et de confidentialité des données).
- L'équipe chargée de la conformité et de la confidentialité des données est chargée de veiller à ce que Moorepay respecte la législation sur la protection des données au Royaume-Uni et en Irlande.
- aux actionnaires l'assurance indépendante et objective que des contrôles internes appropriés sont en place, qu'ils sont solides et qu'ils sont respectés. L'équipe d'audit interne facilite l'évaluation annuelle du système de gestion de la sécurité de l'entreprise.
- La politique et les normes de sécurité physique pour les bâtiments de l'entreprise appartiennent au chef de la sécurité et au directeur des équipments.
- Les fonctions de gestion de la sécurité informatique et de la sécurité des réseaux sont détenues par le domaine d'activité Produits et technologies, avec l'appui de diverses équipes informatiques spécialisées. Les solutions, y compris l'évaluation et l'achat de
- Les produits de sécurité informatique (AV, détection d'intrusion, pare-feu, cryptage des données, etc.) sont convenus avec l'équipe chargée de la sécurité de l'information avant leur déploiement et leur mise en œuvre.

Séparation des tâches

Moorepay dispose d'une politique documentée de séparation des tâches. Cette politique détaille les exigences relatives aux rôles et aux responsabilités afin de réduire

la dépendance à l'égard des personnes clés et de prévenir au minimum les erreurs et les fraudes.

La politique prévoit qu'une séparation adéquate des tâches et des responsabilités de contrôle doit être établie et maintenue dans tous les domaines fonctionnels de Moorepay. En général, les responsabilités en matière de conservation, de traitement et d'exploitation, et de comptabilité sont séparées afin de favoriser un examen et une évaluation indépendants des opérations de Moorepay.

Voici quelques exemples de fonctions qui doivent faire l'objet d'une séparation des tâches.

- Les administrateurs de systèmes ne doivent pas exercer de fonctions d'administrateur de sécurité. L'autorisation de création de comptes d'administrateur doit être enregistrée.
- La fonction d'administration du réseau doit être une fonction distincte de celle de la gestion de l'infrastructure. Cela garantira que l'accès de bout en bout aux données (y compris les données sensibles) n'est possible que par la collusion et réduira donc le risque d'utilisation abusive de l'infrastructure.
- Les équipments d'information de Moorepay.
- Les employés exerçant des fonctions financières ne doivent pas être en mesure d'effectuer toutes les étapes d'une transaction. Par exemple, les employés ne doivent pas être en mesure de créer, d'approuver et d'effectuer toutes les étapes d'une transaction.
- Les activités d'administration de la base de données et du système d'infrastructure (par exemple, l'administrateur de l'hôte du serveur) ne doivent pas être effectuées par la même personne ou la même équipe.
- Les administrateurs de sécurité ne doivent pas avoir accès aux privilèges d'administration de la base de données.
- Le personnel chargé du développement et de la maintenance des logiciels ne doit pas avoir d'accès croisé aux opérations informatiques (environnements de production), y compris l'administration des bases de données, l'administration du réseau et l'administration du système (infrastructure).
- Les administrateurs de sécurité et les administrateurs de pare-feu ne doivent pas avoir de comptes d'accès privilégiés sur les systèmes de production de l'infrastructure (par exemple, rôles opérationnels), à l'exception des technologies de sécurité/pare-feu, IDS/IPS, etc.

Mises à jour juridiques et réglementaires

Les équipes produits de Moorepay surveillent l'impact des réglementations et des lois sur les services et les produits que nous proposons, notamment dans les domaines du travail et de l'emploi, de la paie, des avantages sociaux, de la mobilité mondiale, du recrutement, de la confidentialité et de la protection des données, entre autres, au Royaume-Uni et en Irlande.

L'équipe de Moorepay chargée de la conformité surveille et suit les obligations légales et réglementaires de l'entreprise, y compris les exigences relatives au SMSI.

Contact avec des groupes d'intérêt

Notre plan stratégique de produits est influencé par le marché des ressources humaines et de la paie, les tendances du secteur, les changements technologiques, mais surtout par nos clients, par l'intermédiaire de nos groupes d'utilisateurs et de nos groupes d'intérêts spéciaux.

Moorepay reçoit des renseignements sur les menaces et d'autres informations sur la sécurité de diverses sources, y compris, mais sans s'y limiter, les suivantes :

- des informations sur les vulnérabilités et les mises à jour logicielles des principaux fournisseurs
- abonnement au Centre national de cybersécurité - Partenariat pour le partage d'informations sur le cyberespace (NCSC CISP)
- Évaluation de la cybersécurité par Bitsight
- Plate-forme de veille sur les menaces de Digital Shadows
- Renseignements sur les menaces fournis par notre fournisseur de services de sécurité gérés (MSSP) via le centre d'opérations de sécurité (SOC).

L'inscription à divers groupes d'intérêt et forums spécialisés dans l'information sur la sécurité se fait également sur une base ad hoc au sein de l'équipe de sécurité, des équipes techniques et des niveaux de gestion. Des lignes de communication claires sont disponibles pour le rapport des préoccupations et la notification des nouvelles menaces à l'équipe de sécurité.

La sécurité de l'information dans la gestion de projet

Le comité consultatif technique (TAB) valide les propositions de nouvelles technologies. L'implication de l'équipe de sécurité dans le processus TAB garantit :

- l'intégration de contrôles de sécurité et de protection de la vie privée dans la solution proposée la conformité aux politiques de sécurité et de protection de la vie privée
- l'achèvement satisfaisant de l'évaluation de la sécurité et de la confidentialité des données comme preuve de la conformité aux exigences en matière de sécurité et de confidentialité

Les représentants de l'équipe de sécurité assistent à des sessions hebdomadaires de planification et d'examen (ship rooms) pour s'assurer que la sécurité est informée de tous les développements d'applications et changements d'infrastructure à venir et qu'elle est en mesure de donner des conseils sur les points de risque potentiels et les meilleures pratiques en matière de sécurité.

Appareils mobiles et travail à distance Politique en matière d'appareils mobiles

La politique de sécurité de Moorepay en matière d'informatique mobile et de travail à domicile couvre les exigences relatives à l'utilisation des appareils mobiles. Cette politique s'applique à tous les employés et aux tiers.

les personnes qui utilisent des appareils mobiles (c'est-à-dire des téléphones mobiles, des tablettes, des ordinateurs portables, des ordinateurs macs ou d'autres équipements informatiques facilement transportables) et qui bénéficient d'un accès autorisé aux informations et aux systèmes de traitement de l'information.

- Les employés doivent s'assurer que la politique d'utilisation acceptable des systèmes d'information de Moorepay et la norme de traitement de l'information sont appliquées lors de l'utilisation d'appareils mobiles.
- Tous les appareils autorisés à se connecter aux réseaux et à y accéder doivent être dotés d'une solution de gestion des appareils mobiles appropriée afin de pouvoir être gérés à distance et d'effacer les données si nécessaire.
- Les appareils mobiles doivent être protégés par un logiciel de cryptage approuvé. Les mots de passe doivent être conformes à la politique de Moorepay relative aux mots de passe des utilisateurs.
- Les employés ne doivent pas permettre à un utilisateur non autorisé d'accéder à un appareil Moorepay, y compris les membres de leur famille.
- Les employés doivent :
- Garder les appareils mobiles utilisés à des fins professionnelles cachés lorsqu'ils ne sont pas utilisés et ne pas stocker de dispositifs d'authentification à facteurs

multiples ou tout autre dispositif d'authentification fourni avec les appareils mobiles utilisés pour l'accès.

- Garder les appareils mobiles en leur possession et dans la ligne de mire chaque fois que possible, en faisant attention dans les lieux publics tels que les aéroports, les gares, les hôtels ou les restaurants.
- Veillez à protéger la confidentialité et à minimiser le risque d'exposition en limitant les informations qui peuvent être vues par d'autres personnes.
- Veillez à ce que les conversations confidentielles et les appels téléphoniques aient lieu dans des zones privées, à l'écart des autres personnes. Le port d'un casque ou d'écouteurs est obligatoire pour garantir la confidentialité des conversations professionnelles.
- Désactivez l'équipments Bluetooth lorsqu'il n'est pas indispensable et/ou réglez-le sur "caché" pour éviter que les appels ne soient interceptés.
- En cas de perte ou de vol d'un appareil mobile, signalez-le à la
- Moorepay Service Desk immédiatement pour s'assurer que le compte est désactivé et les données effacées.

Tous les ordinateurs portables fournis sont dotés d'un système de sécurité standardisé, qui comprend les éléments suivants :

- logiciel anti-malware
- les pare-feu personnels.
- cryptage de l'ensemble du disque
- fonctionnalité de l'utilisateur final contrôlée par une politique de groupe (par exemple, pas d'accès administrateur ou de possibilité d'installer des logiciels)

Tous les appareils de téléphonie mobile sont dotés d'un système de cryptage de l'ensemble du disque et l'utilisation d'un code PIN ou d'un mot de passe est obligatoire. L'accès aux informations et aux systèmes n'est pas autorisé tant que ces contrôles de sécurité obligatoires n'ont pas été confirmés.

Moorepay a déployé un service de gestion des appareils mobiles (MDM) et de gestion des applications mobiles (MAM) pour permettre la gestion centralisée des appareils mobiles de l'entreprise. La fonctionnalité du service comprend, sans s'y limiter, les composants de sécurité mobile suivants :

- effacement à distance de l'appareil
- le déploiement de politiques de sécurité
- le déploiement de logiciels
- la confirmation des niveaux de logiciels et des politiques de sécurité

- la prévention et le contrôle de l'accès aux informations et aux systèmes de Moorepay

Travail à distance

La politique de sécurité de Moorepay en matière d'informatique mobile et de travail à domicile couvre les exigences relatives au travail à distance.

Tous les employés travaillant à domicile ou dans d'autres lieux éloignés doivent s'assurer que les informations et les appareils sont utilisés de manière conforme :

- la politique d'utilisation acceptable des systèmes d'information de Moorepay.
- les politiques et normes de contrôle d'accès.
- les politiques et procédures pertinentes en matière de classification des informations.
- toutes les exigences légales et réglementaires.

Lorsqu'ils travaillent à domicile ou à distance, les employés doivent respecter les exigences minimales suivantes.

- Soyez extrêmement prudent lorsque vous utilisez des réseaux sans fil publics ou ceux fournis, par exemple, dans les hôtels, les cafés ou les centres de conférence. Les employés doivent veiller à préserver leur vie privée dans de telles circonstances et à s'assurer que les connexions sont convenablement cryptées et sécurisées.
- Mettre en œuvre des mesures appropriées de protection de la vie privée afin de réduire le risque de divulgation involontaire d'informations à des spectateurs ou à des voisins (par exemple, par les fenêtres, les portes ouvertes et les conversations entendues) ou en travaillant dans des espaces publics tels que les trains, les avions, les restaurants ou les bars.
- Veiller au respect de toutes les politiques et procédures de Moorepay en matière de santé et de sécurité.
- Veiller au respect de toutes les exigences légales, réglementaires, internes et contractuelles pertinentes.
- Éliminer les informations et les dispositifs en toute sécurité et dans le respect de la législation en vigueur.

Moorepay élimination sécurisée des déchets

- Conservez les documents imprimés de l'entreprise hors de vue et en lieu sûr.

- Le personnel ne doit pas se connecter à Moorepay à partir d'un réseau domestique, sauf si des contrôles de sécurité approuvés sont en place, tels que les exigences en matière de logiciels malveillants et de pare-feu.
- En cas de cessation d'emploi, la procédure de départ de Moorepay doit être respectée et tous les équipements et informations doivent être restitués.
- Moorepay peut entreprendre des audits et des contrôles de sécurité.
- Tout le personnel travaillant à distance doit s'assurer qu'une sauvegarde régulière des informations est effectuée et que les sauvegardes sont protégées par des moyens tels que le cryptage.
- Seuls les utilisateurs autorisés peuvent travailler à domicile.

La technologie est déployée pour restreindre l'accès au réseau de l'entreprise, des agents locaux sont installés sur les appareils de connexion qui sont intégrés à l'Active Directory de Moorepay. Les appareils utilisés pour se connecter doivent avoir la configuration requise pour s'authentifier, ce qui, avec l'authentification de l'utilisateur, offre une pseudo-authentification à deux facteurs (quelque chose que vous avez et quelque chose que vous connaissez). Le logiciel vérifie que l'appareil connecté est conforme aux politiques de l'entreprise avant d'autoriser l'établissement de la connexion.

Le logiciel établit une connexion cryptée de réseau privé virtuel (VPN) entre l'appareil de connexion et le réseau de l'entreprise.

Des normes d'entreprise existent et doivent être respectées pour le traitement et l'élimination des informations dans le cadre du travail à domicile.

La possibilité d'ajouter des imprimantes personnelles aux appareils de l'entreprise est limitée et l'impression à domicile doit être autorisée et activée. Les ressources d'impression des centres de services sont utilisées là où c'est possible afin de limiter le nombre d'impressions hors site et le stockage de copies papier d'informations.

Les utilisateurs autorisés à imprimer doivent respecter les normes de Moorepay en matière de traitement de l'information et, le cas échéant, disposer d'un équipement spécialisé pour stocker et détruire les copies papier de l'information.

Sécurité des ressources humaines

Avant l'emploi

Les contrôles suivants ont été mis en place pour s'assurer que les employés et les contractants comprennent leurs responsabilités et qu'ils sont aptes à remplir les fonctions pour lesquelles ils sont envisagés.

Dépistage

La sélection des employés est obligatoire avant de leur donner accès aux actifs de l'entreprise. La vérification des antécédents de tous les candidats à l'embauche, des contractants et des utilisateurs tiers est effectuée conformément aux lois et réglementations locales en vigueur et aux exigences de l'entreprise.

Les exigences de Moorepay en matière de vérification sont les suivantes

- contrôle du droit au travail
- contrôle de la preuve de résidence
- contrôle de probité financière
- cinq ans d'historique d'activité
- vérification du casier judiciaire

En fonction du rôle de l'employé, des contrôles supplémentaires sont effectués conformément aux exigences contractuelles de notre client en matière d'autorisations spécifiques.

Si un candidat ne satisfait pas à l'un des contrôles suivants, la politique de Moorepay est de ne pas l'embaucher :

- droit au travail
- CCJ insatisfaites
- les condamnations non purgées (à l'exception des délits routiers, sauf s'ils ont donné lieu à une déchéance et qu'un permis valide est nécessaire pour exercer leur fonction).

Si le candidat échoue à un autre contrôle, un examen plus approfondi sera entrepris par les RH et les parties prenantes concernées et une décision sera prise sur la manière de procéder au cas par cas.

Conditions d'emploi

Dans le cadre de l'obligation d'emploi, les employés, les sous-traitants et les utilisateurs tiers doivent accepter et signer les conditions du contrat de travail, qui précisent leur responsabilité et celle de l'organisation en matière de sécurité de l'information.

Le contrat de travail type comprend les clauses suivantes, mais ne s'y limite pas :

- Transfert de technologie
- Conflit d'intérêts
- Conduite et devoirs
- Informations confidentielles
- Protection des données
- Non-concurrence et non-sollicitation
- Surveillance des employés

Tout manquement aux conditions d'emploi est traité par la procédure disciplinaire propre à Moorepay et adaptée à la législation locale.

Pendant l'emploi

Les contrôles suivants ont été mis en place pour s'assurer que les employés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils les assument.

Responsabilités du gestionnaire

Les divisions commerciales et les départements locaux sont responsables de la création de procédures et d'instructions de travail appropriées pour s'aligner sur les politiques et les normes de l'entreprise.

Les gestionnaires sont tenus de s'assurer que chaque employé relevant de leur compétence suit et réussit la formation annuelle en matière de sécurité et de conformité et que, là où c'est nécessaire, une formation complémentaire est dispensée pour s'assurer que les employés possèdent les connaissances requises.

Les gestionnaires reçoivent une formation complémentaire pour s'assurer qu'ils comprennent leurs exigences et celles de leurs équipes en matière de sécurité de l'information.

Il incombe aux gestionnaires d'ouvrir une enquête formelle là où l'on soupçonne qu'un employé ne respecte pas leurs exigences en matière de sécurité de l'information.

Sensibilisation, éducation et formation à la sécurité de l'information

Un cadre de formation à la sécurité en ligne est fourni et tous les employés, sans exception, sont tenus de le suivre chaque année. Cette formation fait également partie

du processus d'intégration des employés et doit être suivie dans les quatre semaines suivant leur entrée en fonction.

Les objectifs du cadre de formation e-learning sont les suivants :

- respecter les politiques et les normes de sécurité de Moorepay
- participer à la continuité des activités de Moorepay et à la planification en cas de catastrophe
- comprendre les concepts clés de la protection des données qui sont importants pour l'exercice de votre fonction
- respecter les politiques de Moorepay en matière de lutte contre la corruption et de conformité de l'entreprise
- respecter l'approche de Moorepays visant à encourager l'égalité, la diversité et la dignité
- accepter la responsabilité collective en matière de santé et de sécurité au travail

Tous les membres du personnel sont testés sur leurs connaissances de chaque sujet et doivent obtenir une note de 80% pour compléter chaque module.

Le matériel de formation est revu au moins une fois par an.

Pour compléter la formation annuelle, l'équipe de sécurité fournit régulièrement du matériel supplémentaire axé sur des aspects importants de la sécurité, offrant des conseils supplémentaires sur la manière d'appliquer les bonnes pratiques et de travailler d'une manière plus sûre.

Les besoins supplémentaires en formation sont identifiés au moyen d'une matrice de compétences régulièrement mise à jour. Les formations suivies sont enregistrées dans le système d'évaluation des performances.

Les divisions et les services locaux sont chargés de mettre en place des procédures appropriées.

et des instructions de travail afin de garantir que les activités de traitement et de soutien sont menées de manière cohérente et conformément aux politiques applicables de l'entreprise.

Procédure disciplinaire

Moorepay a mis en place une politique disciplinaire formelle afin d'encourager tous les employés à atteindre et à maintenir des normes de conduite, d'assiduité et d'aptitude. Cette politique permet à l'entreprise et à ses représentants d'agir de manière efficace,

cohérente et équitable lorsqu'ils traitent de questions telles que la mauvaise conduite, le manque d'assiduité et l'incapacité.

Moorepay se réserve le droit de mettre en œuvre la procédure disciplinaire à n'importe quel stade, comme indiqué dans la politique, en tenant compte des actions présumées d'un employé.

Elle s'applique à tous les employés qui travaillent pour Moorepay ou l'une de ses filiales au Royaume-Uni et en Irlande. Elle s'applique à tous les employés permanents et temporaires ainsi qu'aux sous-traitants.

Des mesures disciplinaires peuvent être prises en cas de faute ou d'incapacité.

Les enquêtes sont menées par les gestionnaires et les représentants des ressources humaines concernés.

Les mesures disciplinaires sont déterminées en fonction des résultats de l'enquête et conformément à la politique de l'entreprise.

Licenciement et changement d'emploi

Les contrôles suivants ont été mis en place pour garantir la sécurité de l'information

que les exigences sont comprises et que les informations de Moorepay et de ses clients sont protégées lorsque la résiliation est effectuée.

Cessation ou changement des responsabilités professionnelles

La politique de Moorepay concernant les employés qui quittent l'entreprise est mise en œuvre pour s'assurer que les responsabilités des employés après leur départ sont mises en évidence. Au minimum :

- tous les actifs sont restitués et le gestionnaire des départs soumet un formulaire d'autorisation permettant le paiement final.
- l'accès est révoqué et les comptes d'utilisateurs sont désactivés à l'heure et à la date voulues.
- un entretien de sortie est réalisé, et le sortant doit signer un accord de confidentialité réitérant qu'il maintiendra la confidentialité.

Gestion des actifs

Responsabilité des actifs

Les contrôles suivants ont été mis en place pour identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection.

Inventaire des actifs

Une CMDB ou un registre est utilisé pour enregistrer et gérer les détails des actifs. Une combinaison de découverte automatique et d'intervention manuelle par les actifs est utilisée pour maintenir les enregistrements.

Les actifs informatiques sont enregistrés dans le système de gestion des services informatiques ; les informations enregistrées sont les suivantes :

- nom de l'actif
- numéro d'actif
- le type d'actifs (par exemple, serveur, ordinateur portable, routeur)
- propriétaire désigné
- le statut (par exemple, production, développement, en attente d'élimination)

Propriété des actifs

Tous les actifs informationnels traités au sein de Moorepay ont un Actif Informationnel désigné (IAO) qui doit être une personne senior/responsable impliquée dans le fonctionnement de la fonction commerciale concernée.

Leur rôle est de comprendre quelles informations sont détenues, comment elles sont reçues, supprimées et conservées, qui y a accès et pourquoi. Actif, ils peuvent reconnaître la valeur et les risques liés au cycle de vie de leurs actifs informationnels et s'assurer qu'ils sont traités conformément aux politiques de sécurité de Moorepay.

Les Actifs contribuent formellement à l'évaluation des risques pour la confidentialité, l'intégrité et la disponibilité de leurs actifs informationnels.

La responsabilité de la mise en œuvre des contrôles quotidiens relatifs à leurs actifs informationnels peut être déléguée, mais l'IAO désigné reste responsable. Aux fins de l'application de la classification des informations, un IAO peut également être l'auteur, le créateur ou le destinataire d'une information.

Utilisation acceptable des actifs

La politique d'utilisation acceptable des systèmes d'information fait partie du cadre de la politique de sécurité de l'information de Moorepay. L'objectif de cette politique est d'énoncer les exigences permettant de s'assurer que les contrôles de sécurité sont

appliqués, afin de protéger les systèmes de Moorepay qui stockent ou sont utilisés pour accéder à l'information. Par conséquent, l'utilisation acceptable est définie de manière à garantir à toutes les parties prenantes de Moorepay que les informations sont protégées de manière adéquate.

Les incidents de sécurité de l'information (où une utilisation inacceptable des systèmes est soupçonnée ou s'est produite) doivent être signalés [immédiatement] à l'aide de la procédure de rapport d'incident de sécurité de l'information.

L'accès aux systèmes de Moorepay ne doit pas être tenté sans autorisation appropriée (conformément aux exigences de Moorepay en matière de contrôle d'accès).

Moorepay surveille l'utilisation de ses systèmes d'information à des fins de sécurité. La politique d'utilisation acceptable des systèmes d'information couvre les domaines suivants :

- utilisation générale des systèmes d'information de Moorepay
- la protection des informations confidentielles ou à diffusion restreinte
- l'utilisation sécurisée d'Internet
- utilisation sécurisée des communications électroniques
- la sécurité physique
- mots de passe
- supports de stockage amovibles
- utilisation acceptable des logiciels
- la configuration sécurisée des systèmes d'information de Moorepay
- le contrôle des systèmes d'information de Moorepay

La politique d'utilisation acceptable des systèmes d'information suit les contrôles associés définis dans les politiques et procédures suivantes de Moorepay :

- Politique en matière d'appareils mobiles et de travail à distance
- Politique du bureau clair/de l'écran clair
- Politique en matière de mot de passe
- Politique en matière de cryptographie

Procédure de rapport sur les incidents de sécurité de l'information

Rendement des actifs

Une politique globale de départ est mise en œuvre pour s'assurer que les responsabilités des employés après leur départ sont mises en évidence.

L'attribution des actifs est suivie dans le système de billetterie de l'entreprise, le processus de départ déclenche la création d'un ticket enfant pour que l'assistance informatique locale s'engage avec le gestionnaire hiérarchique du départ et s'assure que tous les actifs sont identifiés et restitués.

Ce n'est que lorsque tous les actifs ont été restitués que le gestionnaire des départs soumet un formulaire d'apurement permettant le paiement final.

Classification des informations

Les contrôles suivants ont été mis en place pour garantir que les informations bénéficient d'un niveau de protection approprié en fonction de leur importance pour Moorepay.

