OCIM

Politique de sécurité de l’information

V.1

01/01/2023

HISTORIQUE DES APPROBATIONS ET DES RÉVISIONS

La Société a approuvé la présente Politique de sécurité de l'information et la réexaminera et la mettra à jour périodiquement, le cas échéant.

Date d'entrée en vigueur	Version	Changements apportés	Signatures
1er janv. 2023	1.0	Création d'une politique de sécurité de l'information	Laurent Mathiot, Directeur général Arnaud Lapière, Directeur de la technologie

Table des matières

I. INTRODUCTION

OCIM Finance (« OCIM ») est un groupe de sociétés privées dont le siège se situe à Paris. Il est détenu et financé par la famille Mathiot. Initialement spécialisée dans l'immobilier, la famille Mathiot s'est diversifiée dans d'autres activités, y compris, mais sans s'y limiter, le financement et le négoce de métaux précieux et stratégiques par l'intermédiaire d'OCIM. L'expansion des activités financières du groupe a également entraîné une expansion géographique, avec la création d'une filiale à Genève.

OCIM est la société holding du groupe ; OCIM Metals & Mining SA (« OMM ») et Electrum SA (« Electrum ») sont deux des principales filiales du groupe. OMM est un négociant en métaux et un financier spécialisé dans l'or, l'argent et le platine. Il est présent à Paris et à Genève, tandis qu'Electrum est une filiale de trading permettant de soutenir les activités du groupe, principalement à des fins d'absorption et de gestion des risques, et possède des équipes à Paris et à Genève.

II. OBJET

OCIM, ses sociétés affiliées et ses entités liées (ci-après dénommées « la Société » ou « OCIM ») s'engagent à respecter les normes les plus strictes en matière de professionnalisme et de conduite éthique dans tous les aspects de leurs activités et attendent de leurs Représentants (par exemple, la direction, les employés, les tiers apparentés, etc.) qu'ils garantissent les normes éthiques les plus élevées et qu'ils respectent toutes les lois en vigueur.

La présente Politique de sécurité de l'information (la « Politique ») vise à sensibiliser ses lecteurs aux questions relatives à la sécurité des informations et à établir des règles pour gérer, régir et appliquer le programme de gestion de la sécurité des informations. La présente Politique vise à compléter, sans les remplacer, les lois applicables régissant les exigences en matière de sécurité de l'information applicables à la Société et à ses filiales.

L'objectif de cette Politique est d'énoncer les principes, le cadre et le raisonnement qui sous-tendent les règles d'usage d'OCIM en matière de sécurité de l'information.

Le cadre de la Politique de sécurité de l'information d'OCIM définit des mesures de contrôle de base que tout collaborateur d'OCIM est censé connaître et suivre de manière cohérente. L'objectif du cadre de sécurité et de ses politiques connexes est de définir des niveaux de sécurité minimaux acceptables pour la Société et de les mettre en œuvre de manière cohérente au sein de l'ensemble de la Société.

Le niveau minimum est défini de manière à prévenir la plupart des risques de sécurité anticipés, tout en offrant à la Société et à ses filiales la possibilité d'adapter les normes et procédures locales pour répondre à leurs besoins quotidiens en matière de sécurité.

En outre, la Politique est conçue pour prévenir la plupart des risques anticipés en fonction des opérations existantes et de la taille de la Société. Par conséquent, la Politique doit être régulièrement mise à jour au fur et à mesure que la Société modifie ses activités et se développe. Tout changement important dans la taille, la portée, les activités, les opérations ou les actifs informationnels de la Société doit donner lieu à une révision et à une mise à jour de la présente Politique. Un registre des versions antérieures et un historique appropriés doivent également être mis en place pour rester cohérent avec les progrès technologiques. Ces registres sont conservés au service d'archivage avec toutes les autres politiques et activités d'archivage d'OCIM.

II.A. DÉROGATIONS

Toute demande de dérogation aux exigences de la présente Politique ou à la Politique elle-même doit être soumise par écrit au Directeur de la technologie qui l'étudiera. La demande de dérogation **doit** préciser :

- La raison professionnelle de la demande ; et
- L'exigence ou la section spécifique de la Politique au sujet de laquelle la modification ou la dérogation est demandée.

Le Directeur de la technologie s'entretiendra avec les parties prenantes appropriées, y compris, mais sans s'y limiter, les Services juridiques et de gestion des risques, afin de juger de la nécessité d'un examen et d'une évaluation plus approfondis.

Les dérogations sont limitées dans le temps pour une durée raisonnable, en fonction des besoins de l'entreprise et du niveau de risque encouru. Si la durée de la dérogation est supérieure à un (1) an, la mise à jour et/ou la modification des politiques et des procédures sera envisagée.

À l'expiration d'une dérogation, le risque doit être réexaminé et le Directeur de la technologie ou le service juridique/conseil décidera de prolonger la dérogation ou de prendre toute autre mesure supplémentaire.

III. CHAMP D'APPLICATION

La présente Politique s'applique aux employés, dirigeants, gestionnaires, administrateurs, cadres supérieurs, employés temporaires, entrepreneurs, consultants, intérimaires et autres travailleurs d'OCIM, ainsi qu'à tous les vendeurs et tiers qui créent, reçoivent, stockent, utilisent, rencontrent ou transmettent des informations relatives à OCIM. Cette Politique couvre les informations stockées ou partagées par tous les moyens, y compris les informations électroniques et papier, et les informations partagées à l'oral ou de manière visuelle (notamment par téléphone et vidéoconférence). Aux fins du présent document, les composants de l'infrastructure se limitent à l'infrastructure d'OCIM nécessaire à ses activités.

IV. DÉFINITIONS

Une « **politique** » désigne une ligne de conduite ou une méthode d'action obligatoire et définitive que la direction choisit pour guider et déterminer les décisions présentes et futures. La politique est indépendante des technologies ou des solutions spécifiques. Les experts en sécurité, en conformité et en diverses technologies spécifiques mettent à jour toutes les politiques, au moins une fois par an.

Une « **règle d'usage** » désigne un mécanisme permettant de mettre en œuvre les orientations politiques de la direction générale. Les règles d'usage font référence aux normes et procédures nécessaires à la mise en œuvre d'une politique.

Une « **norme** » désigne un ensemble d'exigences obligatoires et spécifiques visant à répondre à des objectifs ambitieux définis dans une politique. OCIM doit identifier les pratiques industrielles communes applicables à son activité et à ses filiales et faire en sorte que les contrôles de sécurité soient cohérents avec ces exigences ou utiliser les exigences pour cadrer les normes, et enfin les personnaliser pour répondre aux exigences de la politique de l'organisation. Dans de rares cas, les services de l'entreprise peuvent faire des demandes de dérogations aux normes, à condition de suivre une procédure de demande de dérogation formelle.

Une « **procédure** » désigne un ensemble d'instructions spécifiques et systématiques qui décrivent la manière de respecter les exigences décrites dans une norme ou une ligne directrice. Ces documents changent fréquemment en fonction de la technologie et/ou de l'équipe ou de la personne chargée de la tâche.

Une « **ligne directrice** » désigne un ensemble de recommandations facultatives qui étayent une norme spécifique. OCIM révise les lignes directrices en fonction des besoins.

Un « **accord juridique** » ou « **contrat** » fait référence à tous les instruments écrits, accords, documents, signatures d'actes, procurations, transferts, cessions, contrats, obligations, certificats et autres instruments de quelque nature que ce soit conclus par OCIM (par exemple, contrat-cadre, accord de

confidentialité, énoncé des travaux).

Ce document définit les autorisations. Chaque autorisation est caractérisée par l'un des mots suivants :

- « **devra** » ou « **doit** » indique une activité ou une fonction que la personne concernée est obligée d'accomplir et qu'elle ne peut ni refuser ni déléguer.
- **« devrait »** indique une activité ou une fonction dont la personne concernée est responsable, mais qui peut déléguer son exécution spécifique.
- **« peut »** indique une activité ou une fonction que la personne concernée est capable d'accomplir parmi ses autres tâches.

V. RÔLES ET RESPONSABILITÉS

OCIM utilise les classifications suivantes pour décrire les personnes qui utilisent les actifs numériques d'OCIM :

Utilisateur : toute personne utilisant les actifs informationnels d'OCIM à des fins commerciales légitimes, y compris les tiers externes, tels que les vendeurs et les entrepreneurs. L'utilisateur est tenu de respecter les exigences énoncées dans la présente Politique. Les utilisateurs sont tenus de signaler tout manquement à la présente Politique. Chaque utilisateur doit préserver la confidentialité des informations, même en cas de défaillance ou d'absence de mécanismes techniques de sécurité.

Responsable informatique : toute personne explicitement désignée comme responsable du maintien des opérations et de la sécurité des actifs informationnels d'OCIM. Le Responsable informatique, ou son délégué, doit veiller à ce que les exigences énoncées dans la présente Politique soient respectées. Le Responsable informatique doit informer la direction de toute violation de la présente Politique et prendre les mesures correctives correspondantes. Les mesures correctives seront prises dans un délai raisonnable en fonction du risque et en accord avec la direction.