Classification des informations

Moorepay dispose d'une politique documentée de classification et de propriété des informations. L'objectif de cette politique est d'identifier et de mettre en œuvre des contrôles adéquats et efficaces de traitement et de protection des informations, en fonction de la sensibilité des informations traitées. Le but est de s'assurer que les précieuses informations commerciales et personnelles utilisées au sein de Moorepay et les informations confiées à l'organisation par ses clients sont protégées de manière appropriée tout au long de leur durée de vie.

Une catégorie de classification doit être appliquée à toutes les informations générées.

Cette politique s'applique à la fois aux utilisateurs (employés, employés d'agences de travail temporaire, fournisseurs, partenaires commerciaux, personnel contractuel et clients) et aux systèmes appartenant à l'entreprise qui traitent tout type d'information sensible et s'étend aux informations détenues sur papier et sous forme électronique.

Cette politique s'appuie sur la norme relative au traitement de l'information, qui définit les règles de traitement de l'information à chaque étape de son cycle de vie.

Les principes suivants s'appliquent à tous les actifs informationnels gérés par Moorepay ou en son nom :

- la classification d'un actif informationnel doit indiquer s'il peut être communiqué à l'extérieur de l'organisation et traduire les besoins de protection et de traitement de la sécurité lors du traitement interne de l'information.

- tous les actifs d'information majeurs doivent être comptabilisés, enregistrés et un propriétaire d'actifs d'information (IAO) doit être désigné pour veiller à ce qu'une protection adéquate soit maintenue.
- le niveau de contrôle à exercer doit être basé sur la classification des informations telle qu'elle est détaillée ci-dessous.
- Les propriétaires d'actifs informationnels et les employés doivent :
- classer les actifs informationnels et les équipments de traitement de l'information conformément à la présente politique.
- étiqueter de manière appropriée les actifs informationnels et les équipments de traitement de l'information en fonction de leur classification.
- traiter et protéger les informations en fonction de leur classification et conformément aux exigences des clients et aux normes de Moorepay en matière de traitement de l'information.

Les informations doivent être classées dans l'une des quatre catégories suivantes :

- Public
- Information librement disponible. Elle est identifiée là où il n'y a pas d'étiquette de document ou par toute étiquette de document qui ne correspond à aucune des classifications suivantes.
- Restriction de l'entreprise pour usage interne uniquement
- Les informations classées comme réservées à l'entreprise pour un usage interne peuvent être communiquées à tout employé de Moorepay ou à tout contractant autorisé et approuvé. Dans certaines circonstances, les informations classées dans cette catégorie peuvent être communiquées à des organisations tierces, là où un accord de non-divulgation existe entre les parties et Moorepay.
- Confidentiel pour l'entreprise ou le client
- Toutes les informations personnelles identifiables manipulées, traitées ou stockées par Moorepay ou au nom de Moorepay, ou confiées à Moorepay par ses clients.
- Secret d'entreprise
- Les informations qui, si elles étaient divulguées, auraient un impact significatif sur la réputation et le succès commercial de Moorepay.

La classification doit être basée sur :

- les exigences légales (qui peuvent affecter les contrôles de confidentialité, d'intégrité et/ou de disponibilité),
- valeur et criticité (affectant les contrôles d'intégrité et/ou de disponibilité)

- la sensibilité à la divulgation ou à la modification non autorisée (affectant les contrôles de confidentialité).

Étiquetage des informations

Conformément à la politique de Moorepay en matière de classification et de propriété de l'information et à la norme associée sur le traitement de l'information, les contrôles suivants sont stipulés :

- Les propriétaires d'actifs informationnels (IAO) et les employés doivent étiqueter de manière appropriée les actifs informationnels et les équipments de traitement de l'information en indiquant leur classification.
- Les informations doivent être classées et étiquetées conformément à la norme relative au traitement de l'information, afin de refléter leur criticité et leur classification de sécurité.
- les documents classés comme étant à accès restreint pour l'entreprise doivent avoir un pied de page sur toutes les pages et dans les registres d'actifs pour les systèmes de traitement de l'information.
- Les documents classés comme confidentiels pour l'entreprise ou le client doivent être accompagnés d'un pied de page sur toutes les pages, dans les dossiers manuels et dans les registres d'actifs pour les systèmes qui traitent ou stockent des données confidentielles.

Gestion des actifs

Moorepay dispose d'une norme documentée sur le traitement de l'information. L'objectif de cette norme est d'assurer la protection de ses actifs informationnels, de ses ressources système et de ses informations, et de répondre aux exigences légales et réglementaires de Moorepay, de ses clients et des autres parties prenantes.

La politique de Moorepay est de mettre en œuvre des mesures de contrôle appropriées pour protéger les données confidentielles ou restreintes contre la destruction, l'endommagement, la modification ou la divulgation accidentelle ou malveillante, et pour maintenir les niveaux appropriés de confidentialité, d'intégrité et de disponibilité de ces ressources. La norme décrit les règles de sélection d'une classification pour les informations manipulées, traitées ou stockées pour Moorepay ou en son nom. Elle soutient la politique de classification des informations qui définit les exigences en matière de protection des informations.

La norme décrit les exigences minimales en matière de contrôle. Il incombe au propriétaire de l'information de veiller à ce que des mesures de contrôle appropriées soient appliquées à l'actif.

La norme couvre les règles de traitement de l'information à chaque étape de son cycle de vie, y compris :

- l'étiquetage
- stockage
- élimination
- le recyclage des équipements
- transit
- présentation

Pour chaque classification de données, la norme stipule les outils et les technologies dont l'utilisation est autorisée par l'organisation lors du traitement des informations.

La norme sur le traitement de l'information s'applique à tous les employés de Moorepay, aux vendeurs, aux partenaires et aux autres parties intéressées qui stockent, transmettent ou traitent des informations pour le compte de Moorepay.

Traitement des médias

Les contrôles suivants ont été mis en place pour empêcher la divulgation, la modification, la suppression ou la destruction non autorisées des informations stockées sur les supports.

Gestion des supports amovibles

Seuls les membres du personnel habilités sont autorisés à sortir des locaux des objets, y compris des supports de stockage portables, et sont responsables de leur conservation à tout moment.

Tous les supports amovibles sont cryptés conformément aux normes prescrites par la politique de Moorepay en matière de cryptographie.

Les supports amovibles sont sécurisés de manière adéquate lorsqu'ils ne sont pas utilisés, conformément aux contrôles prévus pour la classification des données contenues sur les supports.

Les supports amovibles sont éliminés en toute sécurité en faisant appel à des tiers agréés pour les détruire. Les supports sont stockés dans des bacs sécurisés en attendant d'être détruits.

Tous les ordinateurs portables fournis aux employés de Moorepay sont dotés d'un système de cryptage de l'ensemble du disque.

L'accès et l'utilisation des clés USB des ordinateurs portables sont contrôlés par des politiques de groupe et restreints en fonction du rôle de l'utilisateur et des exigences spécifiques.

Là où les dispositifs de stockage USB sont autorisés, le cryptage des données est appliqué, ce qui garantit que les données ne peuvent être consultées que par le dispositif utilisé pour la copie des données.

Toute utilisation détectée de ports USB fait l'objet d'un rapport via notre outil de gestion des appareils de l'utilisateur final.

Les ordinateurs de bureau utilisés dans le cadre de la prestation de services sont dotés de dispositifs de sécurité qui limitent l'accès aux clés USB, aux lecteurs de CD/DVD et aux disques durs locaux.

Élimination des supports

Tous les supports utilisés pour la fourniture du service qui ne sont plus utiles ou qui sont défectueux sont physiquement détruits.

Les méthodes de destruction sont proportionnelles à la classification des informations qu'elles contiennent et sont stipulées dans la norme de traitement des informations de Moorepay.

Le matériel est détruit par des tiers agréés, à l'aide d'un équipement spécialement conçu pour déchiqueter ou broyer le disque.

- Le processus de destruction des disques durs consiste à déchiqueter l'ensemble du disque dur en petits morceaux à l'aide d'un équipement de destruction de qualité industrielle, et à détruire les plateaux, les mécanismes et les composants électroniques du disque dur, rendant ainsi les données irrécupérables.
- L'écrasement est effectué en perçant un trou irréparable à travers chaque disque dur, détruisant les plateaux du disque, déchirant et fracturant les surfaces magnétiques et rendant les données du disque irrécupérables.

Le matériel est enregistré et stocké en toute sécurité par Moorepay avant d'être collecté pour être détruit par la tierce partie.

Une chaîne de contrôle est maintenue par la tierce partie tout au long du processus, depuis la collecte du matériel jusqu'à la délivrance d'un certificat de destruction à la fin du processus. Les certificats de destruction sont conservés par Moorepay à des fins d'inspection et d'audit.

Si nécessaire, les données et les logiciels peuvent être retirés des équipements de stockage informatique avant leur destruction.

Pour supprimer les informations et les logiciels avant la destruction, un programme d'assainissement est utilisé pour effacer les données du disque en écrivant un ou plusieurs motifs sur le disque, les motifs devant être d'une longueur de 1, 2 ou 4 octets.

Les informations confidentielles contenues dans les copies papier destinées à être détruites sont stockées dans des bacs sécurisés avant d'être détruites. Les copies papier sont détruites par des méthodes de déchiquetage sécurisées par des tiers agréés. Après le déchiquetage, les morceaux de la taille d'un confetti sont mis en balles et recyclés en produits de papier.

Lorsque le papier est déchiqueté par un fournisseur, un certificat d'élimination est délivré par la tierce partie et conservé par Moorepay à des fins d'inspection et d'audit.

Transfert de supports physiques

La quantité de données transportées à l'aide de supports portables (y compris les ordinateurs portables, les clés USB, les disques durs amovibles et les CD/DVD) est limitée. Tous les supports portables doivent être cryptés conformément à la politique de Moorepay en matière de cryptographie.

Tous les supports basés sur l'infrastructure à transporter doivent être cryptés conformément à la politique de Moorepay en matière de cryptographie.

Pour le transport des supports destinés à être détruits par des tiers, des conteneurs inviolables sont utilisés pour transférer l'équipement, des codes-barres sont scannés à chaque point de contact, des camions verrouillés et des conteneurs sécurisés assurent la sécurité des informations pendant le transport, et des flottes suivies par GPS sont utilisées.

Les supports de sauvegarde doivent être enfermés dans une boîte fermée à clé et être transportés par un service de messagerie autorisé. Le coursier doit signer la réception et la livraison doit être enregistrée.

Si les employés de Moorepay transportent des supports, ceux-ci doivent être conservés dans une boîte fermée à clé, rangée là où ils ne sont pas exposés (par exemple dans le coffre fermé d'une voiture ou d'une camionnette sécurisée).

Au moins deux employés de Moorepay doivent accompagner les médias tout au long du voyage. Le voyage doit être planifié à l'avance et les arrêts doivent être évités si possible ou réduits au minimum.

Gestion des identités et des accès

Exigences professionnelles en matière de contrôle d'accès

Moorepay a mis en place les contrôles suivants pour limiter l'accès aux informations et aux équipments de traitement de l'information.

Politique de contrôle d'accès

L'accès aux informations et aux systèmes de Moorepay est régi par la politique de contrôle d'accès logique et la politique de sécurité physique. Ces politiques s'appliquent à l'ensemble du personnel de Moorepay (qui, dans le cadre de ce document, comprend les employés permanents, temporaires et indépendants, ainsi que les sous-traitants) qui doivent travailler sur des actifs d'information et de traitement de l'information.

Politique de contrôle d'accès logique

La politique s'applique à tous les actifs de Moorepay en matière d'information et de traitement de l'information, y compris, mais sans s'y limiter, les réseaux, les systèmes d'infrastructure informatique, les applications, les référentiels de stockage de l'information, les processus opérationnels, les sauvegardes, les archives et les informations confiées à Moorepay par ses clients.

La politique couvre les domaines suivants :

- principes d'accès logique
- exigences en matière d'accès logique
- bannières
- attribution du mot de passe
- accès privilégié

- séparation des tâches

Politique de sécurité physique

La politique de sécurité physique de Moorepay définit les exigences en matière de sécurité physique pour tous les sites de Moorepay.

La police couvre les domaines suivants :

- les contrôles d'accès physiques
- évaluations de la sécurité physique
- exigences en matière de contrôle de la sécurité physique
- contrôle d'accès et identification
- contrôles environnementaux

Accès aux réseaux et aux services de réseau

Moorepay a déployé des agents logiciels pour protéger tous les terminaux et contrôler l'accès au réseau de l'entreprise.

Le logiciel permet de déployer des politiques et de s'assurer que les appareils disposent des logiciels prérequis, des mises à jour logicielles et de la configuration nécessaires avant d'autoriser l'accès au réseau.

Le logiciel est géré de manière centralisée et intégré à Active Directory. Les appareils qui se connectent au réseau de l'entreprise doivent avoir la configuration requise pour s'authentifier, ce qui, avec l'authentification de l'utilisateur, offre une pseudo-authentification à deux facteurs (quelque chose que vous avez et quelque chose que vous connaissez).

Accès aux applications de l'entreprise

L'accès aux applications clés de l'entreprise est contrôlé par l'authentification multifactorielle (MFA), par laquelle l'utilisateur doit soumettre son nom d'utilisateur et son mot de passe uniques, ainsi qu'un code d'authentification supplémentaire "à usage unique".

Pour certaines applications, des questions de sécurité supplémentaires sont également requises avant que l'accès ne soit accordé.

Accès à distance

L'accès à distance est réservé au personnel autorisé.

La même technologie que celle décrite ci-dessus est utilisée pour gérer l'accès à distance aux systèmes et actifs informationnels de Moorepay. L'accès à distance est régi par la politique relative à l'informatique mobile et au travail à domicile.

Accès au réseau sans fil

Les réseaux sans fil de Moorepay sont configurés pour utiliser le protocole WPA2 Enterprise.

Lorsque l'appareil tente de s'associer au point d'accès, ce dernier interroge le serveur d'authentification au nom de l'appareil et n'autorise l'accès que si le certificat est validé.

Une fois la connexion établie, la transmission des données est cryptée à l'aide des normes AES-CCPM.

Accès à l'environnement d'hébergement

L'accès aux environnements d'hébergement est contrôlé par l'utilisation d'une authentification à plusieurs facteurs et est limité à un groupe spécifique d'utilisateurs "privilégiés".

Gestion de l'accès des utilisateurs

Les contrôles suivants ont été mis en place pour s'assurer que les utilisateurs autorisés ont l'accès requis et que les utilisateurs non autorisés ne peuvent pas accéder aux systèmes et aux services.

Enregistrement et désenregistrement des utilisateurs Pratique des entreprises

Tous les comptes d'accès sont associés à une identité d'utilisateur unique (ID utilisateur). L'attribution de comptes d'utilisateurs génériques ou partagés est expressément interdite, sauf autorisation du responsable de la sécurité des informations (CISO).

Les comptes système ne sont utilisés que là où les processus standard nécessitent un profil pour être exécutés ; ces comptes ne sont pas utilisés et n'ont pas la capacité d'accéder aux systèmes.

Dans les cas où un accès privilégié temporaire est nécessaire, un processus de "bris de glace" est mis en œuvre, selon lequel l'autorisation doit être accordée et consignée, et l'accès est limité dans le temps et surveillé.

Services d'assistance SaaS

Les services disposent d'un cadre de sécurité intégré basé sur les rôles et l'accès à l'application et aux données sous-jacentes est contrôlé par le client.

- un compte opérateur "Moorepay" spécifique est créé et un mot de passe est attribué et modifié régulièrement.
- une autorisation explicite doit être accordée par le client à chaque fois que le compte Moorepay est utilisé pour accéder à l'application, ou,
- une autorisation implicite est accordée, ce qui signifie que si un client demande de l'aide, l'autorisation d'accéder à l'application est implicitement accordée.

Fourniture d'accès aux utilisateurs

Toutes les demandes initiales de mise à disposition d'utilisateurs et de notification de départ pour les employés de Moorepay sont initiées par les RH via le système de gestion des tickets du Service Desk. Un ticket "parent" est créé et les responsabilités de chaque équipe (par exemple les réseaux, l'infrastructure, les applications) sont ensuite indiquées par des "sous tickets" associés.

En enregistrant toutes les activités dans le système de gestion des tickets du Service Desk, les dossiers d'administration des accès sont conservés, ce qui permet d'assurer la traçabilité (c'est-à-dire la preuve de toutes les demandes d'entrées, de sorties et de modifications) de l'autorisation du propriétaire de l'actif d'information, de la création du compte, de l'ajustement permettant les changements de rôle et les modifications des privilèges d'accès, et de la fermeture du compte.

Gestion des droits d'accès privilégiés

Là où les employés de Moorepay ont besoin d'un accès au niveau du système (privilégié) au système et à l'infrastructure sous-jacents, des contrôles appropriés et proportionnels de la gestion des accès sont déployés.

Pour plus d'informations sur la gestion des accès privilégiés, veuillez consulter la documentation complémentaire du MAP spécifique à votre prestation de services.

Gestion des informations secrètes d'authentification des utilisateurs

Pour les nouveaux arrivants, les informations relatives aux mots de passe sont fournies au gestionnaire des utilisateurs à la date d'entrée en fonction et le compte d'utilisateur est configuré de manière à forcer le changement de mot de passe lors de la première utilisation.

Tous les mots de passe attribués sont uniques et conformes à la norme Moorepay Password Management.

Les demandes de réinitialisation de mot de passe sont gérées par le Service Desk pour les comptes d'entreprise et par l'équipe de paie spécifique pour les clients gérés.

L'identité de l'utilisateur est validée avant la modification du mot de passe.

Lorsqu'elle communique un nouveau mot de passe (ou qu'elle suit un reste) à un utilisateur vérifié, l'équipe d'assistance doit utiliser l'une des méthodes suivantes :

- via le système de messagerie instantanée de l'entreprise ou
- par SMS vers un téléphone portable vérifié ou
- verbalement sur un téléphone portable vérifié ou
- par courriel d'entreprise à une adresse courriel officielle de Moorepay

Dans chaque cas, il faut rappeler à l'utilisateur final de supprimer le message dès qu'il est connecté.

Examen des droits d'accès des utilisateurs

Les comptes d'utilisateurs sont examinés périodiquement afin d'identifier les comptes redondants.

Les profils d'utilisateurs des comptes d'entreprise font l'objet de révisions régulières, le cas échéant, et au moins tous les six mois, afin de s'assurer que le personnel s'est vu attribuer le bon niveau de privilèges en fonction de son rôle et de ses responsabilités.

Les systèmes hébergeant les clients des services gérés sont régis par le protocole d'audit SOC1 de type II ; des contrôles de routine sont effectués sur les profils d'utilisateurs sur une base mensuelle et des revues de gestion sont menées tous les trimestres pour s'assurer que le personnel s'est vu attribuer le bon niveau de privilèges en fonction de sa fonction.

Les clients SaaS contrôlent la gestion des accès au sein de leur propre instance d'application. La pratique standard pour la gestion des comptes Moorepay utilisés pour accéder aux applications des clients est que les comptes soient activés/désactivés par le

client sur demande et selon les besoins pour fournir le service contractuel. Les processus sont convenus entre les deux parties et des listes de sources de confiance sont tenues à jour pour garantir que les demandes d'accès ne peuvent être soumises que par des personnes nommément désignées.

Suppression ou adaptation des droits d'accès

L'accès des sortants à tous les systèmes de l'entreprise est supprimé à leur dernière date d'embauche ou en cas de suspension résultant d'une procédure disciplinaire.

Le système de service desk de l'entreprise contient des informations sur les équipments auxquels un utilisateur a accès et dispose d'une fonction permettant de produire des statistiques appropriées sur les demandes.

Dans le cadre du processus de départ des RH, un flux de travail est déclenché dans le système de service desk de Moorepay afin de s'assurer que toutes les parties concernées sont informées de la date de fin d' d'un employé sortant. Des tickets individuels pour les enfants sont créés pour s'assurer que tous les accès pertinents sont révoqués à la date et à l'heure voulues.

Dans les cas où une révocation immédiate de l'accès est nécessaire, un ticket prioritaire est créé et transmis à l'équipe appropriée pour une attention immédiate.

Lorsque l'employé change de fonction au sein de l'entreprise, son attribution d'accès est réexaminée, l'accès approprié est attribué en fonction des exigences de la nouvelle fonction et l'accès est révoqué s'il n'est plus nécessaire. Les changements d'accès sont mis en œuvre dans un délai convenu qui garantit la continuité du service dans l'ancien et le nouveau rôle de l'utilisateur.

Dans les cas où des tiers sont autorisés à accéder aux systèmes et aux informations de Moorepay, l'accès n'est facilité que pour la période requise et révoqué immédiatement à la fin du travail. Les tiers sont supervisés et contrôlés à tout moment par des membres du personnel de Moorepay lorsqu'ils accèdent aux systèmes et aux informations de Moorepay.

Sécurité physique

Dans le cadre du processus de départ des RH, une demande est formulée pour s'assurer que toutes les cartes de contrôle d'accès sont restituées lorsque l'employé quitte Moorepay. La carte sera logiquement désactivée dans le système ACC et la carte physique sera remise en stock.

Lorsque des clés ont été confiées à une personne, elles lui sont rendues avant qu'elle ne quitte son emploi chez Moorepay.

Responsabilités de l'utilisateur

Les contrôles suivants ont été mis en place pour s'assurer que les employés de Moorepay sont responsables de la protection de leurs informations d'authentification.

Utilisation d'informations d'authentification secrètes

La norme de gestion des mots de passe définit le standard technique minimum pour la structure et la maintenance des mots de passe (voir Contrôles de la gestion des mots de passe). La norme est étayée par la politique d'utilisation acceptable des systèmes d'information de Moorepay, qui énonce les exigences visant à garantir l'application de contrôles de sécurité pour protéger les systèmes de Moorepay qui stockent ou sont utilisés pour accéder à des informations.

Conformément à la politique d'utilisation acceptable :

- les mots de passe doivent être conservés en toute sécurité :
- les mots de passe ne doivent pas être écrits d'une manière qui les rendrait faciles à déchiffrer et les mots de passe ne doivent pas être conservés avec le matériel informatique, par exemple dans la sacoche de l'ordinateur portable. Cela inclut les mots de passe pour tous les systèmes d'information et les sites web.
- toute compromission de compte/mot de passe doit être immédiatement rapportée à l'équipe de sécurité afin que les mesures appropriées soient prises

Contrôle d'accès aux systèmes et aux applications

Les contrôles suivants ont été mis en place pour empêcher l'accès non autorisé aux systèmes et aux applications.

Restriction de l'accès à l'information

L'accès aux informations et aux systèmes est accordé strictement sur la base du besoin de savoir et/ou du besoin d'utiliser, et lorsqu'un besoin professionnel légitime a été démontré.

Toutes les demandes d'accès doivent être autorisées par le propriétaire des actifs informationnels (IAO), ou par un délégué autorisé du propriétaire. Le propriétaire doit s'assurer que la sensibilité de ces actifs est connue et comprise afin que des règles de

contrôle d'accès appropriées soient appliquées, le propriétaire reste responsable de la bonne protection des actifs informationnels.

L'accès n'est accordé que pour la période requise. Lorsque l'accès est accordé à des employés non permanents (par exemple, des contractants, des employés temporaires), l'accès doit être limité dans le temps pour expirer à une date correspondant à la durée prévue de l'affectation.

Toute tentative des employés de contourner les contrôles d'accès ou d'accéder à des actifs informationnels pour lesquels ils ne sont pas autorisés sera traitée comme un incident de sécurité et pourra faire l' de mesures disciplinaires.

Procédures de connexion sécurisées

Tout accès aux systèmes d'exploitation et aux applications nécessite l'authentification des utilisateurs, conformément aux normes stipulées dans la politique de gestion de l'accès logique et la norme de gestion des mots de passe.

Des avertissements généraux appropriés sont affichés sur les systèmes afin d'informer les utilisateurs que l'accès et l'utilisation non autorisés des systèmes sont interdits et qu'ils peuvent faire l'objet de mesures supplémentaires en cas de violation grave de la sécurité (par exemple, des mesures disciplinaires ou des poursuites judiciaires).

Les paramètres de verrouillage du compte après une tentative infructueuse sont activés pour protéger contre les attaques par force brute.

Les systèmes d'information appliquent un contrôle d'accès dès leur conception. Pour accéder à l'information, les utilisateurs doivent disposer d'un nom d'utilisateur et d'un mot de passe valides pour accéder à tout système ou application.

Les identités sont gérées par le profilage du domaine et du système, où les politiques de groupe définissent le niveau d'accès.

Des restrictions d'accès sont mises en œuvre là où c'est possible et l'accès est limité (par exemple, consultation, contribution, propriétaire) en fonction des besoins de l'entreprise et conformément aux exigences légales, réglementaires ou contractuelles pertinentes.

Système de gestion des mots de passe

La norme Moorepay sur la gestion des mots de passe définit le standard technique minimum pour la structure et la maintenance des mots de passe.

Cette norme s'applique à l'ensemble du personnel de Moorepay et à toute personne travaillant sur l'infrastructure de Moorepay (par exemple les représentants de l'entreprise de support).

Cette norme s'applique à tous les mots de passe utilisés dans l'infrastructure de Moorepay.

Il est fortement conseillé d'utiliser des "phrases de passe". Il s'agit de mots de passe composés de plusieurs mots, soit un ensemble aléatoire, soit quelque chose de significatif pour l'utilisateur.

La norme sur la gestion des mots de passe stipule les exigences minimales et les considérations à prendre en compte dans les domaines suivants :

- Complexité du mot de passe
- les mots de passe des comptes utilisateurs standard doivent comporter au moins 8 caractères.
- doit contenir à la fois des lettres et des chiffres o doit contenir un mélange de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux
- Vieillissement du mot de passe
- les mots de passe n'expirent pas. Conformément aux bonnes pratiques du NIST, il est conseillé de ne changer les mots de passe que si l'on soupçonne qu'ils sont compromis.
- les mots de passe doivent avoir une durée minimale d'un jour. Cette mesure vise à empêcher les utilisateurs de revenir à leur ancien mot de passe (en épuisant l'historique des mots de passe).
- Historique des mots de passe
- 12 mots de passe antérieurs doivent être mémorisés et bloqués.
- Verrouillage du mot de passe
- Les comptes d'utilisateurs doivent être configurés pour se verrouiller après un maximum de 5 tentatives séquentielles de saisie d'un mot de passe invalide.
- les comptes verrouillés en raison de tentatives de connexion non valides restent verrouillés jusqu'à ce qu'ils soient réactivés par le personnel autorisé.
- En outre, chaque compte professionnel doit avoir un mot de passe différent et unique. Pour permettre aux utilisateurs de conserver plusieurs mots de passe, Moorepay met à leur disposition un logiciel "gestionnaire de mots de passe" (coffre-fort).

Utilisation de programmes utilitaires privilégiés

L'utilisation non autorisée de programmes utilitaires pour passer outre ou contourner les contrôles d'accès est en infraction avec la politique de gestion des accès logiques de Moorepay et est strictement interdite.

Là où des programmes utilitaires sont nécessaires à des fins d'assistance ou de récupération, l'accès est restreint et étroitement contrôlé au moyen d'un processus de "bris de glace", selon lequel l'autorisation doit être accordée et consignée, et l'accès est limité dans le temps et surveillé.

Cryptographie Contrôles cryptographiques

Les contrôles suivants ont été mis en place pour garantir l'utilisation correcte et efficace de la cryptographie afin de protéger la confidentialité, l'authenticité et l'intégrité des informations.

Politique d'utilisation des contrôles cryptographiques

Moorepay a mis en place une politique de cryptographie dont l'objectif est de s'assurer que des mesures appropriées de contrôle du cryptage sont mises en œuvre pour protéger les données sensibles ou critiques contre la destruction, l'endommagement, la modification ou la divulgation accidentelle ou malveillante et pour maintenir des niveaux appropriés de confidentialité, d'intégrité et de disponibilité de ces ressources.

La politique couvre les domaines clés suivants de la cryptographie :

- politique générale
- droit international
- le cryptage des flux de réseaux
- le cryptage des données en transit
- chiffrement des données "au repos
- la gestion des clés de chiffrement

La politique générale en matière de cryptographie stipule que :

- L'utilisation de la cryptographie doit être proportionnelle à la valeur et à la sensibilité des informations concernées, ainsi qu'aux risques auxquels elles sont exposées.
- Des procédures doivent être établies pour garantir la disponibilité des informations chiffrées en cas de perte d'une clé de chiffrement.
- L'utilisation de contrôles cryptographiques doit être conforme à toutes les exigences légales et réglementaires pertinentes.

- Les forces clés et les algorithmes acceptables doivent être définis par l'équipe de sécurité et revus régulièrement.
- Toutes les licences doivent être obtenues pour exporter, importer et/ou utiliser des produits contenant de la cryptographie.
- Toutes les clés doivent être protégées par des contrôles physiques et logiques afin de s'assurer qu'elles ne sont pas compromises.
- Il doit exister un processus de gestion des clés approuvé et documenté pour gérer le cycle de vie complet des clés cryptographiques au sein de Moorepay.
- Le cryptage doit être mis en œuvre lors de la communication d'informations sur les clients ou d'informations personnellement identifiables (IPI) à l'extérieur de l'organisation.
- Tous les mots de passe doivent être communiqués sur un support différent de l'information cryptée (protégée).
- Tout service orienté vers l'internet nécessitant une infrastructure à clé publique (PKI) doit utiliser des certificats signés par une autorité de certification (CA) approuvée par l'équipe de sécurité.
- Tous les ordinateurs portables doivent être cryptés à l'aide d'un système de cryptage du disque entier.
- Tous les appareils mobiles doivent être cryptés à l'aide des protocoles de cryptage mobile de l'entreprise.

Cette politique s'appuie sur la norme Moorepay relative au traitement de l'information, qui décrit les règles à appliquer lors de la manipulation, du stockage et du traitement de l'information.

Gestion des clés

La politique de Moorepay en matière de cryptographie stipule ce qui suit concernant la gestion des clés :

- les clés de chiffrement doivent être gérées de manière à garantir que les données stockées chiffrées ne deviendront ni irrécupérables ni accessibles par une personne non autorisée
- veiller à ce que les clés de chiffrement principales soient stockées dans un endroit sûr et protégées de manière appropriée contre les dommages environnementaux et accidentels.
- veiller à ce que les clés de chiffrement ne soient pas conservées dans une base de données chiffrée avec ces clés ou sur le même hôte

- enregistrer les détenteurs des clés de chiffrement (gardiens des clés) nécessaires au déchiffrement des informations importantes
- révoquer ou modifier le chiffrement lorsque les détenteurs de clés quittent l'entreprise.
- là où c'est techniquement possible, les algorithmes de chiffrement (y compris la longueur des clés) et de hachage les plus puissants doivent être utilisés.
- doivent être signés par un fournisseur connu et fiable.

Sécurité physique et environnementale

Politiques de sécurité physique

Moorepay a mis en place les politiques et normes suivantes pour s'assurer que tous les sites qui hébergent ses équipments informatiques critiques, ses services et ses informations, sont protégés contre les accès physiques non autorisés, les menaces environnementales et autres menaces ayant un impact matériel sur la sécurité des informations.

Politique de sécurité physique

Ce document décrit les exigences en matière de sécurité physique établies par Moorepay pour l'ensemble de ses sites. Tout écart par rapport aux exigences établies doit être approuvé par le service immobilier et sécurité de l'entreprise.

Norme de sécurité pour les centres de données

Ce document définit les normes requises pour protéger les centres de données et l'équipement informatique sur site/les salles de serveurs protégeant les principales ressources informatiques de Moorepay contre une série de menaces physiques et environnementales.

Sécurité des centres de données

Les centres de données utilisés pour les offres de cloud privé et de cloud public de Moorepay sont fournis par des fournisseurs de centres de données tiers bien établis.

Des vérifications approfondies sont effectuées pour s'assurer que le fournisseur du centre de données s'aligne sur les exigences de sécurité de Moorepay et les centres de données font l'objet d'un audit régulier pour garantir une conformité continue.

Pour plus d'informations sur les contrôles de sécurité physique des centres de données, veuillez consulter la documentation complémentaire du MAP spécifique à votre prestation de services.

Zones sécurisées

Les contrôles suivants ont été mis en place dans les centres de services de Moorepay et dans d'autres lieux afin d'empêcher l'accès physique non autorisé, les dommages et les interférences avec les informations de Moorepay et les équipments de traitement de l'information.

Contrôles physiques à l'entrée

Les locaux physiques de tous les bâtiments utilisés par Moorepay et ses filiales sont sécurisés par des moyens appropriés et raisonnables. L'accès est interdit aux personnes qui n'ont pas le droit d'entrer dans les locaux de Moorepay.

L'accès au site est réservé aux personnes ayant un besoin professionnel légitime. Tous les locaux et équivalents suivent des politiques de base et des meilleures pratiques pour assurer la meilleure sécurité physique possible en fonction de la criticité des actifs à protéger et du niveau de risque.

Les garanties minimales autorisées sont les suivantes

- Contrôles d'accès physiques (badges d'accès) : pour éviter que des personnes non payées par Moore ne pénètrent dans les locaux et.. ;
- Contrôle d'identité (badges d'identification) : pour permettre le contrôle des personnes qui entrent dans les locaux de Moorepay.

Les employés ne sont pas autorisés à partager leurs badges ou à accorder l'accès au site à un autre employé (cela inclut le fait de suivre un autre employé dans le bâtiment après que l'employé précédent a retiré son badge, c'est-à-dire le "piggybacking").

Chaque employé est chargé de veiller à la sécurité de son bâtiment en suivant les directives énoncées dans la politique de sécurité physique de Moorepay.

Les visiteurs des centres de services de Moorepay ne doivent être autorisés à entrer que sur invitation préalable de Moorepay, dans la mesure du possible, ou, là où il est nécessaire d'accueillir des visiteurs non planifiés (par exemple en cas d'urgence), un hôte de Moorepay doit être disponible pour accueillir le visiteur et superviser ses activités pendant sa présence.

Tous les visiteurs des centres de services Moorepay doivent toujours s'enregistrer à l'entrée. Les informations suivantes sont enregistrées dans le registre des visiteurs :

- Nom complet
- Signature
- Heure d'arrivée
- Heure de départ
- Contact sur place

Sécurisation des bureaux, des locaux et des équipments

Les informations et les équipments de traitement des informations sont stockés dans une zone sécurisée empêchant tout accès non autorisé.

Une combinaison de cartes, de codes PIN et de serrures mécaniques est utilisée pour contrôler l'accès aux zones sécurisées.

Les codes d'accès ne sont connus que du personnel autorisé à pénétrer dans ces équipments.

Protection contre les menaces externes et environnementales

Des systèmes de suppression, de détection et d'alerte appropriés sont en place pour protéger les actifs contre les menaces environnementales.

Travailler dans des zones sécurisées

Les divisions et les départements locaux sont responsables de la création de procédures et d'instructions de travail appropriées pour travailler dans des zones sécurisées. Les contrôles sont mis en œuvre en fonction de la sensibilité des informations traitées, de toutes les exigences légales, réglementaires et contractuelles, et conformément aux politiques de Moorepay en matière de sécurité et de confidentialité. Les contrôles peuvent inclure, mais ne sont pas limités à ce qui suit :

- protection par écran et/ou fenêtres obscures
- utilisation et possession interdites d'appareils mobiles
- Vidéosurveillance aux entrées et dans les zones de traitement.
- des constructions sécurisées empêchant la possibilité de sauvegarder ou de transférer des données localement

L'accès aux zones sécurisées est accordé sur la base du "besoin d'utilisation", là où une justification commerciale a été soumise et l'accès approuvé.

Des notes d'orientation appropriées sont émises à l'intention du personnel appelé à travailler dans des zones sécurisées.

Aires de livraison et de chargement

Des contrôles de sécurité physique appropriés sont déployés pour garantir que les zones d'accès public, de livraison et de chargement sont isolées des équipments de traitement de l'information.

- les entrées des zones de chargement sont sécurisées conformément à la politique de sécurité physique de Moorepay.
- le personnel désigné est chargé de surveiller et de contrôler l'accès aux zones de chargement.
- le personnel utilisant les zones de chargement et de livraison est surveillé physiquement et par télévision en circuit fermé à tout moment.
- le cas échéant, les itinéraires entre les zones de livraison et de chargement et les équipments opérationnels font l'objet de contrôles de sécurité physique.

Equipement

Les contrôles suivants ont été mis en place pour éviter la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de Moorepay.

Implantation et protection des équipements

Les systèmes d'information sont installés dans des salles de serveurs adaptées.

Une combinaison de cartes, de codes PIN et de serrures mécaniques est utilisée pour contrôler l'accès aux salles de serveurs. Les codes d'accès ne sont connus que du personnel autorisé à pénétrer dans ces équipments.

Les équipements de serveur, de stockage et de réseau sont logés dans des baies de serveur qui sont sécurisées de tous les côtés pour empêcher la manipulation des équipements et l'accès aux ports et aux disques.

Soutien aux services publics

Les contrôles suivants sont mis en œuvre de manière standard pour protéger les équipements concernés :

- les systèmes de détection et de suppression des inondations et des incendies
- Onduleurs et générateurs d'électricité

- régulation de la chaleur (climatisation + capteurs de chaleur)

Des accords de maintenance sont en place et des tests réguliers de l'équipement sont effectués pour garantir l'efficacité des contrôles de soutien.

Des audits sont effectués au moins une fois par an par Moorepay pour s'assurer que l'équipement adéquat est en place et entretenu efficacement.

Entretien des équipements

Moorepay a conclu des contrats adossés et des accords de niveau de service avec les tiers concernés.

L'équipement est entretenu conformément aux recommandations des vendeurs.

Lorsque des tiers sont engagés, un suivi approprié de l'activité est assuré.

Les équipements réparés sont testés de manière approfondie avant d'être réintroduits dans les environnements de production.

Retrait des actifs

Les actifs remis aux utilisateurs finaux sont signés par l'utilisateur et l'enregistrement est conservé dans le système de billetterie de l'entreprise en regard de l'entrée de l'actif.

Les logiciels sont installés par le personnel d'assistance autorisé et conservés dans des bibliothèques sécurisées.

Les actifs ne peuvent être retirés du centre de données sans l'accord préalable du gestionnaire du site.

Tout équipement retiré d'un centre de données ou d'un centre de services est enregistré comme ayant été déplacé hors du site et enregistré lors de son retour.

Sécurité des équipements et des actifs hors site

Moorepay dispose d'une politique de sécurité en matière d'informatique mobile et de travail à domicile qui couvre la sécurité des appareils mobiles.

La présente politique s'applique à tous les employés et tiers travaillant à distance ou utilisant des appareils mobiles (qui, aux fins du présent document, sont considérés comme des téléphones mobiles, des tablettes, des ordinateurs portables, des macs ou d'autres équipements informatiques facilement transportables) qui bénéficient d'un accès autorisé aux informations et aux systèmes de traitement de l'information.

Tous les employés et les tiers autorisés doivent se conformer à cette politique.

- les appareils mobiles fournis et pris en charge par Moorepay sont autorisés à se connecter aux réseaux et à accéder aux informations qui s'y trouvent. Tous ces appareils doivent avoir les outils de gestion de l'entreprise installés pour leur permettre d'être gérés à distance et d'effacer les données si nécessaire.
- le chiffrement des disques doit être appliqué à tous les appareils mobiles.
- tous les appareils mobiles doivent être protégés par un mot de passe ou un code pin.
- les ordinateurs portables doivent être fournis et pris en charge par Moorepay. Il est explicitement interdit de connecter les appareils appartenant à l'utilisateur aux réseaux ou aux actifs informationnels. Une dérogation spéciale peut être appliquée par exception, uniquement là où une justification commerciale spécifique et une approbation sont en place.
- afin d'assurer une protection solide contre l'accès non autorisé aux informations en cas de perte, les ordinateurs portables doivent être protégés par un logiciel de cryptage approuvé. Les mots de passe doivent être conformes à la politique de Moorepay relative aux mots de passe des utilisateurs.
- tous les ordinateurs portables doivent avoir un logiciel anti-malware installé par défaut et les employés doivent s'assurer qu'il est régulièrement mis à jour sur leur appareil. Un logiciel anti-malware doit être installé sur les téléphones portables et les tablettes (y compris les appareils personnels).

Les employés doivent :

- garder les appareils mobiles en leur possession et à portée de vue chaque fois que cela est possible.
- prendre des précautions extrêmes pour protéger la confidentialité et minimiser le risque d'exposition en limitant les informations qui peuvent être vues par d'autres personnes.
- ranger les appareils mobiles hors de vue lorsqu'ils ne sont pas utilisés.
- emporter des appareils mobiles chez eux en dehors des heures de bureau.
- pour que les conversations téléphoniques restent discrètes et ne soient pas entendues, désactivez l'équipement Bluetooth lorsqu'il n'est pas indispensable et/ou réglez-le sur "caché" pour éviter que les appels ne soient interceptés.
- transporter les ordinateurs portables et les tablettes hors de vue lorsqu'ils sont transportés dans une voiture, de préférence dans un coffre fermé à clé.

Les employés ne doivent pas permettre à un utilisateur non autorisé d'accéder à un appareil de Moorepay ou de permettre l'accès aux données ou aux réseaux de Moorepay à partir d'un appareil appartenant à l'utilisateur qui est autorisé pour un usage professionnel, cela inclut les membres de la famille.

En cas de perte ou de vol d'un appareil mobile, les services informatiques doivent être informés immédiatement afin que le compte soit désactivé et les données effacées.

Élimination ou réutilisation sécurisée des équipements

Tous les supports utilisés pour la fourniture du service qui ne sont plus utiles ou qui sont défectueux sont physiquement détruits.

Le matériel est enregistré et stocké en toute sécurité par Moorepay avant d'être collecté pour être détruit par la tierce partie.

Un programme d'assainissement est utilisé pour supprimer les informations et les logiciels avant leur destruction. Les certificats de destruction sont conservés par Moorepay à des fins d'inspection et d'audit.

Matériel utilisateur non surveillé

Tous les postes de travail des utilisateurs sont verrouillés lorsqu'ils sont laissés sans surveillance.

La stratégie de groupe garantit que tous les systèmes des utilisateurs finaux qui traitent les données des clients sont automatiquement verrouillés après une période d'inactivité définie. Une nouvelle authentification de l'utilisateur est nécessaire pour retrouver l'accès au système après le verrouillage.

Politique de bureaux et d'écrans clairs

La politique "Clear Desk - Clear Screen" de Moorepay définit les exigences auxquelles doivent satisfaire les employés pour garantir la protection des informations confidentielles lorsqu'ils sont en possession de fichiers et de documents électroniques :

La présente politique s'applique à tous les employés de Moorepay et aux tiers autorisés à accéder aux locaux, aux informations et au traitement de l'information de Moorepay

équipements ou équipments, y compris les réseaux de données, de communication ou de téléphonie, les applications en nuage, les dispositifs informatiques statiques et mobiles et les supports amovibles associés.

Tous les gestionnaires sont responsables de la mise en œuvre de la politique de nettoyage des bureaux et des écrans dans leur domaine de compétence. Tous les employés doivent se conformer à cette politique de bureau clair/écran clair.

- en dehors des heures de travail, les bureaux doivent être débarrassés de toute information confidentielle documentée, qu'elle soit protégée ou non.
- chaque fois qu'un bureau est laissé sans surveillance, les informations confidentielles documentées doivent être conservées dans un endroit approprié et verrouillé.
- des équipments de verrouillage d'écran doivent être utilisés lorsqu'un ordinateur de bureau ou un appareil portable est laissé sans surveillance afin d'empêcher la visualisation non autorisée d'informations confidentielles.
- en dehors des heures de travail, tous les ordinateurs de bureau et portables doivent être éteints, sauf s'ils doivent rester allumés pour des raisons opérationnelles. Tous les appareils qui restent allumés doivent être déconnectés.
- toutes les informations classées comme confidentielles ou restreintes par l'entreprise doivent être éliminées en toute sécurité, conformément à la norme relative au traitement de l'information.
- les documents doivent être retirés rapidement des imprimantes, photocopieurs et télécopieurs.
- en dehors des heures de travail, le courrier non ouvert doit être mis sous clé.
- en dehors des heures de travail, les ordinateurs portables, les téléphones mobiles et autres actifs portables ainsi que les clés doivent être mis sous clé.
- les responsables de réunions doivent veiller à ce qu'aucune information confidentielle ne soit laissée dans la salle, que ce soit sur la table, les diapositives, les tableaux à feuilles mobiles ou les tableaux lorsque la salle n'est pas occupée

Les bureaux fermés à clé et les zones à accès restreint ne constituent pas une dérogation à cette politique de bureau et d'écran clairs.

Sécurité des opérations

Procédures opérationnelles et responsabilités

Les contrôles suivants ont été mis en place pour garantir le fonctionnement correct et sécurisé des équipments de traitement de l'information.

Procédures opérationnelles documentées

Les divisions commerciales et les départements locaux sont responsables de la création d'instructions et de procédures de travail appropriées pour s'aligner sur les politiques et les normes de l'entreprise.

Lorsque des données sont traitées, des procédures opératoires normalisées (PON) sont mises en place afin que chaque opérateur comprenne parfaitement les étapes du processus qui doivent être suivies.

doivent être respectées. Les procédures opérationnelles standard intègrent des étapes de validation pour garantir l'intégrité et la confidentialité des données.

Une documentation détaillée est conservée, qui comprend notamment les éléments suivants :

- la documentation relative à la construction et au déploiement
- les diagrammes de systèmes et les flux de données
- processus et guides de sécurité
- Processus ITIL

Gestion du changement

Pour s'assurer qu'il n'y a pas d'impact négatif sur les opérations commerciales ou la sécurité de l'information, des responsabilités et des procédures formelles de gestion des changements ont été mises en œuvre pour contrôler toutes les modifications apportées aux systèmes d'information.

Lorsque des modifications sont apportées, le processus de modification couvre au minimum les éléments suivants :

- l'identification et l'enregistrement du changement
- la planification et l'essai du changement
- l'évaluation des incidences potentielles du changement sur la sécurité, conformément à la politique de l'Union européenne en matière de sécurité.

Politiques et procédures de Moorepay en matière de gestion des risques liés à la sécurité de l'information

- l'approbation formelle de la modification proposée
- la communication des détails du changement à toutes les personnes concernées
- les procédures de repli, y compris les procédures et les responsabilités relatives à l'abandon et au rétablissement d'un changement infructueux et/ou d'événements imprévus.

Les gestionnaires de comptes clients et les propriétaires de services de Moorepay sont chargés de

la communication de changements aux clients lorsque ces changements ont une incidence sur la confidentialité, l'intégrité ou la disponibilité des données des clients.

Évaluation des risques

Des évaluations des risques sont effectuées, si nécessaire, par l'équipe de sécurité avant d'approuver les changements.

Les projets visant à traiter des informations confidentielles ou restreintes font l'objet d'une évaluation de l'impact sur la vie privée (DPIA).

Changement d'urgence

Dans les cas où un changement est nécessaire dans le cadre des activités de remédiation en raison d'un incident de niveau de gravité 1 ou 2, le processus de changement d'urgence peut être lancé pour garantir la résolution de l'incident en temps voulu.

La procédure de modification d'urgence exige qu'un comité d'approbation des modifications d'urgence (Emergency Change Approval Board - ECAB) soit convoqué pour examiner les détails de la modification et la traiter efficacement. La procédure de modification d'urgence couvre au minimum les éléments suivants :

- l'identification et l'enregistrement du changement
- la planification et l'essai du changement
- l'évaluation des incidences potentielles du changement sur la sécurité, conformément aux politiques et procédures de gestion des risques liés à la sécurité de l'information de l'UKI

Les équipes techniques et/ou le responsable de la mise en œuvre de la tâche de changement doivent être présents à la réunion de l'E-CAB et être en mesure de s'exprimer au nom de l'état d'avancement du changement et des critères techniques.