Direction : toute(s) personne(s) explicitement désignée(s) comme responsable(s) des opérations et tenue(s) à une obligation fiduciaire envers OCIM. La direction est tenue de superviser et d'orienter le programme de sécurité de l'information et d'approuver la présente Politique.

Visiteur/Invité : toute personne ayant besoin d'accéder de manière temporaire aux actifs informationnels d'OCIM à des fins limitées ou non professionnelles (par exemple, accès au Wi-Fi ou à l'imprimante pour les invités). Les Visiteurs et/ou Invités n'auront pas accès aux informations décrites dans la Politique d'identification et de classification des données. Le Responsable informatique configurera les actifs informationnels de sorte qu'un Visiteur et/ou un Invité ne puisse accéder à aucune information interne d'OCIM (par exemple, segmentation des systèmes, réseaux réservés aux invités, etc.) Les Visiteurs et/ou les Invités ne se verront pas attribuer de compte d'utilisateur OCIM.

VI. POLITIQUE D'IDENTIFICATION ET DE CLASSIFICATION DES DONNÉES

La Politique d'identification et de classification des données définit les objectifs d'OCIM en matière d'établissement de normes spécifiques permettant l'identification, la classification et l'étiquetage des actifs informationnels d'OCIM. Cette Politique fournit les règles d'usage en matière de protection des données critiques pour l'organisation et tous les employés doivent avoir connaissance de ces classifications et procédures de traitement.

La classification des données se divise en quatre niveaux en fonction de leur sensibilité, de leur criticité et de leur valeur. Les données doivent être classées en fonction de l'un des quatre (4) niveaux suivants : Restreint/Exclusif, Confidentiel, Sensible ou Public. Toutes les données nécessitent un certain niveau de protection, mais plus leur sensibilité, leur criticité et leur valeur augmentent, plus les contrôles de sécurité doivent être importants. Les contrôles de sécurité doivent être mis en œuvre en fonction de la valeur, de la sensibilité et du risque des données, et conformément aux exigences légales et réglementaires.

Niveau I : Restreint/Exclusif

Concerne les données de nature stratégique, exclusive ou critique. La perte ou l'endommagement de ces données pourrait avoir des conséquences négatives **graves ou catastrophiques** sur la capacité de l'organisation à poursuivre ses activités, des conséquences négatives **graves ou catastrophiques** sur la réputation de l'organisation, des conséquences négatives **graves ou catastrophiques** sur le personnel ou les biens de l'organisation. Ces données sont destinées à être utilisées au sein de l'organisation et par les personnes qui ont un besoin professionnel légitime d'y accéder. Toute diffusion externe intentionnelle de ces données à des fins commerciales légitimes (par exemple, régulateurs, investisseurs stratégiques, conseillers externes, etc.) doit être gérée par les Services juridiques et de gestion des risques.

Niveau II : Confidentiel

Concerne les données dont l'accès non autorisé, la compromission ou la destruction entraînerait de **graves** dommages pour OCIM, ses clients ou ses employés (par exemple, les numéros d'identification, les dates de naissance, les informations relatives à la santé, les informations financières, etc. ou, collectivement, les « données personnellement identifiables » ou « données personnelles »). Ces données sont destinées à être utilisées au sein de l'organisation et par les personnes (internes ou externes) ayant un besoin professionnel légitime d'y accéder.

Niveau III : Sensible

Concerne les données qui doivent rester confidentielles pour des raisons d'éthique ou de protection de la vie privée. L'utilisation, l'accès, la divulgation, l'acquisition, la modification, la perte ou la suppression non autorisés de données appartenant à ce niveau pourraient entraîner des pertes financières, nuire à la réputation d'OCIM ou enfreindre tout droit à la vie privée d'une personne. Il s'agit notamment de données réservées à un usage exclusivement lié aux activités d'OCIM.

Niveau IV : Public

Concerne les données qui ne sont pas diffusées publiquement, mais qui peuvent être accessibles au grand public au moyen d'une diffusion légitime. Ces données sont soit explicitement définies comme des données publiques, destinées à être facilement accessibles aux personnes, soit ne sont pas spécifiquement classées par la norme de classification des données protégées. La diffusion de données publiques n'expose pas OCIM, ses actifs ou son personnel à des préjudices financiers, d'image ou à d'autres types de préjudices.