L'approbation de la procédure peut être donnée par le E-CAB si les critères ci-dessus sont remplis.

Gestion des capacités

Les systèmes sont conçus de manière à ce qu'une capacité supplémentaire soit toujours disponible pour faire face aux pics de traitement imprévus et planifiés.

Les demandes de capacité sont contrôlées et des projections des besoins futurs en capacité sont établies.

Les composants du système pris en compte lors de l'examen de l'état actuel de la capacité de l'environnement sont les performances du processeur, de la mémoire, du stockage et du réseau hôte dans les environnements de systèmes de production. Il existe différents ensembles d'outils permettant de recueillir ces données

L'information est transmise quotidiennement, fournissant différents points d'information sur chaque élément de l'environnement qui contribuent à fournir un résumé de la capacité globale d'un environnement.

Les multiples sources de données sont rassemblées pour établir un rapport sur le modèle d'utilisation de l'infrastructure.

Séparation des environnements de développement, d'essai et d'exploitation

Les équipments de développement, de test et d'exploitation sont physiquement et logiquement séparés. Le développement est effectué sur des serveurs spécifiques qui ne font pas partie de l'infrastructure d'hébergement de la production.

Les changements sont effectués dans des environnements de test pour l'application et l'infrastructure avant d'être mis en production.

La mise en œuvre des changements dans l'environnement de production est soumise à un contrôle strict des modifications.

Protection contre les logiciels malveillants

Les contrôles suivants ont été déployés pour garantir la protection des informations et des équipments de traitement de l'information contre les logiciels malveillants.

Contrôles contre les logiciels malveillants

Un logiciel anti-malware est installé sur tous les ordinateurs de bureau et portables de Moorepay, ainsi que sur les serveurs utilisés pour fournir le service.

Les pare-feu personnels sont activés sur tous les points d'extrémité.

Les employés ne sont pas autorisés à supprimer ou à désactiver les logiciels d'analyse antivirus ou les pare-feu personnels.

En outre :

- des dispositifs d'inspection du trafic et des dispositifs d'analyse de l'inspection du trafic sont déployés dans les environnements de réseau de Moorepay afin d'analyser le trafic entrant et sortant et de détecter et mettre en quarantaine les contenus suspects.
- tous les courriels entrants sont analysés à la recherche de codes malveillants à l'aide d'une suite de produits distincte.
- La liste blanche est en place pour garantir que l'accès est limité aux sites et services Internet approuvés, là où il y a un besoin professionnel légitime.

Les employés de Moorepay sont sensibilisés aux techniques permettant d'identifier les activités malveillantes et d'éviter de propager des virus et des logiciels malveillants ou d'être victimes d'une attaque malveillante.

Tout problème de logiciel malveillant ou d'hameçonnage doit être rapporté comme un incident de sécurité (qu'il soit réel ou suspecté) en suivant les conseils de la politique de gestion des incidents de sécurité de Moorepay.

Sauvegardes

Moorepay a mis en place des solutions de sauvegarde des données sur l'ensemble de ses plates-formes afin de se prémunir contre la perte de données et d'assurer la récupération des données conformément aux exigences contractuelles.

Pour plus d'informations sur les sauvegardes de données, veuillez consulter la documentation complémentaire du MAP spécifique à votre prestation de services.

Journalisation et surveillance

Une journalisation appropriée est activée sur tous les serveurs et appareils du réseau, conformément à la politique de sécurité opérationnelle de Moorepay, afin de s'assurer que les événements importants liés à la sécurité sont enregistrés :

- enregistrés dans les journaux
- stockées et protégées contre toute modification ou tout accès non autorisé
- transmis en toute sécurité aux analyseurs appropriés de la gestion des journaux
- examinés et analysés régulièrement ; et
- conservés pendant une période appropriée

Pour plus d'informations sur la journalisation et la surveillance, veuillez consulter la documentation MAP supplémentaire spécifique à votre prestation de services.

Conservation des journaux

Les journaux sont archivés avant d'être supprimés et conservés pendant au moins 12 mois.

Gestion des informations et des événements de sécurité

Moorepay a mis en place un système de gestion des informations et des événements de sécurité (SIEM).

Les journaux des serveurs, des dispositifs de réseau et de la base de données sont copiés dans le SIEM et analysés par le personnel qualifié du centre d'opérations de sécurité (SOC) pour détecter toute activité anormale susceptible de représenter un indicateur de compromission (IoC).

Les alertes sont mises en corrélation et examinées par le SOC afin de déterminer s'il s'agit d'authentiques informations de référence. Des plans de réponse documentés sont en place pour garantir la remontée et la réponse en temps voulu aux contrôles internes.

Le SOC fonctionne 24 heures sur 24, 7 jours sur 7 et 365 jours par an.

Les journaux SIEM sont conservés pendant 60 jours par défaut.

Journaux de l'administrateur et de l'opérateur

Pour garantir que les journaux qui enregistrent l'activité des comptes d'utilisateurs privilégiés sont protégés et examinés afin de s'assurer que les titulaires de comptes privilégiés ne manipulent pas les journaux sur les équipments de traitement de l'information sous leur contrôle direct, les journaux sont copiés sur le système SIEM pour analyse.

Il existe une politique de séparation des tâches qui garantit que les administrateurs de système n'ont pas accès au système SIEM.

Synchronisation de l'horloge

Toutes les horloges appropriées sont synchronisées à l'aide d'un service NTP ou équivalent et alignées sur une source unique. Cela concerne à la fois les systèmes d'exploitation et les applications où des horaires précis sont nécessaires pour des questions de non-répudiation.

Contrôle du logiciel opérationnel

Les contrôles suivants garantissent l'intégrité des systèmes opérationnels.

Installation de logiciels sur les systèmes opérationnels

Toutes les installations de logiciels doivent suivre le processus standard de gestion des modifications et, à ce titre, faire l'objet des étapes d'autorisation, d'examen et d'approbation requises avant l'installation.

Le logiciel est déployé dans un environnement d'assurance qualité et entièrement testé avant d'être mis en production.

Pour les nouvelles acquisitions de logiciels, le fournisseur doit au préalable se soumettre aux vérifications nécessaires conformément au processus Moorepay Supplier Assurance.

En fonction de la nature du logiciel et de l'impact potentiel sur la sécurité des données, l'équipe chargée de la sécurité peut procéder à d'autres évaluations de la solution et demander l'approbation avant le déploiement.

Pour les acquisitions et les modifications importantes de logiciels, le comité consultatif technique (TAB) est chargé d'évaluer et d'approuver pleinement l'acquisition.

Gestion des vulnérabilités techniques

Les contrôles suivants ont été mis en place pour empêcher l'exploitation des vulnérabilités techniques.

Gestion des vulnérabilités techniques

Moorepay dispose d'une norme de gestion des vulnérabilités qui établit les exigences minimales à déployer pour un système solide de découverte et de gestion des vulnérabilités.

La norme couvre les domaines clés suivants de la gestion de la vulnérabilité :

- gestionnaire de correctifs
- tests de pénétration
- analyse de la vulnérabilité

La norme comprend des exigences relatives à la découverte des vulnérabilités et à la réponse à ces vulnérabilités.

En outre, Moorepay maintient une norme pour la gestion des correctifs qui vise à définir un cadre de gestion commun pour l'application des correctifs sur les systèmes de

production afin de réduire les risques résultant de l'exploitation des vulnérabilités techniques, d'une manière efficace, systématique et reproductible.

La norme couvre les types de correctifs suivants :

- correctif de sécurité
- correctif à chaud
- Service Pack
- mise à jour du logiciel

La norme Moorepay Patch Management s'applique à tous les appareils informatiques susceptibles de présenter des vulnérabilités, notamment :

- routeurs et commutateurs de réseau
- serveurs
- bureaux
- ordinateurs portables
- appareils mobiles
- les applications logicielles et micrologicielles associées au sein du paysage technologique de Moorepay.

Pratique de Moorepay en matière de gestion des correctifs

Les informations concernant les correctifs et les mises à jour sont reçues de sources fiables et l'analyse du bilan de santé du système est effectuée quotidiennement.

Le délai de déploiement des correctifs dépend de nombreux facteurs, notamment de la criticité du correctif, de la criticité du système nécessitant le correctif, du temps d'arrêt du service et de son impact sur les clients.

- Les correctifs critiques sont déployés dans l'environnement de production dans les 14 jours suivant leur publication.
- Les correctifs hautement prioritaires sont déployés dans l'environnement de production dans les 14 jours suivant leur publication.
- Tous les autres correctifs Windows applicables sont déployés dans les 30 jours suivant l'approbation du correctif.
- Les correctifs supplémentaires dans l'environnement d'hébergement sont déployés au moins deux fois par an.

Déploiement des correctifs

Les correctifs sont installés dans un environnement de test avant d'être installés dans l'environnement de production.

Dans la mesure du possible, les correctifs sont installés dans la production pendant les fenêtres de maintenance convenues à l'avance, lorsque des temps d'arrêt sont nécessaires.

Le processus de déploiement des correctifs dans l'environnement de production est le suivant :

- l'identification des vulnérabilités et des correctifs
- Les informations concernant les correctifs et les mises à jour de sécurité sont reçues de sources fiables et l'analyse du bilan de santé du système est effectuée quotidiennement. Des tests de sécurité sont effectués régulièrement pour mettre en évidence l'exposition aux vulnérabilités connues.
- les informations générales sur les correctifs sont examinées régulièrement et les correctifs sont appliqués lorsqu'il existe un besoin spécifique, c'est-à-dire lorsqu'une nouvelle fonctionnalité est jugée utile ou que les calendriers d'assistance imposent une mise à jour.
- les conditions contractuelles standard déterminent le calendrier de mise à disposition des applications de base.
- la validation et le test des correctifs.
- le fichier de correctifs est validé, afin de s'assurer qu'il n'a pas été modifié en cours de route.
- le fichier de correctifs validé fait l'objet d'un contrôle antivirus, le cas échéant, à l'aide d'un logiciel d'analyse antivirus à jour, dans un emplacement isolé et sûr du réseau.
- les tests de déploiement des correctifs sont effectués sur un système "test" qui représente le plus fidèlement possible le système de production, afin de s'assurer que le correctif corrige la vulnérabilité qu'il est censé corriger et que l'introduction de nouveaux correctifs n'interrompt pas ou n'altère pas la fonctionnalité du système nécessaire aux applications ou aux services critiques pour l'entreprise.
- déploiement des correctifs
- une sauvegarde appropriée des systèmes est effectuée, là où c'est possible, avant d'installer le correctif dans l'environnement de production.
- une demande de modification est formulée et approuvée avant d'appliquer le correctif aux systèmes et applications de production

- des tests de fonctionnalité sont effectués après l'application du correctif, là où il y a lieu, pour s'assurer que le correctif a été déployé comme prévu et que la vulnérabilité a été éliminée avec succès.
- l'inventaire des actifs et/ou le document de configuration de base est mis à jour pour refléter le détail des correctifs nouvellement installés.

Pratique des tests de pénétration de Moorepay

Moorepay passe des contrats avec des tiers indépendants pour effectuer les opérations suivantes :

- des tests de pénétration de l'infrastructure deux fois par an
- tests de pénétration des applications avant leur diffusion

L'objectif des tests de pénétration de l'infrastructure est de s'assurer que l'infrastructure qui supporte les services publics n'est pas susceptible d'être attaquée par des vulnérabilités et des menaces connues. Les tests sont effectués sur les interfaces publiques applicables dans l'environnement de production.

Les tests de pénétration des applications font partie des processus de développement des applications adoptés par les équipes de développement de logiciels de Moorepay afin de s'assurer que les vulnérabilités sont identifiées et corrigées dans les nouvelles versions des produits.

Les tests de pénétration des applications sont effectués dans l'environnement QA. L'environnement QA reflète l'environnement de production en termes de plateforme, d'infrastructure et de périmètre de sécurité.

La méthodologie globale adoptée par les testeurs de pénétration sous contrat est basée sur les meilleures pratiques de l'OpenSource Security Testing Methodology Manual (OSSTMM), qui définit un ensemble de règles, de lignes directrices et d'approches internationalement reconnues pour les tests de sécurité et l'évaluation de la sécurité d'une organisation.

Les tests sont non intrusifs et n'impliquent aucune exploitation intentionnelle des vulnérabilités au-delà de ce qui est nécessaire pour démontrer l'existence des vulnérabilités, sauf demande expresse préalable.

Le processus de test de pénétration se décompose globalement en plusieurs phases résumées ci-dessous :

- empreinte (recherche)

- des renseignements de base sont recueillis sur l'internet afin d'obtenir des informations sur les adresses de réseau, le déploiement des technologies de l'information et la topologie du réseau.
- énumération
- un balayage des systèmes est effectué pour identifier les ports ouverts, les services et les caractéristiques architecturales. L'analyse est automatisée et les données brutes générées sont interprétées par un spécialiste de la sécurité.
- l'exploitation
- Les méthodes employées par les pirates informatiques sont simulées dans la mesure où les données recueillies lors de l'énumération sont utilisées pour planifier les étapes suivantes de la pénétration et de l'exploitation des systèmes cibles.
- l'analyse
- sont examinées, mises en corrélation avec les meilleures pratiques et les bases de connaissances actuelles, et les vulnérabilités sont classées par ordre de priorité.
- rapport
- un rapport est produit, mettant en évidence les zones de risque analysées.

Pratique d'analyse de la vulnérabilité de Moorepay

Une analyse des vulnérabilités internes et externes est effectuée tous les mois. L'analyse interne est effectuée par le personnel qualifié de Moorepay.

L'analyse des vulnérabilités externes est effectuée par un tiers qualifié. L'analyse porte sur toutes les infrastructures tournées vers l'extérieur.

L'évaluation de la vulnérabilité est basée sur une technologie propriétaire éprouvée, créée pour fournir un service d'analyse précis tout en maintenant la disponibilité du réseau.

La base de données des vulnérabilités est régulièrement mise à jour avec les dernières vulnérabilités et est alignée sur la norme CVE (Common Vulnerability and Exposures) pour les noms des vulnérabilités en matière de sécurité de l'information.

Les évaluations de la vulnérabilité gérées sont réalisées conformément à la méthodologie d'évaluation suivante :

- vérification
- Les contrôles sont effectués uniquement lors de la première analyse pour chaque adresse IP et se concentrent sur les contrôles associés à la vérification, afin de

garantir que les erreurs dans les données d'entrée ne se propagent pas dans les étapes ultérieures de l'évaluation et d'assurer l'intégrité des opérations d'analyse.

- numérisation des services
- la phase d'analyse des services de l'évaluation identifie tous les services TCP, UDP et ICMP qui répondent.
- énumération des services
- une fois que la présence d'un service a été confirmée, la capture d'informations de la bannière est tentée pour aider à déterminer l'état de vulnérabilité de la machine.
- détection des vulnérabilités
- cette phase consiste à effectuer un nombre configurable de tests, allant d'une série de tests de vulnérabilité de la couche d'application à un seul test spécifique si nécessaire, contre les services découverts dans les phases précédentes de l'évaluation. Un grand nombre de tests distincts sont effectués ; les outils sont continuellement mis à jour avec les derniers exploits de vulnérabilité.
- rapport
- Le rapport contient les constatations ainsi que les mesures correctives, les tendances historiques et les statistiques récapitulatives.

Toutes les vulnérabilités sont enregistrées dans le système de ticketing de Moorepay et corrigées en fonction de leur priorité par le personnel qualifié de Moorepay.

Les rapports de synthèse ne font actuellement pas partie de l'offre de services standard et ne peuvent pas être distribués à l'extérieur.

Remédiation aux vulnérabilités

Pour chaque vulnérabilité détectée, un score CVSS (Common Vulnerability Scoring System) est attribué (sur une échelle de 1 à 10). Ce score est utilisé avec d'autres facteurs déterminants pour classer chaque vulnérabilité détectée.

Les niveaux d'évaluation des risques attribués sont basés sur les définitions suivantes :

- critique

la vulnérabilité expose gravement le client à un risque de compromission ou est fort probable qu'il ait déjà été compromis parce qu'il est largement connu et qu'il est facile de l'exploiter.

- élevé

un problème qui, s'il est exploité, peut avoir de graves répercussions sur la confidentialité, la disponibilité et/ou l'intégrité de vos actifs informationnels ; le problème peut être relativement simple à découvrir ou son exploitation technique peut être relativement triviale.

- moyen

un problème qui, s'il est exploité, peut avoir un impact modéré sur la confidentialité, la disponibilité et/ou l'intégrité de vos actifs informationnels ;

la découverte du problème peut nécessiter un niveau raisonnable de capacité technique et il peut également être techniquement très difficile à exploiter ou nécessiter un niveau raisonnable de ressources/de temps.

- faible

un problème qui, s'il est exploité, a un niveau d'impact potentiellement faible sur la confidentialité, la disponibilité et/ou l'intégrité de vos actifs informationnels ; il peut également être techniquement difficile à exploiter dans la réalité ou nécessiter une allocation importante de ressources/de temps.

Toutes les vulnérabilités identifiées font l'objet de mesures correctives et sont suivies tout au long de leur cycle de vie. Les vulnérabilités critiques, élevées et moyennes sont traitées en priorité, tandis que les vulnérabilités faibles et informatives sont enregistrées et mises en évidence en vue d'un examen ultérieur.

considération. Dans le cas des applications, il peut s'agir d'un correctif de sécurité isolé fourni une fois que la nouvelle version est déjà en production. Toutes les actions de remédiation suivent une procédure de déploiement interne standard sous un contrôle strict des changements.

Les paramètres standards du service desk de Moorepay sont appliqués pour répondre et remédier aux vulnérabilités comme suit :

- critique - dans les 14 jours suivant la découverte
- élevé - dans les 14 jours suivant la découverte
- moyenne - dans les 6 mois suivant le signalement de la vulnérabilité.
- faible - dans les 12 mois suivant le signalement de la vulnérabilité.

Les délais de correction des vulnérabilités détectées sont principalement dictés par la gravité et l'impact, comme indiqué ci-dessus. Toutefois, la complexité et l'impact des activités de remédiation sur les services peuvent également être pris en considération

et, dans certaines circonstances, des retards peuvent être convenus et des risques à court terme acceptés lorsque la remédiation est axée sur des projets à plus long terme.

Restrictions à l'installation de logiciels

Toutes les installations de logiciels doivent suivre le processus standard de gestion des modifications et, à ce titre, faire l'objet des étapes d'autorisation, d'examen et d'approbation requises avant l'installation.

Les versions standard sont déployées sur les ordinateurs de bureau et les ordinateurs portables et comprennent la suppression des droits d'administrateur et la possibilité d'installer des logiciels.

Une liste des logiciels approuvés est tenue à jour et accessible à partir de chaque ordinateur de l'utilisateur final, via le Moorepay Software Centre.

Les demandes de logiciels sont soumises par l'intermédiaire du Centre de logiciels, une demande est ensuite enregistrée dans le système de gestion des services de Moorepay et l'approbation du gestionnaire est confirmée après évaluation avant de procéder à l'installation.

D'autres contrôles sur l'installation et l'utilisation des logiciels sont contenus dans la politique d'utilisation acceptable des systèmes d'information de Moorepay.

Le non-respect de ces politiques peut donner lieu à des procédures disciplinaires.

Considérations relatives à l'audit des systèmes d'information

Les contrôles suivants ont été mis en place pour minimiser l'impact des activités d'audit sur les systèmes opérationnels.

Contrôles d'audit des systèmes d'information

Des tests de contrôle spécifiques (automatisés et manuels) sont effectués régulièrement et les résultats sont enregistrés à des fins d'audit.

Les tests sont conçus pour donner l'assurance que des contrôles techniques et opérationnels spécifiques sont efficaces et fonctionnent dans les limites convenues.

Les tests sont conçus pour s'assurer qu'il n'y a pas d'impact négatif sur la confidentialité, l'intégrité et la disponibilité des informations.

Les audits sont planifiés et réalisés en tenant compte des exigences opérationnelles et avec l'accord des hauts responsables et des actifs.

Sécurité des communications

Gestion de la sécurité des réseaux

Les contrôles suivants ont été mis en place pour garantir la protection des informations contenues dans les réseaux et les équipments de traitement de l'information.

Pour plus d'informations sur la sécurité du réseau, veuillez consulter la documentation complémentaire du MAP spécifique à votre prestation de services.

Contrôles du réseau Moorepay a mis en place les politiques et normes suivantes pour s'assurer que tous les réseaux et leurs composants sont configurés de manière sécurisée et gérés de manière appropriée pour protéger la confidentialité, l'intégrité et la disponibilité des informations de Moorepay et de ses clients :

- Politique de sécurité du réseau
- Politique de gestion des pare-feux
- Norme de gestion des pare-feux

Moorepay dispose d'une équipe chargée de l'exploitation du réseau, qui se consacre à la gestion des environnements de Moorepay, y compris le réseau local et le réseau étendu de l'entreprise, l'environnement d'hébergement et les réseaux sans fil.

L'accès aux dispositifs du réseau et du pare-feu est limité à une IP de gestion spécifique.

situées sur le réseau interne "de confiance". HTTPS et SSH sont les protocoles cryptés sécurisés utilisés pour l'accès au gestionnaire.

Des pare-feux sont déployés à chaque frontière du réseau. Tout le trafic IP entrant ou sortant d'un réseau Moorepay doit traverser le pare-feu. Conformément aux meilleures pratiques de gestion des pare-feux, les éléments suivants sont mis en œuvre de manière standard.

- Par défaut, les pare-feux doivent fonctionner avec un refus implicite et empêcher tout trafic de circuler vers l'intérieur ou vers l'extérieur, à moins que ce trafic n'ait été spécifiquement approuvé par le biais d'un contrôle des modifications.
- les pare-feux ne doivent jamais être "fail open", c'est-à-dire qu'ils permettent au trafic de passer librement en cas de défaillance d'un dispositif. Toute défaillance doit entraîner un débit nul (fail secure).

- tous les systèmes périmétriques doivent être configurés de manière sécurisée (renforcés).

Lorsque des modifications individuelles sont apportées aux pare-feux, les ensembles de règles sont examinés pour s'assurer qu'ils ne posent aucun problème de sécurité et pour supprimer les règles redondantes qui ont pu être créées.

Ségrégation dans les réseaux

Les principes architecturaux suivants sont appliqués de manière standard :

- le trafic est empêché de circuler directement entre les applications et les réseaux externes (internet) par la mise en œuvre de pare-feu hébergés dans la zone démilitarisée (DMZ).
- des pare-feu sont déployés entre les réseaux d'entreprise et les environnements d'hébergement des clients.
- des pare-feu sont déployés pour séparer les environnements des clients.

Transfert d'informations

Les contrôles suivants ont été mis en place pour maintenir la sécurité des informations transférées au sein de Moorepay et avec toute entité externe.

Politiques et procédures de transfert d'informations

La politique de Moorepay en matière de classification et de propriété des informations décrit les règles de sélection d'une classification pour les informations traitées ou stockées pour Moorepay ou en son nom. Cette politique s'appuie sur la norme relative au traitement de l'information, qui définit les exigences en matière de protection de l'information afin de répondre aux exigences légales, contractuelles et commerciales.

Des allocations sont établies pour le transfert de données entre Moorepay et ses clients. Les méthodes suivantes sont autorisées et conformes à la norme de traitement des données et à la politique de cryptographie :

- le transfert de données entre les centres de données et les PC des clients est sécurisé par HTTPS et des certificats numériques.
- Le transfert de fichiers par interface est assuré par un portail SFTP qui utilise des informations d'identification uniques pour chaque client.
- Les protocoles HTTPS, SFTP et FTPS utilisent les algorithmes de cryptage SSL/TLS/SSH avec une longueur de clé de 256 lorsque les systèmes cibles le permettent.

Le transfert de données entre Moorepay et ses tiers est convenu et réglé par le biais de contrats, d'énoncés de travaux et d'accords de partenariat stratégique.

Des évaluations de l'impact sur la protection des données (DPIA) sont réalisées et des diagrammes de flux de données sont établis pour comprendre pleinement le flux de données, les points de risque associés afin de permettre la mise en œuvre de solutions de transfert sécurisées.

Accords sur le transfert d'informations

Moorepay a conclu des contrats adossés et des accords de niveau de service avec les tiers concernés.

Les exigences en matière de sécurité sont traitées dans le cadre de contrats, de cahiers des charges et d'accords de partenariat stratégique.

Les contrats types stipulent que les fournisseurs doivent se conformer aux lois et réglementations relatives à la confidentialité et à la protection des données, y compris, mais sans s'y limiter, la loi de 2018 sur la protection des données.

Les fournisseurs doivent se conformer à la politique de Moorepay en matière de confidentialité des données et à la norme de sécurité et de conformité pour les services de tiers externalisés.

Les fournisseurs doivent mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées et d'autres protections pour les données à caractère personnel.

Messagerie électronique

Le système de courrier électronique de Moorepay est configuré pour utiliser TLS spéculatif pour les courriels sortants, ce qui signifie que si le système de réception a une capacité TLS, TLS est utilisé pour crypter l'information en transit.

La norme de Moorepay sur le traitement des informations stipule que les informations confidentielles doivent être cryptées lorsqu'elles sont transférées par courriel, sauf accord écrit avec le client.

Tous les courriels entrants sont analysés à la recherche de codes malveillants.

L'accès au webmail est interdit et une liste blanche est en place pour garantir que l'accès est limité aux sites et services Internet approuvés, là où il existe un besoin professionnel légitime.

Accords de confidentialité ou de non-divulgation

Les accords de confidentialité sont inclus dans les contrats de travail standard des employés et stipulent que les employés maintiennent la confidentialité des informations de l'entreprise, ne discutent pas des affaires de l'entreprise dans des lieux publics et ne divulguent pas d'informations confidentielles à l'extérieur de l'entreprise sans autorisation.

Le non-respect de ces règles entraînera des mesures disciplinaires et toute violation de la confidentialité pourra être considérée comme une faute grave.

Les clauses de confidentialité sont incluses dans les conditions générales en vigueur avec les fournisseurs, et stipulent que les fournisseurs doivent garder la confidentialité, n'utiliser que dans le but de fournir les produits ou services de Moorepay et éviter de divulguer à des tiers toutes les informations confidentielles de Moorepay.

Les "informations confidentielles de Moorepay" comprennent toutes les informations non publiques que Moorepay fournit aux fournisseurs dans le cadre de l'accord, ou qui sont obtenues ou créées par le fournisseur lors de la fourniture des produits ou services, et que le fournisseur utilisera des procédures de sécurité appropriées pour assurer la non-divulgation des informations confidentielles de Moorepay.

Acquisition, développement et maintenance des systèmes Exigences de sécurité des systèmes d'information

Les contrôles suivants ont été mis en place pour garantir que la sécurité de l'information fait partie intégrante des systèmes d'information tout au long de leur cycle de vie.

Analyse et spécification des exigences en matière de sécurité de l'information

Le comité consultatif technique (TAB) valide les propositions de nouvelles technologies.

Le comité consultatif des changements (CCC) valide les propositions de modifications majeures des systèmes existants.

L'implication de l'équipe de sécurité dans les processus TAB et CAB garantit :

- l'intégration de contrôles de sécurité et de protection de la vie privée dans la solution proposée la conformité avec les politiques de sécurité et de protection de la vie privée

- l'achèvement satisfaisant de l'évaluation de la sécurité et de la confidentialité des données comme preuve de la conformité aux exigences en matière de sécurité et de confidentialité.

Sécuriser les services d'application sur les réseaux publics

Les applications publiques (Internet) sont sécurisées conformément à la norme de traitement de l'information et à la politique de cryptographie de Moorepay.

Les méthodes de connexion et de transfert de données sont incluses dans les accords de service à la clientèle, les contrats avec les fournisseurs et les accords de partenariat stratégique.

Protection des transactions des services d'application

Des connexions point à point sécurisées sont maintenues entre le service et le client.

Des technologies de cryptage appropriées sont déployées pour les informations en transit, conformément à la norme de traitement de l'information de Moorepay et aux politiques de cryptographie.

Les certificats numériques sont sécurisés conformément aux normes de gestion des clés de Moorepay. Les règles de validation des applications assurent l'intégrité des données.

Sécurité dans les processus de développement et de soutien

Les contrôles suivants ont été mis en place pour garantir que la sécurité de l'information est conçue et mise en œuvre dans le cadre du cycle de développement des systèmes d'information.

Une politique de développement sûre

La politique de Moorepay en matière de développement sécurisé s'applique à l'acquisition, au développement et à la maintenance de tous les logiciels, systèmes, équipements et services qui soutiennent les actifs informationnels de Moorepay.

Toutes les activités de développement des systèmes informatiques de Moorepay et les fournisseurs qui fournissent des systèmes d'information et des services à Moorepay sont tenus de se conformer à cette politique.

Les objectifs du développement d'applications sécurisées sont les suivants :

- pour intégrer la sécurité de l'information dans l'ensemble du cycle de vie de l'acquisition, du développement et de la maintenance des applications.
- s'assurer que, lors de la conception et de la mise en œuvre des systèmes d'information, la sécurité de l'information fait partie intégrante du cycle de vie.
- mettre en place des niveaux appropriés de protection des données utilisées pour tester les systèmes d'information.

La politique couvre les principes suivants de développement, d'acquisition et d'entretien qui devraient être suivis de manière standard :

- exigences, analyse et spécification en matière de sécurité
- normes de codage sécurisées
- traitement correct des demandes
- le contrôle des logiciels opérationnels
- fournisseurs de logiciels
- développement externalisé
- protection des données d'essai
- l'accès au code source du programme
- le déploiement des applications

Procédures de contrôle des modifications du système

Les modifications de l'infrastructure et des systèmes sont gérées et contrôlées par le processus de gestion des modifications opérationnelles décrit précédemment dans le présent document.

Examen technique des demandes après modification de la plate-forme d'exploitation

Les modifications apportées aux plates-formes d'exploitation sont testées dans un environnement sécurisé d'assurance qualité avant d'être mises en production.

Des scripts de test personnalisés sont élaborés et des critères d'acceptation sont définis pour garantir que les problèmes sont identifiés et résolus et que le potentiel d'impact négatif est éliminé avant la mise en œuvre des changements dans les environnements de production.

Restrictions concernant les modifications apportées aux logiciels

La modification des logiciels fournis par les fournisseurs n'est pas une pratique courante au sein de Moorepay. Là où des modifications sont nécessaires, la pratique standard est de s'assurer qu'il n'y a pas d'impact sur les accords de service et de support en place.

Toutes les modifications apportées aux progiciels (développés en interne ou acquis) sont effectuées conformément au processus de gestion des changements et entièrement testées dans un environnement d'assurance qualité avant d'être déployées en production.

Principes d'ingénierie des systèmes sécurisés

Moorepay dispose d'une norme de construction de serveurs sécurisés qui fournit les principes fondamentaux formant la base d'une architecture de construction standard et garantit que des constructions répétables et cohérentes sont déployées sur l'ensemble du parc de serveurs. La norme se concentre sur les principes et les objectifs qui constituent le composant du système d'exploitation d'un serveur, appelé environnement d'exploitation standard (SOE).

La norme SOE s'applique aux serveurs physiques ou virtuels construits pour être utilisés par Moorepay. La norme Secure Build couvre en détail les exigences clés suivantes :

- configuration du système d'exploitation
- le durcissement du système d'exploitation, y compris, mais sans s'y limiter,
- désactivation des protocoles, services et ports non requis
- suppression des outils de développement et de gestion
- la suppression ou le changement de nom des comptes et des mots de passe par défaut
- cryptage des disques
- gestion des identités et des accès
- rapiéçage
- exploitation forestière
- les services de sécurité, y compris, mais sans s'y limiter,
- configuration et gestion des logiciels anti-malveillants
- enregistrement auprès d'un service d'analyse de la vulnérabilité
- enregistrement avec SIEM
- l'enregistrement avec la politique de gestion des correctifs
- sauvegarde

Environnement de développement sécurisé

Les équipments de développement, d'essai et d'exploitation sont physiquement et logiquement séparés.

Le développement est effectué sur des serveurs spécifiques qui ne font pas partie de l'infrastructure d'hébergement de production. L'accès aux environnements de développement et de test est contrôlé conformément à la politique de gestion des accès logiques de Moorepay.

Développement externalisé

Les systèmes utilisés pour la prestation des services sont détenus et entretenus par Moorepay. Toute la propriété intellectuelle (IP) est détenue et contrôlée par Moorepay.

Seuls les fournisseurs privilégiés de Moorepay sont utilisés pour la fourniture de ressources de développement externalisées.

Toutes les ressources doivent respecter et s'aligner sur toutes les politiques de l'entreprise en matière de sécurité, de conformité et de ressources humaines.

Là où des services professionnels sont utilisés pour la mise en œuvre de nouvelles technologies, une supervision et un suivi sont obligatoires.

Tests de sécurité des systèmes

Informations sur les procédures internes d'examen et d'essai, y compris les scripts d'essai, les critères d'acceptation, l'élaboration d'histoires, etc.

Les applications hébergées par Moorepay font toutes l'objet de tests de pénétration, au moins une fois par an ou à chaque version majeure du logiciel, sur la base des tests recommandés par l'OWASP, The Open Web Application Security Project (Projet de sécurité des applications Web ouvertes).

Les tests de pénétration sont effectués par des tiers indépendants et qualifiés.

Essais d'acceptation du système

Les builds sont compilés et l'automatisation complète des tests s'exécute (et réussit) avant qu'un build puisse être mis à disposition dans un environnement d'assurance qualité formel. Après l'approbation de l'assurance qualité, les versions sont mises à la disposition de la production ou des correctifs mensuels programmés et ne peuvent être promues qu'ensuite à l'étape de test et de mise en service.

Des réunions hebdomadaires sont organisées pour discuter du contenu et de l'état d'avancement de la prochaine version du SMR.

Protection des données d'essai

Les données réelles ne sont pas utilisées en dehors des environnements de production sans instruction explicite du responsable du traitement.

Relations avec les fournisseurs

Sécurité de l'information dans les relations avec les fournisseurs

Les contrôles suivants ont été déployés pour assurer la protection des actifs de Moorepay accessibles aux fournisseurs.

Politique de sécurité de l'information pour les relations avec les fournisseurs

La politique de sécurité des fournisseurs de Moorepay prescrit l'exigence de l'entreprise pour une sécurité appropriée dans les relations avec les fournisseurs. Moorepay reconnaît que pour fournir des services à ses parties prenantes (clients, employés, etc.), elle peut avoir besoin de faire appel aux produits et services d'un tiers (et de ses fournisseurs).

Ces exigences visent à protéger la confidentialité, l'intégrité et la disponibilité des informations manipulées, stockées et/ou traitées par les fournisseurs agréés (et leurs fournisseurs).

Toutes les personnes agissant au nom de Moorepay doivent adhérer à la politique de sécurité des fournisseurs lorsque ceux-ci accèdent, ou sont susceptibles d'accéder, aux informations de Moorepay ou de ses clients.

L'équipe chargée des achats procède à un ensemble strict d'étapes d'évaluation dans le cadre de la recherche et de l'embarquement de fournisseurs potentiels. Le cycle de vie de la recherche de fournisseurs comprend les principales étapes suivantes.

- l'inventaire des fournisseurs potentiels pour les catégories de fournisseurs cibles, c'est-à-dire la recherche de fournisseurs offrant la bonne offre de services et la mise en conformité requise.
- engager un dialogue avec les candidats fournisseurs recensés pour discuter de l'objectif des services.
- compléter les accords de non-divulgation.

- présenter le modèle d'engagement des fournisseurs aux fournisseurs potentiels.
- gérer le fournisseur tout au long du processus d'évaluation.

Le modèle d'évaluation des fournisseurs de Moorepay varie en fonction du niveau de risque des fournisseurs, avec des degrés d'analyse variables selon la nature et la sensibilité des services fournis.

L'équipe de sécurité est engagée par les services d'approvisionnement pour la recherche, la sélection et l'embarquement de tout nouveau fournisseur. Cela se fait dès que le besoin d'un fournisseur est reconnu par l'entreprise.

Tous les fournisseurs font l'objet d'une évaluation initiale des risques en matière de sécurité et de respect de la vie privée avant la conclusion d'un contrat. L'évaluation des risques en matière de sécurité et de protection de la vie privée comprend des vérifications de la conformité de l'entreprise et une évaluation des certifications et des documents d'assurance disponibles chez le fournisseur.

L'approche de Moorepay en matière de diligence raisonnable basée sur les risques consacre son attention et ses ressources aux relations qui présentent les risques les plus importants. Bien que tous les fournisseurs soient soumis à un contrôle de sécurité et de conformité et à un programme d'assurance des fournisseurs, l'évaluation de la sécurité des fournisseurs est effectuée conformément à une approche basée sur le risque, avec des audits potentiels sur site pour les partenaires à haut risque.

L'approche tient compte de divers facteurs de risque, tels que

- le pays d'opération
- l'opportunité commerciale
- le type de relation avec le fournisseur
- l'importance de la relation d'affaires et
- le niveau potentiel d'interaction avec Moorepay et/ou les informations sur les clients dans les catégories définies dans la politique de traitement et de propriété de l'information.

Aborder la question de la sécurité dans les accords avec les fournisseurs

Les exigences en matière de sécurité sont traitées dans le cadre de contrats, de cahiers des charges et d'accords de partenariat stratégique.

Les contrats types stipulent que les fournisseurs doivent se conformer aux lois et réglementations relatives à la confidentialité et à la protection des données, y compris, mais sans s'y limiter, le GDPR / Data Protection Act 2018.

Les fournisseurs doivent se conformer à la politique de Moorepay en matière de confidentialité des données et à la norme de sécurité et de conformité pour les services tiers externalisés.

Les fournisseurs et doivent mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées et d'autres protections pour les données à caractère personnel, dans des domaines comprenant, mais sans s'y limiter, les suivants :

- gestion des risques
- sensibilisation des utilisateurs
- gestion des incidents et des changements
- l'accès des utilisateurs
- protection des données
- la sécurité physique
- continuité des activités et reprise après sinistre
- cryptographie
- gestion de la vulnérabilité

Chaîne d'approvisionnement en technologies de l'information et de la communication

Les risques associés aux technologies de l'information et de la communication sont pris en compte dans le cadre de l'évaluation des risques des fournisseurs. Le cas échéant, un examen plus approfondi de ces éléments du service est entrepris et un contrôle des risques approprié est convenu avec le fournisseur.

Gestion des prestations de services des fournisseurs

Les contrôles suivants ont été mis en place pour maintenir un niveau convenu de sécurité de l'information et de prestation de services conformément aux accords conclus avec les fournisseurs.

Suivi et examen des services des fournisseurs

Les fournisseurs sont réévalués périodiquement pour s'assurer qu'ils respectent les exigences de Moorepay.

La fréquence de cet examen est déterminée par la classification du fournisseur et peut être augmentée ou diminuée en fonction de l'évaluation des risques liés à toute constatation en matière de sécurité et/ou de conformité au cours d'une période d'évaluation donnée, y compris, mais sans s'y limiter, tout incident grave ou répété en matière de sécurité et/ou de conformité qui indique une défaillance du système de conformité, ou tout changement organisationnel majeur.

Un désengagement potentiel est envisagé là où il y a des constatations graves et/ou répétées.

Les fournisseurs sont évalués par un personnel qualifié qui examine les politiques, les processus et les procédures fournis par le fournisseur.

Les évaluations sont examinées en vue d'un suivi et d'une remédiation.

Les constatations sont documentées et un plan d'action de suivi est établi, où les demandes d'actions correctives sont formulées par Moorepay et les actions correctives et préventives sont fournies par le fournisseur.

Si nécessaire, un audit est entrepris pour évaluer l'efficacité des mesures correctives proposées.

Gérer les modifications apportées aux services des fournisseurs

Un système d'échelonnement est utilisé pour garantir une évaluation appropriée des risques. Lorsque la prestation de services d'un fournisseur est modifiée, le classement de ce dernier est réévalué et l'évaluation des risques est alignée.

Gestion des incidents de sécurité de l'information

Gestion des incidents et des améliorations en matière de sécurité de l'information

Les contrôles suivants ont été mis en place pour garantir une approche cohérente et efficace de la gestion des incidents liés à la sécurité de l'information, y compris la communication sur les événements et les faiblesses en matière de sécurité.

Responsabilités et procédures

Moorepay dispose d'une procédure opérationnelle standard de gestion des incidents de sécurité (SOP) formellement documentée qui sous-tend la politique de gestion des incidents de sécurité.

Le manuel de procédures de gestion des incidents de sécurité vise à décrire le processus de gestion des incidents de sécurité avec suffisamment de clarté pour permettre aux équipes opérationnelles d'établir et d'appliquer efficacement le processus et de mettre en œuvre la politique de gestion des incidents de sécurité.

Le SOP de gestion des incidents de sécurité exige qu'une équipe de réponse aux incidents de sécurité (SIRT) soit constituée à partir des secteurs concernés de l'entreprise afin d'assurer une représentation appropriée et un parrainage de la direction pour répondre efficacement à l'incident.

Les SIRT sont responsables des activités suivantes tout au long du cycle de vie de l'incident de sécurité :

- la réaction efficace et rapide à l'incident de sécurité
- la participation aux réunions du SIRT
- veiller à ce que des ressources soient disponibles dans le domaine d'activité délégué, le cas échéant
- veiller à ce que les activités d'investigation et d'assainissement bénéficient de la priorité et de l'engagement nécessaires
- veiller à ce que la communication avec les clients soit gérée efficacement.
- faire remonter l'information au sein de l'entreprise le cas échéant.

Rapport sur les événements liés à la sécurité de l'information

Dans le cadre de la phase d'analyse du POS de gestion des incidents de sécurité, une équipe de réponse aux incidents de sécurité (SIRT) est mise en place pour assurer une gestion efficace de l'incident de sécurité.

et de veiller à ce que les responsables des activités concernées et la direction générale soient tenus informés.

La communication avec les parties prenantes internes est maintenue tout au long du processus sous la forme d'une déclaration de sécurité régulière et de la fourniture d'un rapport d'incident détaillé, le cas échéant.

Conformément à l'article 33 du GDPR, la "notification d'une violation de données à caractère personnel à l'autorité de contrôle" relève de la responsabilité du responsable du traitement des données et stipule que le responsable du traitement est tenu de notifier l'ICO dans les 72 heures, et que ce délai ne commence à courir qu'à partir du moment où le responsable du traitement a pris connaissance de la violation. De même, la notification (si nécessaire) aux personnes concernées (lorsqu'il existe un risque élevé

pour les droits et libertés des personnes concernées, relève de la responsabilité du contrôleur de données (GDPR Article 34).

L'article 33, paragraphe 2, s'applique à Moorepay (en tant que sous-traitant) et stipule que "le sous-traitant notifie au responsable du traitement, dans un délai raisonnable, toute violation de données à caractère personnel dont il a connaissance".

Comme défini dans le processus de gestion des incidents de sécurité, et aligné sur le GDPR, les violations de données sont rapportées aux propriétaires d'entreprise et à la haute direction, qui assurent les communications externes avec les clients dès que cela est pratiquement possible.

Si elles sont connues à ce moment-là, les informations suivantes seront fournies par Moorepay dans le cadre de la communication initiale :

- description de la violation
- quand et comment Moorepay a été informé de la violation
- les personnes susceptibles d'avoir été affectées par la violation
- résumé des activités de confinement
- informations de contact pour plus d'informations

Un plan de communication sera alors convenu avec le client et mis en œuvre pour garantir une communication continue tout au long du processus.

Rapport sur les faiblesses de la sécurité de l'information

Il existe un processus clairement défini pour le rapport des événements de sécurité (y compris les incidents et les faiblesses), soit directement au gestionnaire, soit au service de sécurité par l'intermédiaire du Service Desk.

Des informations sur le rapport des incidents et des faiblesses en matière de sécurité sont publiées sur l'intranet de l'entreprise, incluses dans la formation annuelle en ligne sur la conformité et abordées dans les bulletins d'information et les programmes de sensibilisation locaux et centraux.

Évaluation des événements liés à la sécurité de l'information et prise de décision à ce sujet.

Dès la notification d'un événement de sécurité potentiel, l'événement est évalué par un membre de l'équipe de sécurité au cours de la phase de triage. Si cela est jugé approprié sur la base de l'évaluation initiale, l'événement est évalué par un membre de l'équipe de sécurité.

Après évaluation des faits, l'événement sera qualifié d'incident de sécurité et un plan d'intervention approprié sera mis en œuvre.

Réponse aux incidents liés à la sécurité de l'information

Moorepay dispose d'une procédure opérationnelle standard de gestion des incidents de sécurité (SOP) formellement documentée qui sous-tend la politique de gestion des incidents de sécurité.

Aux fins du manuel de procédures de gestion des incidents de sécurité, un incident de sécurité de l'information est défini comme tout événement irrégulier ou indésirable qui a eu ou peut avoir un impact indésirable sur la sécurité des actifs informationnels, des opérations commerciales ou des informations traitées pour le compte des clients. Le terme "incident" peut s'appliquer à des situations d'urgence, à des violations législatives ou contractuelles, à des défaillances opérationnelles ou à des situations ou perceptions anormales.

Le SOP de gestion des incidents de sécurité est suivi dans tous les cas où un incident de sécurité est rapporté à l'équipe de sécurité, y compris en cas de cyberattaque potentielle ou réalisée ou de violation de données.

Le processus de bout en bout du POS de gestion des incidents de sécurité comprend les étapes suivantes :

- l'analyse
- confinement
- éradication
- récupération
- examen
- rapports et communication

Tirer les leçons des incidents liés à la sécurité de l'information

Les procédures opérationnelles standard de gestion des incidents de sécurité prévoient qu'une enquête détaillée est menée avec les collègues et les gestionnaires responsables. Dans le cadre de la phase d'éradication, une analyse des causes profondes (RCA) est entreprise et des observations et recommandations sont soumises par l'équipe de sécurité pour s'assurer que les leçons sont tirées et que les problèmes sont traités.

Collecte des preuves

La norme Moorepay sur la gestion des enquêtes judiciaires établit le standard de sécurité pour la gestion des enquêtes judiciaires afin de maximiser la capacité à préserver et à analyser les données générées par un système informatique qui peuvent être requises à des fins légales et réglementaires.

Les preuves sont collectées et stockées dans un dépôt de preuves sécurisé.

Lorsqu'il s'agit d'éléments de preuve, une chaîne de possession est maintenue tout au long du cycle de vie de l'incident. Les informations relatives à la chaîne de possession sont saisies dans les notes d'incident chaque fois que des éléments de preuve sont manipulés, stockés, recueillis ou transférés. Les détails suivants sont enregistrés au minimum :

- ce que
- quand
- où
- qui
- comment

Aspects de la sécurité de l'information dans le cadre de la gestion de la continuité des activités

Continuité de la sécurité de l'information

Les contrôles suivants ont été mis en place pour garantir que la continuité de la sécurité de l'information est intégrée dans les systèmes de gestion de la continuité des activités de Moorepay.

Planification de la continuité de la sécurité de l'information

Moorepay dispose d'une politique de résilience des activités qui décrit les buts et les objectifs du système de gestion de la continuité des activités (BCMS). Ces objectifs soutiennent les objectifs commerciaux de l'entreprise en fournissant l'assurance que les produits et services clés seront disponibles en cas de besoin par les parties autorisées à y avoir accès.

Les parties intéressées comprennent les clients, les employés, les autorités légales, les partenaires et les propriétaires de l'entreprise.

Les objectifs de la gestion de la continuité des activités sont les suivants :

- attribuer des rôles et des responsabilités appropriés pour la gestion de la CB, tout d'abord pour se préparer à un incident majeur et ensuite pour s'assurer que la réponse à un incident majeur bénéficie du niveau de soutien approprié de la part des fonctions clés de l'entreprise.
- veiller à ce qu'une analyse d'impact sur les activités (BIA) et une évaluation des risques soient réalisées pour toutes les activités, tous les produits et tous les services critiques.
- veiller à ce que des plans de reprise documentés soient maintenus et révisés régulièrement pour les activités qui fournissent et soutiennent des produits et services critiques.
- mener des exercices et des tests selon un calendrier convenu, en veillant à ce que les résultats soient évalués et à ce que les lacunes éventuelles soient enregistrées, les mesures d'amélioration documentées et les propriétaires convenus.
- veiller à ce que tous les membres du personnel reçoivent une formation adaptée à leur rôle dans le BCMS afin qu'ils puissent s'acquitter de leurs tâches au sein du BCMS.
- veiller à ce que des audits internes et des revues de direction soient réalisés à des intervalles convenus afin de garantir l'efficacité du BCMS.

Moorepay a mis en place des plans de reprise après sinistre (DR) documentés pour le centre de données. L'objectif de ce plan est de s'assurer que Moorepay peut rétablir tous les services concernés, dans le cadre des niveaux de service convenus, en cas d'incident perturbateur.

Le plan fournit des informations sur l'environnement de l'application, les exigences en matière de reprise et les tâches nécessaires au basculement vers un emplacement secondaire. Le plan intègre le plan de reprise de l'environnement de l'application hébergée.

Le plan DR est conçu pour s'intégrer au processus d'incident majeur, qui doit être suivi lorsqu'il a été déterminé que le plan DR doit être lancé.

Le plan DR comprend les informations clés suivantes :

- aperçu des services
- actions de redressement
- l'équipe de gestion de la récupération
- détails du site
- activités de préemption - dépendances de récupération
- procédures de recouvrement

- contact principal

Objectifs de récupération

Le SLA standard alloue 24 heures à partir d'une panne majeure pour envisager l'invocation du DR. L'objectif de temps de récupération (RTO) est de 24 heures à partir de l'invocation d'un incident DR par le gestionnaire de Moorepay. Le temps d'arrêt total maximum est de 48 heures.

L'objectif de point de récupération (RPO) standard est garanti dans les 4 heures suivant l'invocation d'un incident DR par le gestionnaire de Moorepay.

Mise en œuvre de la continuité de la sécurité de l'information

Chaque plan de continuité des activités et de reprise après sinistre stipule l'obligation d'appliquer des contrôles de sécurité de l'information pour garantir la confidentialité, l'intégrité et la disponibilité des informations et des systèmes en cas d'incident perturbateur.

Le cas échéant, des instructions spécifiques sont incluses dans les étapes de récupération afin de garantir la poursuite de la mise en œuvre des contrôles de sécurité.

Des équipes d'intervention d'urgence sont constituées pour coordonner la continuité des activités et la reprise après sinistre. Ces équipes comprennent des spécialistes de la sécurité de l'information qui veillent à ce que la sécurité soit maintenue tout au long de la période de reprise.

Une évaluation des risques est effectuée et des contrôles d'atténuation sont mis en œuvre là où l'efficacité des contrôles de sécurité est réduite en raison de l'incident perturbateur.

Vérifier, examiner et évaluer la continuité de la sécurité de l'information.

Des tests de reprise après sinistre des applications sont effectués au moins une fois par an ou lorsque des changements importants interviennent dans l'infrastructure d'hébergement, afin de confirmer que les exigences en matière de reprise peuvent être satisfaites. Les clients sont invités à participer aux exercices de reprise. Pour de plus amples informations sur les tests de reprise après sinistre, veuillez consulter le document MAP 04 Business Continuity.

Licenciements

Disponibilité des équipments de traitement de l'information

Les centres de données sont dupliqués sur un site géographique distinct.

L'infrastructure utilisée pour fournir le service est dotée d'une redondance N+1 à tous les niveaux afin de se prémunir contre les défaillances des composants. Les centres de données sont de niveau 3, offrant une résilience à l'échelle du site et des contrôles environnementaux appropriés pour protéger la disponibilité des systèmes et des données.

Pour assurer une connexion résiliente entre le site du client et les centres de données de Moorepay, deux tunnels VPN IPSec sont créés au moment de l'installation, l'un vers le centre de données principal et l'autre vers notre site secondaire (DR).

Conformité

Respect des exigences légales et contractuelles

Les contrôles suivants ont été mis en place pour s'assurer que les obligations légales, statutaires, réglementaires ou contractuelles liées à la sécurité de l'information sont comprises et respectées par les parties prenantes.

Identification de la législation applicable et des exigences contractuelles

L'équipe de conformité de Moorepay surveille et suit les obligations légales et réglementaires de l'entreprise, y compris les exigences relatives au SMSI.

Les contrôles normaux du SMSI de Moorepay sont conçus pour répondre aux exigences contractuelles standard des clients. Là où des exigences contractuelles non standard sont identifiées, des contrôles spécifiques au client peuvent être mis en place au sein des équipes de livraison du client. Droits de propriété intellectuelle.

L'utilisation acceptable des logiciels est incluse dans la politique d'utilisation acceptable de Moorepay.

Moorepay tient un registre des actifs logiciels et a mis en place un outil d'audit des logiciels qui sont utilisés pour déterminer quels logiciels sont installés et pour s'assurer que Moorepay dispose des licences adéquates pour tous les produits logiciels et que les employés n'ont pas installé de logiciels non autorisés.

Des contrôles sont mis en place pour s'assurer que les utilisateurs ne peuvent pas installer de logiciels sans autorisation préalable.

Moorepay n'acquiert des logiciels qu'à partir de sources connues et réputées afin de s'assurer que les droits d'auteur ne sont pas violés.

Protection des dossiers

Moorepay dispose d'une politique documentée de classification et de propriété des informations. L'objectif de cette politique est d'identifier et de mettre en œuvre des contrôles adéquats et efficaces de traitement et de protection des informations, en fonction de la sensibilité des informations traitées. Le but est de s'assurer que les précieuses informations commerciales et personnelles utilisées au sein de Moorepay et les informations confiées à l'organisation par ses clients sont protégées de manière appropriée tout au long de leur durée de vie.

Respect de la vie privée et protection des informations personnelles identifiables

Une activité essentielle au sein de Moorepay est le traitement des données personnelles des employés de ses clients, afin de fonctionner efficacement et de fournir ses services. Ce traitement est effectué conformément aux lois applicables en matière de protection des données et/ou de la vie privée dans les pays où Moorepay fournit des services.

Le règlement général sur la protection des données est utilisé comme norme de meilleure pratique dans les pays où il n'existe pas de loi ou de règlement équivalent en matière de protection des données et/ou de la vie privée.

La législation locale peut nécessiter une mise en œuvre spécifique des politiques et des pratiques pour s'aligner sur les exigences légales locales.

En tant que dépositaire de données personnelles, Moorepay s'assure que les données sont toujours traitées correctement et en toute sécurité, qu'elles soient conservées sous forme électronique ou physique, et qu'elles couvrent l'ensemble du cycle de vie des données, y compris :

- l'obtention de données à caractère personnel
- le stockage et la sécurité des données à caractère personnel
- l'utilisation des données à caractère personnel
- l'élimination/destruction des données à caractère personnel

Moorepay et les entreprises de son groupe sont enregistrés auprès de l'Information Commissioners Office (bureau des commissaires à l'information) comme suit :

- Zellis Holdings Ltd - numéro d'enregistrement ZA331332
- Zellis UK Ltd - numéro d'enregistrement Z6810325
- Moorepay Limited - numéro d'enregistrement Z9176805
- Moorepay Compliance Limited - numéro d'enregistrement ZA731897
- Benefex Ltd - numéro d'enregistrement Z8773454
- Benefex Financial Solutions Limited - numéro d'enregistrement Z3103927

Réglementation des contrôles cryptographiques

La norme Moorepay sur le traitement de l'information définit les exigences relatives à la protection des actifs informationnels, des ressources du système et des informations, afin de répondre aux exigences légales et réglementaires de Moorepay, de ses clients et des autres parties prenantes. La norme garantit que des contrôles cryptographiques sont déployés là où ils sont applicables.

La politique de Moorepay en matière de cryptographie établit les exigences minimales de sécurité pour la gestion de la cryptographie.

Examens de la sécurité de l'information

Les contrôles suivants ont été mis en place pour s'assurer que la sécurité de l'information est mise en œuvre et exploitée conformément aux politiques et procédures de Moorepay.

Examen indépendant de la sécurité de l'information

L'approche de Moorepay en matière de gestion de la sécurité de l'information et sa mise en œuvre, qui comprend notamment les objectifs de contrôle, les contrôles, les politiques, les normes et les procédures, font l'objet d'un examen indépendant à intervalles planifiés, en interne et en externe, par des personnes dûment qualifiées.

Les audits internes sont réalisés indépendamment par l'équipe de sécurité et l'équipe de conformité de Moorepay.

Les audits internes peuvent être déclenchés par divers événements, notamment, mais pas exclusivement, les suivants :

- dans le cadre du programme d'audit continu
- dans le cadre de l'analyse des causes profondes et des activités d'éradication et de récupération d'un incident de sécurité
- dans le cadre des activités d'évaluation des risques et d'assainissement.

- dans le cadre des activités de gestion du changement.

Des audits externes sont réalisés par des tiers indépendants dans les domaines suivants,

ISO 27001:2013

Champ d'application : Système de gestion de la sécurité de l'information pour les produits et les activités de soutien permettant de développer, de soutenir, de manipuler, de transférer, d'administrer, de stocker et de traiter les informations relatives à la paie et aux ressources humaines.

Cyber Essentials

Champ d'application : Périmètre du réseau de Moorepay UK Limited et dispositifs de point de terminaison

Respect des politiques et des normes de sécurité

Les gestionnaires sont tenus de participer aux activités d'audit interne et externe et sont responsables de la création et de la mise en œuvre de mesures correctives visant à améliorer la maturité des contrôles de sécurité.

Des réunions régulières d'examen de la gestion du SGSI sont organisées, qui incluent la contribution des chefs d'entreprise et un examen des risques de sécurité. Ce processus est contrôlé et vérifié par le BSI (British Standards Institute) pour notre certification ISO 27001.

Examen de la conformité technique

Les évaluations des contrôles de sécurité sont définies et exécutées selon un calendrier précis. Les résultats de ces évaluations sont examinés par le gestionnaire et, le cas échéant, vérifiés chaque année par des tiers indépendants.

Document 3 - Aperçu de la protection des données

Introduction

Une activité essentielle au sein de Moorepay est le traitement des données personnelles des employés de nos clients, afin de fonctionner efficacement et de fournir nos services. Ce traitement est effectué conformément aux lois applicables en matière de protection des données et/ou de la vie privée dans les pays où nous fournissons des services.

Le règlement général sur la protection des données (RGPD) est utilisé comme norme de bonnes pratiques dans les pays où il n'existe pas de loi ou de règlement équivalent en matière de protection des données et/ou de la vie privée.

La législation locale peut nécessiter une mise en œuvre spécifique des politiques et des pratiques pour s'aligner sur les exigences légales locales. Pour les personnes concernées au Royaume-Uni, Moorepay s'aligne sur le GDPR et la loi britannique sur la protection des données 2018. Pour les personnes concernées irlandaises (personnes concernées de l'UE), le GDPR de l'UE s'appliquera.

En tant que dépositaire de données personnelles, Moorepay s'assure que les données sont toujours traitées correctement et en toute sécurité, qu'elles soient conservées sous forme électronique ou physique, et qu'elles couvrent l'ensemble du cycle de vie des données, y compris :

- L'obtention de données à caractère personnel
- Le stockage et la sécurité des données personnelles
- L'utilisation des données personnelles
- L'élimination/destruction des données à caractère personnel

Ce document vise à consolider les informations pertinentes sur la mise en œuvre des pratiques et des politiques adoptées par Moorepay pour assurer le traitement sécurisé des données conformément aux lois et réglementations applicables, comme indiqué ci-dessus.

Organisation

Le directeur juridique de Moorepay a la responsabilité globale des questions juridiques et de conformité. L'équipe juridique et l'équipe de conformité et d'audit sont placées sous l'autorité du directeur juridique.

Le chef de l'information et de la cybersécurité (HIS) est responsable et comptable de l'information et de la cybersécurité au sein de Moorepay, rapportant directement au chef de la sécurité de l'information (CISO).

Une équipe de sécurité de l'information et une équipe de sécurité technique sont rattachées au SIS.

Identification de la législation applicable

Les équipes juridiques et de conformité de Moorepay sont chargées de suivre et de contrôler les lois et les réglementations qui ont un impact sur les services que Moorepay

fournit à ses clients. Elles assurent un suivi quotidien dans les domaines du travail et de l'emploi, de la paie, des avantages sociaux, de la gestion globale des ressources humaines et de l'environnement, la mobilité, le recrutement, ainsi que la confidentialité et la protection des données, entre autres, dans tous les pays où les clients ont des employés.

Enregistrement auprès de l'Information Commissioners Office (ICO)

Moorepay et les entreprises de son groupe sont enregistrés auprès de l'Information Commissioners Office (bureau des commissaires à l'information) comme suit :

- Zellis Holdings Ltd - numéro d'enregistrement ZA331332
- Zellis UK Ltd - numéro d'enregistrement Z6810325
- Moorepay Limited - numéro d'enregistrement Z9176805
- Moorepay Compliance Limited - numéro d'enregistrement ZA731897
- Benefex Ltd - numéro d'enregistrement Z8773454
- Benefex Financial Solutions Limited - numéro d'enregistrement Z3103927

Transparence (informations sur la protection de la vie privée communiquées aux clients concernés)

Moorepay agit en tant que processeur de données en ce qui concerne les services fournis à ses clients, et en tant que tel traite les données personnelles entièrement sous l'instruction (générale ou spécifique) du client (qui est le contrôleur de données). Il incombe donc au client de se conformer aux exigences de transparence et de notification du GDPR (GDPR Art 5(1a) et spécifiquement les exigences pour les avis de confidentialité dans GDPR Art 12, Art 13 et Art 14 selon le cas).

Le client doit donc fournir des informations de confidentialité appropriées (par exemple des avis de confidentialité) à ses employés/pensionnés, etc. (c'est-à-dire les personnes concernées) qui expliquent comment leurs données sont traitées (y compris la façon dont le client utilise les services d'un processeur de données tiers si nécessaire (par exemple pour les services SaaS ou gérés).

Assurance cybernétique

Moorepay dispose d'une assurance cybernétique qui peut couvrir certaines pertes liées à des incidents cybernétiques.

Contrôle des employés

La sélection des employés est obligatoire avant de leur donner accès aux actifs de l'entreprise. La vérification des antécédents de tous les candidats à l'emploi, des sous-traitants et des utilisateurs tiers est effectuée conformément aux lois et réglementations locales en vigueur et aux exigences de l'entreprise. Dans le cadre de l'obligation d'emploi, les employés, les sous-traitants et les utilisateurs tiers doivent accepter et signer les conditions du contrat de travail, qui précisent leur responsabilité et celle de l'organisation en matière de sécurité de l'information. Tout manquement sera traité dans le cadre du processus disciplinaire de Moorepay.

Nos exigences habituelles en matière de contrôle sont les suivantes

- Contrôle du droit au travail
- Contrôle de la preuve de résidence
- Contrôle de probité financière
- 5 ans d'historique d'activité
- Vérification du casier judiciaire

En fonction du rôle de l'employé, des contrôles supplémentaires sont effectués conformément aux politiques et aux exigences de notre client en matière d'habilitations spécifiques.

Exigences en matière de protection des données dans les contrats d'employés

Les clauses de confidentialité et l'obligation de se conformer aux politiques de l'entreprise figurent dans les contrats de travail standard et stipulent que l'employé est tenu de préserver la confidentialité des informations techniques et commerciales sensibles de l'entreprise et des informations détenues en fiducie pour le compte de tiers.

Tout manquement aux conditions d'emploi est traité par la procédure disciplinaire propre à Moorepay et adaptée à la législation locale.

Formation de sensibilisation

Un cadre annuel de formation en ligne à la sécurité est fourni et est obligatoire pour tous les employés sans exception ; il fait également partie du processus d'initiation des employés.

Les objectifs du cadre annuel de formation à l'apprentissage en ligne sont les suivants :

- Respecter les politiques et les normes de sécurité de Moorepay.
- Comprendre les concepts clés de la protection des données qui sont importants pour l'exercice de votre fonction.

Tous les membres du personnel sont testés sur leurs connaissances de chaque sujet et doivent obtenir une note de 80% pour compléter chaque module.

Pour compléter la formation annuelle, l'équipe de sécurité fournit régulièrement du matériel supplémentaire axé sur des aspects importants de la sécurité, offrant des conseils supplémentaires sur la manière d'appliquer les bonnes pratiques et de travailler d'une manière plus sûre.

Les divisions et les services locaux sont chargés de créer des procédures et des instructions de travail appropriées afin de garantir que les activités de traitement et de soutien sont menées de manière cohérente et conformément aux politiques de l'entreprise et aux exigences légales et réglementaires applicables.

Mesures techniques et organisationnelles

Moorepay a mis en place des mesures techniques et organisationnelles appropriées et proportionnelles pour assurer une gestion efficace des risques liés aux informations et aux systèmes d'information.

La sécurité dès la conception est intégrée dans la conception, le développement et l'acquisition des systèmes d'information.

Des contrôles physiques, logiques et environnementaux appropriés sont en place dans les centres de services et les centres de données afin d'empêcher tout accès non autorisé, tout dommage et toute interférence dans les équipments de traitement de l'information, ainsi que dans les informations relatives à l'entreprise et aux clients.

L'infrastructure utilisée pour fournir le service est dotée d'une redondance N+1 à tous les niveaux afin de se prémunir contre les défaillances des composants.

Des technologies de cryptage des données sont déployées là où elles sont applicables.

Des technologies anti-malware sont déployées sur tous les appareils et serveurs.

Des technologies de pare-feu et de détection des intrusions sont déployées dans l'ensemble de l'infrastructure d'hébergement et du réseau de l'entreprise afin de se protéger contre les intrusions et les attaques par déni de service.

Des tests de pénétration et de vulnérabilité sont effectués sur les systèmes et les applications à des intervalles définis et les systèmes sont régulièrement corrigés.

Un système de gestion des informations et des événements de sécurité (SIEM) est en service, la journalisation est activée sur les systèmes, l'infrastructure et les applications, et les événements sont surveillés par le centre des opérations de sécurité (SOC).

Des tests de contrôle sont effectués à intervalles définis pour s'assurer de l'efficacité des mesures de sécurité.

Moorepay a mis en place un processus et des procédures de gestion des incidents de sécurité formellement documentés qui sous-tendent la politique de gestion des incidents de sécurité.

La capacité à maintenir la prestation de services et à restaurer les systèmes dans des situations défavorables est assurée par un programme de gestion de la continuité des activités. Les plans de continuité des activités et de reprise après sinistre sont maintenus et testés à intervalles réguliers.

Moorepay dispose d'un système de gestion de la sécurité de l'information (ISMS) conforme aux normes internationales et au code de pratique ISO 27002. Les contrôles de sécurité de Moorepay sont basés sur les meilleures pratiques de l'industrie et alignés sur la norme ISO 27001. Moorepay est certifié selon la norme ISO 27001:2013, dont les exigences générales sont les suivantes :

Gestion des risques

- Conformité juridique et réglementaire

Continuité des activités

- Sensibilisation à la sécurité
- Gestion des incidents de sécurité et des faiblesses
- Gestion des fournisseurs

L'accès aux systèmes est géré par les politiques de gestion de l'accès logique et de gestion de l'accès physique.

Des contrôles réguliers sont effectués tous les trimestres sur les profils d'utilisateurs, afin de s'assurer que le personnel s'est vu attribuer le bon niveau de privilèges en fonction de son rôle et de ses responsabilités.

La séparation des tâches est mise en œuvre pour réduire la dépendance à l'égard des personnes clés et pour prévenir les erreurs et la fraude.

Politique de gestion de la sécurité de l'information

La politique de gestion de la sécurité de l'information de Moorepay définit l'approche de l'organisation pour gérer ses objectifs en matière de sécurité de l'information.

La politique définit l'engagement stratégique de Moorepay en matière de gestion de la sécurité de l'information :

- Assurer le maintien de la qualité du service
- Répondre aux obligations contractuelles, légales et réglementaires de l'organisation
- Répondre aux besoins et aux attentes des clients et des autres parties intéressées

Les principaux objectifs de la présente politique sont les suivants :

- Activer les actifs informationnels de Moorepay et de ses clients contre toutes les menaces, qu'elles soient internes ou externes, délibérées ou accidentelles.
- Minimiser les risques de dommages en cherchant à prévenir les incidents de sécurité et en réduisant leur impact potentiel.

La politique de gestion de la sécurité de l'information s'appuie sur un ensemble de politiques, de normes, de guides, de processus et d'autres documents spécifiques. Un résumé de cet ensemble de politiques est disponible sur demande.

Politique de protection des données

Moorepay dispose d'une politique de protection des données documentée qui s'applique à toutes les données personnelles traitées par l'entreprise, y compris les données personnelles des employés de ses clients.

L'objectif de cette politique est de s'assurer que Moorepay :

- Respecter la législation applicable en matière de protection des données et de la vie privée et suivre les bonnes pratiques
- Protéger les droits de nos employés, de nos clients et de leurs employés, ainsi que de nos partenaires.
- est ouvert sur la manière dont il stocke et traite les données ; et
- Se protéger contre les risques d'une violation de données

La politique stipule qu'au minimum, Moorepay doit s'assurer que

- Seules les personnes autorisées à utiliser les informations peuvent y accéder ;
- Les informations sont exactes et adaptées à la finalité pour laquelle elles sont traitées
- Les personnes autorisées peuvent accéder aux informations si elles en ont besoin à des fins autorisées ; et
- Les données personnelles ne sont jamais stockées ou transportées sur un ordinateur portable, un téléphone mobile ou un dispositif de stockage amovible, ni envoyées en clair par quelque canal que ce soit (sauf exception enregistrée).

La politique couvre les sujets suivants :

- Responsabilités
- Conservation des données
- Principes et droits relatifs à la protection des données
- Cookies et données de tiers
- Transfert international de données

La protection de la vie privée dès la conception

La prise en compte du respect de la vie privée dès la conception signifie que les organisations doivent prendre en compte la protection de la vie privée dès les premières étapes de la conception et tout au long du processus de développement de nouveaux produits, processus ou services qui impliquent le traitement de données à caractère personnel.

Moorepay promeut une approche "Privacy by design" (respect de la vie privée dès la conception) par le biais de :

- Formation et sensibilisation : en veillant à ce que tout le personnel concerné soit conscient des obligations et des risques en matière de protection de la vie privée, de manière à ce que cette connaissance imprègne le processus de développement ;
- Nos mesures techniques et organisationnelles telles qu'elles sont détaillées ailleurs dans le présent document ;
- Adopter une approche axée sur la protection de la vie privée ;
- des outils tels que les évaluations de l'impact de la protection des données (DPIA) ou d'autres outils d'évaluation des risques, si nécessaire ou utile.

La politique de Moorepay en matière de développement d'applications sécurisées s'applique à l'acquisition, au développement et à la maintenance de tous les logiciels, systèmes, équipements et services qui soutiennent les actifs informationnels de

Moorepay. Toutes les activités de développement des systèmes informatiques de Moorepay et les fournisseurs qui fournissent des systèmes d'information et des services à Moorepay sont tenus de se conformer à cette politique.

Les objectifs du développement d'applications sécurisées sont les suivants :

- Intégrer la sécurité de l'information dans l'ensemble du cycle de vie de l'acquisition, du développement et de la maintenance des applications.
- Veiller à ce que, lors de la conception et de la mise en œuvre des systèmes d'information, la sécurité de l'information fasse partie intégrante du cycle de vie.
- Mettre en place des niveaux appropriés de protection des données utilisées pour tester les systèmes d'information.

Le comité consultatif technique de Moorepay (TAB) valide les propositions de nouvelles technologies. Dans le cadre du processus d'examen, les experts en matière de sécurité et de conformité apportent leur contribution pour s'assurer que :

- Les exigences légales et réglementaires sont comprises par les parties prenantes.
- Des contrôles de sécurité et de confidentialité suffisants sont incorporés dans la solution proposée.
- Tout projet impliquant le traitement de données à caractère personnel peut faire l'objet d'une évaluation de l'impact sur la vie privée (DPIA).

Dans le cadre du cycle de développement des logiciels (SDLC), l'assurance qualité et l'examen régulier du code garantissent que toute vulnérabilité potentielle en matière de sécurité est identifiée et corrigée avant que l'application ne soit diffusée dans l'environnement de production.

Les examens du code comprennent des vérifications de l'analyse statique du code pour les vulnérabilités du Top 10 de l'OWASP ainsi que le respect des normes de codage.

Le processus SDLC garantit que chaque amélioration logicielle est soumise à une série de contrôles et d'approbations avant d'être mise en production. Une DPIA peut être une exigence obligatoire dans le cadre de ce processus.

Les développeurs travaillent en étroite collaboration avec des experts en sécurité tiers qui leur fournissent des conseils sur les meilleures pratiques en matière de techniques de codage sûres, dans le cadre du cycle de développement durable (SDLC), et ce dans le cadre du programme de gestion des vulnérabilités.

Classification des données

Moorepay dispose d'une politique documentée de classification et de propriété des informations. L'objectif de cette politique est d'identifier et de mettre en œuvre des contrôles adéquats et efficaces en matière de traitement et de protection des informations, en fonction de la sensibilité des informations traitées. Le but est de s'assurer que les informations commerciales et personnelles de grande valeur sont traitées de manière appropriée.

Les informations utilisées au sein de Moorepay et celles confiées à l'organisation par ses clients sont protégées de manière appropriée tout au long de leur durée de vie.

Cette politique s'appuie sur la norme relative au traitement de l'information, qui définit les règles de traitement de l'information à chaque étape de son cycle de vie.

Les informations doivent être classées dans l'une des quatre catégories suivantes :

- Public

Information librement disponible. Elle est identifiée là où il n'y a pas d'étiquette de document ou par toute étiquette de document qui ne correspond à aucune des classifications suivantes.

- Restriction de l'entreprise pour usage interne uniquement

Les informations classées comme étant réservées à l'entreprise pour un usage interne peuvent être divulguées à tout employé de l'entreprise ou à tout contractant autorisé et approuvé.

- Confidentiel pour l'entreprise ou le client

Toutes les informations personnellement identifiables manipulées, traitées ou stockées par l'entreprise ou au nom de l'entreprise.

- Secret d'entreprise

Des informations qui, si elles étaient divulguées, auraient un impact significatif sur la réputation et le succès commercial de l'entreprise.

Accès aux données des clients

Les employés de Moorepay chargés des opérations de service, ainsi que les partenaires agréés qui ont été désignés pour fournir le service, auront accès aux informations du client. Dans le cas d'une implémentation SaaS, la majorité des accès aux données sera effectuée par le personnel du client uniquement ; cependant, les administrateurs du

système Moorepay et le personnel de support peuvent également avoir un accès indirect aux informations du client.

Des contrôles sont en place pour gérer ce type d'accès privilégié des utilisateurs.

Exigences en matière de confidentialité des données dans les contrats avec les fournisseurs

Les exigences en matière de sécurité sont prises en compte dans les contrats, les cahiers des charges et les accords de partenariat stratégique.

Les contrats types stipulent que les fournisseurs doivent se conformer aux lois et réglementations relatives à la confidentialité et à la protection des données, y compris, mais sans s'y limiter, le GDPR / Data protection Act 2018.

Les fournisseurs doivent se conformer à la politique de Moorepay en matière de confidentialité des données et à la norme de sécurité et de conformité pour les services tiers externalisés.

Les fournisseurs et doivent mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées et d'autres protections pour les données à caractère personnel, dans des domaines comprenant, mais sans s'y limiter, les suivants :

Gestion des risques

- Sensibilisation des utilisateurs
- Gestion des incidents et des changements
- Accès des utilisateurs
- Protection des données
- Sécurité physique

Continuité des activités et reprise après sinistre

- Cryptographie
- Gestion de la vulnérabilité

Évaluation du risque pour les tiers

Une évaluation des risques est réalisée avant d'accorder des droits d'accès à des tiers.

L'évaluation des risques doit inclure une évaluation de l'impact sur la vie privée dans les cas où des informations personnelles doivent être stockées, traitées ou transmises.

Des évaluations permanentes des fournisseurs essentiels sont entreprises pour garantir l'alignement continu des contrôles dans les contrats avec les fournisseurs. Le droit d'audit est inscrit dans les contrats types avec les fournisseurs.

Sous-traitants tiers

Les détails des sous-processeurs qui peuvent être utilisés par Moorepay sont maintenus et détaillés dans le contrat de service spécifique et/ou dans le document en ligne suivant :

De plus amples informations peuvent être fournies par le gestionnaire du compte concerné.

Stockage des données

En règle générale, toutes les données des clients sont stockées sur un support crypté dans l'environnement sécurisé du centre de données. Il est possible que les fonctions RH (là où un service externalisé est fourni) conservent les données localement pour des raisons de traitement spécifiques.

Des contrôles sont en place pour protéger les données dans ces circonstances.

Les ordinateurs de bureau utilisés dans le cadre de la prestation de services sont dotés d'une configuration standard qui limite l'accès aux lecteurs USB, aux lecteurs de CD/DVD et aux disques durs locaux, empêchant ainsi le stockage local de données.

Tous les ordinateurs portables et les appareils mobiles sont cryptés sur l'ensemble du disque. Tous les supports amovibles sont cryptés conformément aux normes prescrites par la politique de Moorepay en matière de cryptographie.

Les supports amovibles sont sécurisés de manière adéquate lorsqu'ils ne sont pas utilisés, conformément aux contrôles prévus pour la classification des données contenues sur les supports.

Conservation des données

Lorsqu'il traite les données des employés de ses clients, Moorepay agit en tant que responsable du traitement des données et, à ce titre, il appartient au responsable du traitement des données (le client) de déterminer en dernier ressort la conservation et la destruction de ses données.

Les données ne sont conservées que le temps nécessaire pour fournir les services indiqués et remplir les obligations légales, réglementaires et contractuelles ; dans le cas contraire, les données sont renvoyées ou détruites.

Pour plus de détails sur la conservation des données, reportez-vous à l'accord avec le client.

Destruction des données

Les environnements de serveurs SaaS utilisent des systèmes de fichiers partagés. Par conséquent, à la fin du service, les données du client sont supprimées et le stockage est renvoyé à l'environnement SaaS partagé.

Un processus manuel est suivi pour supprimer les données du client : les instances de l'application et de la base de données sont supprimées, de même que les systèmes de fichiers dédiés que le client peut avoir. Les données de sauvegarde du client sont supprimées dans le cadre de ce processus de résiliation.

Là où les clients ont des volumes de disques virtuels dédiés sur le SAN, les volumes peuvent être supprimés à la fin du service. Les disques physiques sont alors mis à la disposition d'autres volumes virtuels.

Un programme d'assainissement est utilisé pour retirer les informations et les logiciels des équipements avant leur destruction.

Les informations confidentielles contenues dans les copies papier destinées à être détruites sont stockées dans des bacs sécurisés avant d'être détruites. Les copies papier sont détruites par des méthodes de déchiquetage sécurisées par des tiers agréés. Un certificat de destruction est délivré par le tiers et conservé par Moorepay à des fins d'inspection et d'audit.

Collecte de données

Si les données sont collectées directement auprès de la personne concernée par le biais du service, le client doit s'assurer qu'il existe une base juridique valable pour la collecte de ces données.

Transfert de données

Les transferts de données entre les centres de données et les PC des clients sont sécurisés à l'aide de HTTPS et de certificats numériques.

Le transfert de fichiers de l'interface est assuré par un portail SFTP qui utilise des informations d'identification uniques pour chaque client.

Gestion des risques

Pour s'assurer que les informations commerciales précieuses et les actifs de traitement de l'information utilisés au sein de Moorepay, ainsi que les informations confiées à l'organisation par ses clients et partenaires commerciaux, sont protégés de manière appropriée tout au long de leur durée de vie, l'entreprise exploite une structure formelle de gouvernance des risques liés à la sécurité de l'information et un modèle de gestion des risques afin de s'assurer que :

- L'entreprise est en mesure de prendre des décisions éclairées sur le traitement des risques liés à la sécurité de l'information
- L'acceptation et la gestion des risques identifiés en matière de sécurité de l'information sont assurées par les personnes habilitées à le faire.
- Adoption d'une méthodologie cohérente et reproductible pour l'évaluation des risques liés à la sécurité de l'information
- La propriété des risques et des actions de traitement des risques est formellement attribuée.

La mise en œuvre de la stratégie de l'entreprise en matière de risques liés à la sécurité de l'information repose sur des méthodes formelles et reproductibles d'évaluation, de gestion et d'acceptation des risques.

Les projets visant à traiter des données à caractère personnel peuvent faire l'objet d'une analyse d'impact sur la protection des données (DPIA).

Les actifs critiques sont classés par catégories pour l'évaluation des risques, par exemple les fournisseurs, l'infrastructure informatique, les centres de données, et les menaces, vulnérabilités et impacts associés sont pris en compte. Il s'agit d'une évaluation générale pour chaque catégorie d'actifs critiques. S'il s'avère nécessaire de procéder à un examen plus spécifique d'un seul actif critique, cet examen sera entrepris et les résultats seront ajoutés au registre des risques en vue d'une gestion continue.

Les risques de sécurité identifiés sont examinés dans le cadre d'un examen régulier de la gestion du SGSI et, le cas échéant, une évaluation formelle des risques est entreprise. L'évaluation des risques est documentée et soumise au responsable de la sécurité et au gestionnaire de la sécurité de l'information, qui l'examinent. En cas d'approbation, le chef de la sécurité informera le propriétaire du risque (généralement un membre de l'équipe de direction élargie) et recommandera une option de traitement du risque.

Réponse aux violations de données

En cas de violation de données suspectée ou réalisée, Moorepay suivra son processus établi de gestion des incidents de sécurité.

Le processus vise à décrire le processus de gestion des incidents de sécurité avec suffisamment de clarté pour permettre aux équipes opérationnelles d'établir et d'appliquer efficacement le processus et de mettre en œuvre la politique de gestion des incidents de sécurité. Le processus intègre les éléments suivants

les étapes suivantes du processus :

- Analyse
- Confinement
- L'éradication
- Récupération
- Révision
- Rapports et communication

Conformément à l'article 33 du GDPR, la "notification d'une violation de données à caractère personnel à l'autorité de contrôle" relève de la responsabilité du responsable du traitement des données et stipule que le responsable du traitement est tenu de notifier l'ICO dans les 72 heures, et que ce délai ne commence à courir qu'à partir du moment où le responsable du traitement a pris connaissance de la violation. De même, la notification (si nécessaire) aux personnes concernées (lorsqu'il existe un risque élevé pour les droits et libertés des personnes concernées), relève de la responsabilité du contrôleur des données (GDPR Art 34).

L'article 33, paragraphe 2, s'applique à Moorepay et stipule que "le sous-traitant notifie au responsable du traitement, dans un délai raisonnable, toute violation de données à caractère personnel dont il a connaissance".

Comme défini dans le processus de gestion des incidents de sécurité, et aligné sur le GDPR, les violations de données sont rapportées aux propriétaires d'entreprise et à la haute direction, qui assurent les communications externes avec les clients dès que cela est pratiquement possible.

Si elles sont connues à ce moment-là, les informations suivantes seront fournies par Moorepay dans le cadre de la communication initiale :

- Description de la violation

- Quand et comment Moorepay a-t-il été informé de la violation ?
- Les personnes susceptibles d'avoir été affectées par la violation
- Résumé des activités de confinement
- Coordonnées pour de plus amples informations

Un plan de communication sera alors convenu avec le client et mis en œuvre pour garantir une communication continue tout au long du processus.

Alignement réglementaire Contexte

Comme défini par le GDPR et le DPA 2018, Moorepay est le processeur de données lorsqu'il traite les données des clients dans le cadre de la prestation de services à ses clients (qui sont les contrôleurs de données).

Base juridique

En tant que responsable du traitement des données, Moorepay n'a pas à déterminer la base juridique du traitement des données personnelles des clients. Les personnes concernées du client sont probablement des employés et, en tant que tels, ils peuvent très bien traiter les données personnelles dans le cadre du contrat de travail ; afin de se conformer à la législation ou à l'intérêt légitime / tâche publique (ou toute autre base juridique détaillée dans l'article 6 GDPR).

Lorsque des données à caractère personnel sensibles (catégorie spéciale) sont traitées, alors une ou des bases juridiques supplémentaires peuvent être requises, comme détaillé dans l'article 9 du GDPR et dans les sections 10 & 11 de la loi sur la protection des données 2018 (UK).

Dans tous les cas, il appartiendra au contrôleur (le client) de déterminer (et de notifier aux personnes concernées par le biais des avis de confidentialité du contrôleur) la base juridique applicable au traitement.

Finalité du traitement

Nos clients (en tant que responsables du traitement des données) devront déterminer (et communiquer aux personnes concernées par le biais d'avis de confidentialité) la finalité du traitement des données (même s'ils font appel à un tiers pour le traitement des ressources humaines et des salaires).

Consolidation des données

Les données provenant de sources multiples peuvent être reliées entre elles et faire l'objet de références croisées dans les différents composants de l'offre de produits.

Les détails de la conception spécifique du service seront inclus dans les contrats de service. De plus amples informations peuvent être fournies par le gestionnaire du compte concerné.

Catégories de personnes concernées

Moorepay traite les informations relatives à ses clients pour les catégories de personnes concernées suivantes.

- Demandeurs d'emploi
- Employés du client
- Anciens employés du client
- Plus proche parent de la personne susmentionnée

Types de données

Les données personnelles traitées par Moorepay peuvent être les suivantes :

- Nom
- Coordonnées du domicile (adresse et numéro de téléphone)
- Date et lieu de naissance
- Genre
- Droit de séjour
- Citoyenneté
- Numéro de passeport
- Courriels et/ou autres documents et données sous forme électronique
- Coordonnées bancaires et autres informations financières
- Situation familiale
- Informations sur les personnes à charge
- Nom, adresse et numéro de téléphone de la personne à contacter en cas d'urgence
- Localisation
- Groupe/ancienneté, Niveau de travail
- Informations sur le régime de rémunération
- Numéro d'identification de l'associé
- Département
- Branche et sous-branche d'activité
- Nom de l'entité de la banque locale

- Coordonnées du lieu de travail (numéro de téléphone, adresse, numéro de télécopie et adresse courriel)
- Autres informations relatives à l'adresse, le cas échéant, telles que la résidence temporaire
- Informations sur les centres de coûts
- Date de début et date de fin (le cas échéant) de l'emploi
- Dates importantes pour la carrière, telles que les événements de promotion et de réembauche
- Structure des rapports
- Dossiers de prestations et informations connexes
- Informations sur le temps et les présences, y compris les heures supplémentaires, les primes d'équipe et les remplacements.
- Modes de travail et heures de travail contractuelles, y compris les indicateurs de temps plein/partiel
- Informations relatives à la redondance
- Antécédents professionnels
- Langue(s) parlée(s)
- Informations sur la saisie-arrêt et destinataires de la saisie-arrêt
- Informations sur les pensions, y compris le régime de pension et les cotisations
- Informations relatives aux performances (actuelles et historiques, y compris les primes et les objectifs individuels)
- Informations sur le plan de développement personnel (y compris les forces et faiblesses personnelles, les domaines de développement et l'évaluation du potentiel)
- Informations concernant le droit au travail, y compris les visas
- Données relatives aux impôts et à l'assurance nationale/la sécurité sociale
- Informations relatives à la cessation d'emploi

Moorepay peut également traiter les catégories spéciales d'informations suivantes :

- Données personnelles révélant l'origine raciale ou ethnique ;
- Données personnelles révélant les opinions politiques ;
- les données à caractère personnel qui révèlent les convictions religieuses ou philosophiques (y compris les traitements nécessaires à l'établissement des déclarations fiscales) ;
- Données à caractère personnel révélant l'appartenance à un syndicat (y compris les paiements, la position et les informations bancaires) ;
- Données à caractère personnel de nature génétique ou biométrique ;

- Données personnelles concernant les informations sur la santé ;
- Données à caractère personnel révélant la vie sexuelle ou l'orientation sexuelle d'une personne physique ; ou
- Données à caractère personnel révélant des détails sur la commission (présumée) d'un acte criminel ou d'une infraction, y compris des détails sur toute procédure ou condamnation prononcée par un tribunal.

Données sur les enfants

Il n'est pas prévu que les responsables du traitement des données utilisent les services de Moorepay pour traiter les données des enfants. Toutefois, là où cela se produit, il appartient au responsable du traitement des données de veiller à ce que la transparence et la détermination de la base juridique soient respectées.

Droits des personnes concernées (y compris les droits d'accès)

Le contrôleur des données est responsable du respect de tout droit de la personne concernée (par exemple, le DAS, la rectification, l'effacement, la restriction, la portabilité, l'objection).

Là où cela est nécessaire, Moorepay, en tant que responsable du traitement des données, exécutera les instructions du contrôleur des données pour répondre aux exigences du GDPR en ce qui concerne toute demande de droits. Toute demande émanant des Personnes concernées (c'est-à-dire les employés de nos clients) doit être envoyée au Responsable du traitement des données.

Les fonctionnalités intégrées du système et les procédures opérationnelles solides garantissent que Moorepay peut exécuter les instructions du contrôleur des données en ce qui concerne les droits des personnes concernées.

Droits relatifs à la prise de décision automatisée et au profilage.

La prise de décision automatisée n'est utilisée que là où elle est nécessaire pour fournir le service contracté. Les données relatives aux clients ne sont pas utilisées à des fins de profilage.

Registres des activités de traitement (RoPA)

L'article 30 du GDPR exige que Moorepay, en tant que processeur, tienne des registres :

- Notre nom et nos coordonnées.

- Le nom et les coordonnées de chaque responsable du traitement au nom duquel nous agissons (le responsable du traitement est notre client et l'organisation qui décide pourquoi et comment les données à caractère personnel sont traitées).
- Le cas échéant, le nom et les coordonnées du représentant de chaque contrôleur (une autre organisation qui représente le contrôleur s'il est basé en dehors de l'UE mais surveille ou offre des services à des personnes dans l'UE).
- Les catégories de traitement que nous effectuons au nom de chaque contrôleur - les types de choses que nous faisons avec les données personnelles, par exemple le traitement des salaires, les services administratifs des ressources humaines.
- Le cas échéant, le nom des pays tiers ou des organisations internationales auxquels nous transférons des données à caractère personnel (tout pays ou organisation en dehors de l'UE).
- Le cas échéant, les garanties mises en place pour les transferts exceptionnels de données à caractère personnel vers des pays tiers ou des organisations internationales. Un transfert exceptionnel est un transfert non répétitif d'un petit nombre de données à caractère personnel, fondé sur un besoin professionnel impérieux, tel que visé à l'article 49, paragraphe 1, deuxième alinéa, du GDPR. (Remarque : il est peu probable que nous ayons à effectuer un transfert exceptionnel).
- Si possible, une description générale des mesures de sécurité techniques et organisationnelles (nos mesures de protection des données à caractère personnel, par exemple le cryptage, les contrôles d'accès, la formation, etc.)

La plupart de ces informations sont également contenues dans la documentation contractuelle du client (y compris le MAP).

Remarque : nos clients (les responsables du traitement des données) sont également tenus de maintenir une APR pour les données à caractère personnel qu'ils traitent. L'APR du contrôleur contiendra plus de détails sur la base juridique du traitement, etc.

Extraction / retour de données

Là où les données des clients sont renvoyées, le processus standard consiste à extraire les données et à les fournir au format Oracle Extract. D'autres formats peuvent être fournis après accord.

Pseudonymisation et anonymisation

Le cas échéant, des techniques de pseudonymisation ou d'anonymisation seront appliquées aux données à caractère personnel afin de minimiser le risque d'identification.

Exactitude des données

Pour les services SaaS, le client est responsable de l'exactitude des données.

Les systèmes de gestion des ressources humaines et des salaires utilisés dans le cadre de la prestation de services intègrent des contrôles de validation afin de garantir l'exactitude des données.

Les procédures opérationnelles intègrent des étapes de validation afin de garantir l'exactitude du traitement des données relatives aux clients.

Avis de confidentialité

Les détails sur la façon dont Moorepay utilise les données des clients (par exemple, les contacts avec les clients, etc.) en tant que contrôleur de données peuvent être trouvés dans nos avis de confidentialité accessibles sur nos sites Internet à l'adresse suivante :

Document 4 - Continuité des activités de Moorepay

Introduction

Ce document fait partie du Moorepay Assurance Pack (MAP) et doit être consulté avec tous les autres documents et artefacts inclus dans le MAP afin d'obtenir une compréhension globale du programme de sécurité de Moorepay.

Ce document a pour but de donner un aperçu du plan de continuité des activités de Zellis et de fournir une illustration de haut niveau :

- l'engagement des dirigeants
- l'approche de la planification et de l'évaluation de la continuité des activités - les garanties associées
- les analyses d'impact
- aperçu des tests

Déclaration de leadership

Moorepay s'engage fermement à fournir ses services et ses solutions selon les normes les plus élevées possibles, sans mettre en danger la santé et le bien-être de ses collègues ou de ses clients.

Là où une pandémie est déclarée, il y a un certain nombre de considérations essentielles à prendre en compte et une série de scénarios qui pourraient se concrétiser.

Nos plans d'intervention et d'urgence sont continuellement revus et ajustés pour s'aligner sur les lignes directrices publiées par l'OMS et par le gouvernement.

Les principaux fournisseurs tiers de notre chaîne d'approvisionnement sont pleinement engagés avec Moorepay pour s'assurer qu'ils ont mis en place des plans de continuité des activités appropriés.

Approche

Les objectifs de la gestion de la continuité des activités (BCM) sont les suivants :

- Attribuer les rôles et responsabilités appropriés pour la gestion de la continuité des activités, se préparer à un incident majeur et s'assurer que la réponse à un incident majeur bénéficie du niveau de soutien approprié de la part des fonctions clés de l'entreprise.
- Veiller à ce qu'une analyse d'impact sur les activités (BIA) et une évaluation des risques soient réalisées pour toutes les activités, tous les produits et tous les services critiques.
- Veiller à ce que des plans de reprise documentés soient maintenus et révisés régulièrement pour les activités qui fournissent et soutiennent des produits et services critiques.
- Effectuer des exercices et des tests selon un calendrier convenu, en veillant à ce que les résultats soient évalués et à ce que les lacunes éventuelles soient enregistrées, les mesures d'amélioration étant documentées et les propriétaires convenus.
- Veiller à ce que l'ensemble du personnel reçoive une formation appropriée pour s'acquitter de ses tâches dans le cadre des activités de préparation et d'intervention en matière de gestion des crises.
- Veiller à ce que des audits internes et des revues de direction soient effectués à des intervalles convenus afin de garantir l'efficacité du système de gestion de la continuité des activités.

Garantie BCM

Les types de documents suivants sont intégrés dans le plan de continuité des activités :

Politique

La politique de Moorepay en matière de continuité des activités décrit les buts et les objectifs du système de gestion de la continuité des activités de Moorepay (BCMS) et définit les exigences de la politique en termes de ce qui suit :

- Responsabilités

Considérations relatives à la sécurité de l'information

- Analyse de l'impact sur l'entreprise et évaluation des risques
- Planification et réaction en cas d'urgence
- Essais

Évaluation et planification de la continuité des activités

Le document d'évaluation et de planification contient les résultats de l'évaluation des menaces et de l'analyse de l'impact sur les activités, telles que décrites dans la section "Évaluation de l'impact" du présent document.

Moorepay utilise une approche PESTEL pour l'analyse de l'impact sur les entreprises, qui prend en compte les facteurs de menace dans les domaines suivants : politique, économique, social, technologique, environnemental et juridique.

Les calculs de risque suivent la méthodologie standard de Moorepay en matière de gestion des risques afin de garantir la cohérence et la reproductibilité.

Playbook

Document de planification basé sur des faits fournissant un inventaire des ressources, des capacités, des fournitures et des dépendances de service à utiliser avec le Runbook.

Manuel d'utilisation

Le runbook est un guide d'instruction pratique basé sur les processus pour gérer les incidents avant et après l'invocation, et comprend les informations suivantes :

- Des organigrammes de processus qui suivent une approche basée sur le risque
- Séquence d'activités à entreprendre, étape par étape, en cas de déclaration d'un événement de continuité des activités.
- Rôles et responsabilités clairement définis pour chaque étape du processus

- Des instructions détaillées pour chaque étape du processus Les runbooks sont pratiques et conviviaux.

Analyse d'impact

L'évaluation de l'impact est entreprise dans le cadre de la planification de la continuité des activités. Les sources de menace, les facteurs de menace et les facteurs de vulnérabilité sont définis pour chaque scénario de continuité des activités et peuvent inclure les domaines suivants, sans toutefois s'y limiter :

- Risque de dommages ou de refus d'accès aux sites
- Indisponibilité du personnel clé
- Indisponibilité de l'infrastructure et des technologies informatiques critiques
- Indisponibilité des services des fournisseurs essentiels

Les risques sont identifiés et des mesures d'atténuation sont définies et intégrées dans le plan de continuité des activités.

Là où c'est nécessaire, des évaluations de l'impact sur la vie privée (DPIA) sont entreprises pour définir les flux de données et les activités de traitement pertinents.

L'analyse de l'impact sur l'entreprise est effectuée pour chaque service fourni par le site et prend en considération les éléments suivants :

- Temps maximum sans service (MTWS) - le temps maximum pendant lequel l'entreprise pourrait continuer à fonctionner sans que cette activité ne soit effectuée.
- Objectif de temps de rétablissement (RTO) - le temps prévu pour que le service soit disponible après une interruption.

L'analyse des incidences sur l'activité et la planification de la reprise associée garantissent qu'il existe une marge de manœuvre suffisante entre l'OTR et le MTWS pour que l'OTR soit réalisable.

Des exercices sont menés pour s'assurer que le RTO reste réalisable et que les activités d'amélioration continue creusent l'écart entre le RTO et le MTWS afin de disposer d'une marge de manœuvre suffisante.

Test de continuité des activités

Les tests de continuité des activités sont conçus pour

- Examiner et évaluer la solidité de nos plans
- Sensibiliser et éduquer les employés sur la manière de réagir en cas de continuité des activités.
- Tester les capacités à reprendre le contrôle de la situation le plus rapidement possible
- Identifier les nouvelles menaces et les évaluer à l'aide de notre méthodologie basée sur les risques
- Saisir les opportunités d'amélioration pour renforcer nos plans de continuité des activités et de reprise après sinistre

Test du plan de reprise après sinistre Nuage privé

Des tests de reprise après sinistre des applications sont effectués au moins une fois par an ou lorsque des changements importants interviennent dans l'infrastructure d'hébergement, afin de confirmer que les exigences en matière de reprise peuvent être satisfaites. Les clients sont invités à participer aux exercices de reprise.

Les tests de reprise après sinistre sont effectués dans le centre de données secondaire.

Les données sont répliquées au niveau de la couche SAN du centre de données primaire au centre de données secondaire 24 heures sur 24, 7 jours sur 7, et ces données sont utilisées dans les tests de récupération.

Une copie ponctuelle des données est effectuée et mise en correspondance avec les profils d'hôte des serveurs à récupérer.

Les serveurs sont mis en ligne, un ensemble de tests prédéfinis est ensuite exécuté sur les systèmes et une comparaison identique est effectuée avec les serveurs concernés dans le centre de données principal.

Des tests de restauration des données à partir du système de sauvegarde sont effectués et testés pour confirmer l'intégrité des données et l'efficacité de la solution de sauvegarde.

Une fois les tests de reprise de l'infrastructure terminés, les équipes chargées des applications et des bases de données effectuent les restaurations nécessaires et présentent les applications récupérées aux clients et aux équipes internes pour qu'ils les testent individuellement.

Le temps de restauration global de bout en bout est mesuré par rapport au RTO publié de 24 heures.

Le RTO est calculé sur la base d'une remise en service complète de toutes les plateformes et ne prend pas en compte les systèmes individuels.

Les clients participants reçoivent un rapport de synthèse à la fin du rapport.

Document 5 - Aperçu de la sécurité de l'application Moorepay

Introduction

Ce document fait partie du Moorepay Assurance Pack (MAP) et doit être consulté avec tous les autres documents et artefacts inclus dans le MAP afin d'obtenir une compréhension globale du programme de sécurité de Moorepay.

La sécurité des applications de Moorepay et HRWize est une priorité absolue en raison de la nature sensible des données présentées aux utilisateurs. Ce document vise à fournir une vue d'ensemble des fonctions de sécurité disponibles à la fois dans les applications et dans la conception du système.

Moorepay Gestion de l'identité et de l'accès Fonctionnalité de connexion sécurisée

L'autorisation est toujours effectuée au sein de Moorepay, il y a une seule étape où l'utilisateur doit fournir un nom d'utilisateur, un mot de passe. Le profil de sécurité de l'utilisateur est référencé pour déterminer les droits d'accès de l'utilisateur. L'authentification est assurée par le service d'identité de Moorepay qui peut être relié à l'extérieur ou à l'intérieur de l'application.

Les messages de connexion invalide ne précisent pas si c'est le nom d'utilisateur ou le mot de passe qui est incorrect.

Une liste blanche d'adresses IP est disponible et peut être appliquée aux utilisateurs. Il peut s'agir de n'importe quelle adresse IP publique ou d'une plage CIDR.

L'authentification multifactorielle (MFA) est disponible en option (sous réserve de l'offre de services) et ajoute une couche de protection supplémentaire à votre nom d'utilisateur et à votre mot de passe.

Signature unique

Moorepay supporte l'authentification unique en utilisant OpenID Connect par le biais du service d'identité de Moorepay.

OpenID Connect est une couche d'authentification construite au-dessus du cadre Oauth2.0 qui utilise un jeton web JSON (JavaScript Object Notation) pour valider l'authenticité d'un utilisateur, ce qui permet à l'utilisateur d'accéder à des sites web et à des applications sans avoir à se connecter ou à partager à nouveau ses informations d'identification.

Moorepay prend également en charge l'authentification unique basée sur un jeton USB en utilisant les services d'identité de Moorepay.

Authentification multi-facteurs (MFA)

Le processus de connexion avec le nom d'utilisateur et le mot de passe authentifie l'utilisateur avec "ce qu'il sait". L'AMF introduit un niveau supplémentaire d'authentification avec "ce qu'ils ont".

Notre solution incorpore les mécanismes de sécurité standard de l'industrie, vous pouvez basculer MFA sur Moorepay et sélectionner l'une des deux méthodes d'authentification secondaire ou les deux. Les deux méthodes reçoivent un code d'accès à usage unique que l'utilisateur doit saisir au moment de la connexion.

Lors de l'authentification auprès d'un domaine d'entreprise tel que Azure Active Directory (AAD), tout MFA en place tel que Microsoft Authenticator sera hérité et demandé lorsque l'utilisateur se connecte au domaine.

Politique de Moorepay en matière de mots de passe

Dans Moorepay, la fonctionnalité du mot de passe ne peut pas être réinitialisée car il s'agit d'un paramètre global de l'application :

- Longueur minimale 9
- Longueur maximale 128
- 5 tentatives de connexion au maximum, avec verrouillage temporisé.
- Nombre minimum de caractères alphabétiques majuscules de 1
- Minimum Caractères numériques et symboles 1 de chaque
- Un masque de mot de passe.

Les clients de Moorepay peuvent définir leur propre politique de mot de passe en utilisant l'authentification unique (Single Sign On) dans leur domaine d'entreprise.

Question de sécurité

Moorepay demande à l'utilisateur de répondre à des questions secrètes pour la réinitialisation du mot de passe lorsqu'il n'utilise pas le Single Sign On. La réinitialisation du mot de passe enverra un jeton temporisé à l'utilisateur afin de

être en mesure de réinitialiser leur mot de passe après avoir répondu correctement à leurs questions de sécurité secrètes qui sont définies lors de la première connexion.

Rôle de l'administrateur

Moorepay dispose d'un module d'administration distinct qui gère les utilisateurs et la sécurité. Les utilisateurs dont le profil comprend le module d'administration peuvent effectuer les tâches administratives suivantes :

Moorepay

- Accès aux profils de sécurité
- Limiter l'accès des opérateurs aux dossiers des employés par le biais de profils de sécurité
- Création de nouveaux opérateurs et attribution d'un profil de sécurité
- Modifier le profil de sécurité d'un opérateur
- Modifier le mot de passe d'un opérateur Moorepay
- Exécuter les rapports de l'outil d'interrogation

Moorepay Me

- Attribuer, modifier ou suspendre un mot de passe pour un employé

Accès de Moorepay aux données

Les employés de Moorepay chargés des opérations de service, et les partenaires agréés qui ont été désignés pour fournir le service, peuvent avoir accès aux informations du client dans le but de remplir leur rôle dans le contexte convenu du service.

Dans le cas d'une implémentation du logiciel Moorepay, la majorité des accès aux données sera réservée au personnel du client ; toutefois, les administrateurs du système Moorepay et le personnel d'assistance peuvent également avoir un accès indirect aux données.

Des contrôles d'accès robustes sont en place pour gérer l'accès de Moorepay aux données des clients, en veillant à ce que :

- L'accès est approuvé avant d'être attribué

- L'accès est attribué sur la base du "besoin d'utilisation".
- L'accès est limité dans le temps et l'attribution est revue régulièrement
- L'activité est contrôlée

Audit de l'application Moorepay

L'audit au sein de Moorepay est en partie configurable et sous le contrôle de l'équipe de Moorepay.

Moorepay utilise des tâches et des tables de base de données pour saisir et stocker les données.

- une tâche est un ensemble d'écrans que vous pouvez configurer pour vous assurer que les bons écrans sont disponibles pour la tâche que vous cherchez à effectuer
- une table ou un fichier se situe au niveau de la base de données et sert à stocker des données spécifiques associées à un enregistrement dans le système

Au sein des tâches, il y aura des tables différentes pour chaque ensemble de données, c'est-à-dire qu'il y aura une table pour contenir les informations fiscales et une ou plusieurs tables différentes pour les informations personnelles.

Les enregistrements d'audit comprennent l'ancienne et la nouvelle valeur, la date et l'heure de la modification, et l'opérateur qui a effectué la modification.

L'extracteur peut être utilisé pour interroger les données d'audit.

Les changements de Moorepay Me peuvent également être vérifiés par le même mécanisme.

Cryptage Moorepay

Cryptage du stockage des données (au repos)

Les bases de données de Moorepay sont stockées sur un réseau de stockage SAN qui est crypté à l'aide d'un disque entier.

le cryptage. Au moment de la rédaction du présent document, les codes de cryptage déployés sont conformes à la norme AES-256.

Protection par mot de passe

Les mots de passe sont stockés dans la base de données du service d'identité de Moorepay.

Le serveur d'identité Moorepay utilise un hachage à sens unique avec PBKDF2 avec HMAC-SHA256, sel de 128 bits, sous-clé de 256 bits, 10000 itérations.

HTTPS et SSL

Moorepay est configuré par défaut pour n'autoriser que l'accès via HTTPS.

HTTPS crypte et décrypte les demandes de pages et les informations sur les pages entre le serveur et l'ordinateur.

Le protocole HTTPS permet de relier le navigateur du client et le serveur web au moyen d'un protocole SSL (Secure Socket Layer). Par défaut, HTTPS utilise le port 443 par opposition au port HTTP standard de 80. URL commençant par HTTPS

indiquent que la connexion entre le client et le navigateur est cryptée à l'aide du protocole SSL. La mise en œuvre de SSL et l'utilisation de HTPPS offrent un niveau de sécurité beaucoup plus élevé que la soumission de requêtes via HTTP uniquement.

Transfert de fichiers par Internet

Le transfert de fichiers par Internet se fait via un portail SFTP pour les clients qui n'utilisent pas l'application Moorepay Payroll, le portail SFTP utilise des identifiants uniques par client. Les protocoles SFTP et FTPS utilisent les algorithmes de cryptage SSL/TLS/SSH avec une longueur de clé de 256 lorsque les systèmes cibles le permettent.

Moorepay Cookies de session

Moorepay est configuré par défaut pour utiliser des cookies de session afin de maintenir l'affinité de session.

Une fois l'utilisateur connecté, chaque application établit un simple cookie de session afin que les données de l'utilisateur soient "mémorisées" entre les requêtes de page.

L'expiration de la session par défaut est fixée à trente minutes d'inactivité pour Moorepay. Cette durée est généralement considérée comme optimale pour ce type d'application, de sorte que les tâches habituelles des employés et des gestionnaires en matière de ressources humaines ne soient pas affectées.

Conservation des données

Par défaut, les données sont conservées pendant la durée du contrat avec le client. Les données peuvent être supprimées conformément aux directives du HMRC et les

personnes qui quittent l'entreprise peuvent être supprimées après 4 ans, conformément aux périodes de conservation des données de l'employeur.

Suppression des données

Le module GDPR fourni dans le cadre de Moorepay offre la fonctionnalité suivante de suppression des données :

- Suppression en bloc Départs, candidats et personnel externe
- Suppression individuelle

Demandes des personnes concernées

Des tâches spécifiques sont disponibles dans le module GDPR de Moorepay, qui permettent aux utilisateurs autorisés d'exécuter des rapports sur toutes les données associées à un utilisateur spécifique.

Architecture de Moorepay Segmentation des données

Un environnement dédié aux applications Moorepay est partagé entre les clients au sein de notre locataire Azure. Des schémas de données et des systèmes de fichiers dédiés sont fournis par client au sein de notre infrastructure virtualisée. Cela offre des garanties importantes en matière de confidentialité et de sécurité des données et signifie que les données ne sont pas mélangées avec celles d'autres clients. D'importantes mesures de protection de la confidentialité et de la sécurité des données sont déployées dans l'environnement hébergé ; par exemple, chaque service se voit attribuer sa propre plage d'adresses de sous-réseau, son propre ensemble de règles sur nos pare-feu périphériques.

Séparation des réseaux

Moorepay se compose des niveaux de prestation de services suivants :

- Présentation (MVC)
- API
- Micro Services
- Services de logique d'entreprise/traitement par lots
- Base de données

Une séparation logique est mise en œuvre pour séparer chaque niveau de livraison.

Architecture de l'application

HRWize Gestion des identités et des accès Fonctionnalité de connexion sécurisée

L'autorisation est toujours effectuée dans HRWize, il y a une seule étape où l'utilisateur doit fournir un nom d'utilisateur et un mot de passe ou un nom d'utilisateur, un mot de passe et un code PIN.

- Il s'agit d'un code PIN à 6 chiffres et l'utilisateur est invité à saisir 3 chiffres aléatoires de ce code PIN.
- La connexion par code PIN est activée globalement et deux options s'offrent à vous : tous les utilisateurs OU uniquement les utilisateurs des RH et les administrateurs.

Le profil de sécurité de l'utilisateur est référencé pour déterminer les droits d'accès de l'utilisateur. L'authentification est assurée à partir de l'application.

Les messages de connexion invalide ne précisent pas si c'est le nom d'utilisateur ou le mot de passe qui est incorrect.

Les pages de connexion sont protégées par Google reCaptcha v3 - il s'agit d'un processus transparent (contrairement aux anciennes versions qui vous demandent d'entrer des lettres ou de cliquer sur des bouches d'incendie, etc.)

Une liste blanche d'adresses IP est disponible et peut être appliquée aux utilisateurs. Il peut s'agir de n'importe quelle adresse IP publique ou d'une plage CIDR.

L'authentification multifactorielle (MFA) est disponible en option (sous réserve de l'offre de services) et ajoute une couche de protection supplémentaire à votre nom d'utilisateur et à votre mot de passe.

Signature unique

HRWize prend en charge l'authentification unique auprès de différents fournisseurs d'identité, énumérés ci-dessous ;

- Azure Active Directory
- Okta
- OnleLogin
- Google oAuth
- Google SAML

Authentification multi-facteurs (MFA)

Le processus de connexion avec le nom d'utilisateur et le mot de passe authentifie l'utilisateur avec "ce qu'il sait". L'AMF introduit un niveau supplémentaire d'authentification avec "ce qu'ils ont".

Notre solution intègre des mécanismes de sécurité standard, vous pouvez activer MFA sur HRWize et l'authentification est basée sur les QR Codes en utilisant diverses applications d'authentification telles que Microsoft Authenticator, Google Authenticator ou Authy.

La connexion MFA peut être activée globalement pour tous les utilisateurs ou spécifiquement pour les utilisateurs RH et administrateurs.

Lors de l'authentification auprès d'un domaine d'entreprise tel que Azure Active Directory (AAD), tout MFA en place tel que Microsoft Authenticator sera hérité et demandé lorsque l'utilisateur se connecte au domaine.

Politique de mot de passe HRWize

- Dans HRWize, les clients peuvent configurer certains éléments de leur politique en matière de mots de passe.
- Longueur minimale - Configurable par le client - minimum 8
- Pas de longueur maximale
- Le nombre de tentatives de connexion est limité à 5, avec un délai de blocage. 15 tentatives bloquent l'IP.
- Changement forcé du mot de passe - Configurable par le client

Les clients de HRWize peuvent entièrement définir leur propre politique de mot de passe en utilisant l'authentification unique (Single Sign On) sur leur domaine d'entreprise.

Accès aux données par Moorepay/HRWize

Dans le cadre d'une implémentation HRWize, la majorité de l'accès aux données est réservée au personnel du client ; cependant, les administrateurs du système HRWize, le personnel d'implémentation et d'assistance peuvent également avoir un accès indirect aux données du client.

Des contrôles d'accès robustes sont en place pour gérer l'accès de Moorepay/HRWize aux données des clients, en veillant à ce que :

- L'accès est approuvé avant d'être attribué
- L'accès est attribué sur la base du "besoin d'utilisation".

- L'accès est limité dans le temps et l'attribution est revue régulièrement
- L'activité est contrôlée

Audit des applications HRWize

HRWize dispose d'une fonction d'audit qui vérifie toutes les actions entraînant une modification de la base de données, c'est-à-dire toutes les actions d'écriture, de mise à jour et de suppression. D'autres actions significatives telles que les connexions, l'exécution d'un rapport, le téléchargement de données de formulaires et la consultation de documents sont également auditées.

Le journal d'audit n'est visible que par les utilisateurs de niveau administrateur. Les informations sont accessibles via le module d'audit ainsi que via les rapports.

Le format d'un enregistrement d'audit est le suivant :

Datetime - elle est toujours enregistrée en UTC Username

Adresse IP

Action - le format exact varie en fonction du cas d'utilisation, mais il suit généralement le format suivant : "Mise à jour des coordonnées bancaires : Phoebe Parker (47)" ou "Ajout d'un temps libre : Maladie (2023-07-20 - 2023-07-21) Aimee Hancock (G7LQE7) (390)"

HRWize Encryption

Cryptage du stockage des données (au repos)

Les bases de données de HRWize sont cryptées au repos - au moment de la rédaction du présent document, les codes de cryptage déployés sont conformes à la norme AES-256.

En outre, certains champs de la base de données sont cryptés au niveau du champ :

- Numéro d'assurance nationale
- Date de naissance
- Code de tri du compte bancaire
- Numéro de compte bancaire
- Banque IBAN
- Code Swift de la banque
- Numéro de permis de conduire
- Numéro de passeport

Protection par mot de passe

Les mots de passe sont stockés dans la base de données de l'application HRWize. Les mots de passe sont salés et hachés à l'aide de BCrypt avec un coût de 10. HTTPS et SSL.

HRWize est configuré par défaut pour n'autoriser que l'accès via HTTPS.

HTTPS crypte et décrypte les requêtes et les informations de la page entre le navigateur du client et le serveur web à l'aide de Transport Layer Security (TLS 1.2), anciennement Secure Socket Layer (SSL). Par défaut, HTTPS utilise le port 443 par opposition au port HTTP standard de 80. Les URL commençant par HTTPS indiquent que la connexion entre le client et le navigateur est cryptée à l'aide de TLS 1.2. La mise en œuvre de TLS 1.2 et l'utilisation de HTPPS offrent un niveau de sécurité bien plus élevé que l'envoi de requêtes via HTTP uniquement.

Cookies de session HRWize

HRWize utilise des cookies de session pour maintenir l'affinité de la session. Une fois connecté, chaque application établit un simple cookie de session afin que les détails de l'utilisateur soient "mémorisés" entre les requêtes de page.

Le cookie utilisé est un cookie HTTP et nous utilisons un cookie sécurisé.

L'expiration de la session est fixée par défaut à trente minutes d'inactivité, mais cette durée peut être modifiée par l'entreprise jusqu'à un maximum de 240 minutes (4 heures).

HRWize Gestion des données Conservation et suppression des données

HRWize ne supprime aucune donnée client et, par conséquent, la conservation des données est infinie si le client le souhaite - en tant que responsable du traitement des données, nous n'agirons jamais qu'en conformité avec les instructions du responsable du traitement des données.

Si vous décidez de supprimer des données, vous pouvez supprimer des enregistrements individuels via les modules appropriés de HRWize - en outre, beaucoup de ces modules ont la capacité de sélectionner et de supprimer des enregistrements en vrac pour rendre ce processus plus rapide.

Lorsque vous supprimez des données, vous ne supprimez en général que l'enregistrement en question - par exemple une demande de formation. En revanche, si

vous supprimez un employé, vous supprimez l'employé et TOUS les enregistrements associés, y compris les documents.

Demandes d'accès des personnes concernées

Si une personne fait une demande d'accès, HRWize permet au responsable du traitement d'effectuer une recherche dans l'ensemble du système sur la base de l'entité de l'employé - il est à noter que cette recherche ne trouvera pas les cas où l'employé est référencé dans un autre enregistrement (par exemple, si son nom est mentionné dans l'évaluation des performances de quelqu'un d'autre, cela ne sera pas pris en compte).

Une fois la recherche terminée, vous pouvez télécharger toutes les données contenues dans le système au format HTML, PDF ou XML, ce qui vous permet de les partager avec le sujet une fois que vous en avez confirmé le contenu conformément à vos politiques.

Architecture HRWize

Segmentation des données clients

La base de données de HRWize est multilocataire et les données sont séparées à l'aide d'identifiants uniques par client et d'une sécurité d'application.

Séparation des réseaux

HRWize se compose des niveaux de prestation de services suivants :

- Application
- API
- Base de données

Architecture de l'application

Centres de données

Tous les centres de données utilisés pour fournir les services HRWize sont situés au Royaume-Uni.

Les services sont fournis dans une combinaison de centres de données Actif, utilisant des offres de cloud public, et de centres de données tiers distincts hébergeant des actifs matériels et logiciels loués, détenus, gérés et entretenus par Moorepay/HRWize.