VII. POLITIQUE EN MATIÈRE DE DONNÉES DES CLIENTS

Conservation des données des clients

Pour assurer un traitement équitable, les données des clients ne seront pas conservées par OCIM plus longtemps que la durée nécessaire à la réalisation des finalités pour lesquels elles ont été collectées à l'origine, ou pour lesquelles elles ont été traitées ultérieurement. La durée pendant laquelle OCIM doit conserver les données des clients doit être indiquée dans les exigences légales et contractuelles, dans la mesure du possible. En l'absence d'exigences légales, réglementaires et contractuelles, OCIM conservera les données des clients en suivant la norme publiée dans les meilleures pratiques de l'industrie **applicable aux activités d'OCIM**. Toutes les données relatives aux clients doivent être supprimées ou détruites dès que possible dès lors qu'il est confirmé que leur conservation n'est plus nécessaire.

Protection des données des clients

OCIM adoptera des mesures physiques, techniques et organisationnelles pour assurer la sécurité des données des clients, y compris, mais sans s'y limiter, les données personnelles identifiables.

Ces mesures permettront notamment d'empêcher leur perte, endommagement, altération, accès ou

traitement non autorisés, ainsi que les autres risques auxquels elles peuvent être exposées, qu'ils découlent de l'action humaine ou de l'environnement physique ou naturel.

Les mesures de sécurité minimales adoptées sont destinées à :

- Empêcher toute personne non autorisée d'accéder aux systèmes de traitement des données dans lesquels les données des clients sont traitées ;
- Empêcher toute personne autorisée à utiliser un système de traitement des données d'accéder aux données des clients au-delà de ses besoins et des autorisations qui lui ont été accordées ;
- Veiller à ce que les données du client transmises par voie électronique ne puissent être lues, copiées, modifiées ou supprimées sans autorisation ;
- Veiller à la mise en place de registres d'accès pour définir si, et par qui, les données relatives au client ont été introduites, modifiées ou supprimées d'un système de traitement des données ;
- Veiller à ce que, dans le cas où le traitement est effectué par un sous-traitant de données (par exemple, un tiers autre qu'OCIM), les données ne puissent être traitées que conformément à la Politique de sécurité de l'information d'OCIM ;
- Veiller à ce que les données des clients soient protégées contre la destruction, la perte ou l'altération indésirables ;
- Veiller à ce que les données des clients collectées à des fins différentes puissent être traitées séparément et le soient, en fonction des besoins et des exigences de l'entreprise ;
- Veiller à ce que les données relatives aux clients ne soient pas conservées plus longtemps que la durée nécessaire.

VIII. **POLITIQUE DE PROTECTION DES ACTIFS INFORMATIONNELS**

La Politique de protection des actifs informationnels aide OCIM à définir des pratiques visant à protéger la confidentialité, l'intégrité et la disponibilité des actifs informationnels d'OCIM. Cette politique définit les objectifs à atteindre pour gérer correctement l'infrastructure informatique d'OCIM, y compris les réseaux, les systèmes et les applications qui stockent, traitent et transmettent les informations. Dans le cadre de cette politique, les actifs peuvent comprendre les éléments suivants, sans toutefois s'y limiter :

- Les terminaux (par exemple, les dispositifs informatiques fournis et gérés par OCIM qui comprennent, sans s'y limiter, les ordinateurs portables, les smartphones, les tablettes, les serveurs, l'équipement de réseau) ;
- Les appareils BYOD ou « *bring your own device* » (par exemple, les appareils n'appartenant pas à OCIM mais utilisés dans le cadre des activités d'OCIM) ;
- Les données et informations (par exemple, les codes sources, les plans de projet, la disponibilité du fournisseur du client) ;
- Les comptes système (par exemple, les comptes administrateur ProtonMail, AWS Console, AWS Linux, les comptes de service) ;
- Les comptes d'application (par exemple, SIRH, Confluence, GitHub) ;
- Les logiciels (par exemple, Slack, GSuite) ;
- Les comptes de réseaux sociaux (par exemple, compte Twitter d'OCIM, Facebook, Instagram, etc.) ;
- Les réseaux privés (par exemple, les actifs utilisés pour les tests de développement) ;
- Les connexions de réseaux publics aux réseaux privés d'OCIM (par exemple, VPN) ;
- Les infrastructures de bureau.

L'utilisateur accédera aux ressources d'OCIM et bénéficiera du niveau minimum d'accès requis pour répondre à un besoin professionnel approuvé après obtention de l'approbation du Responsable informatique et de la direction, ou de leurs délégués. L'accès est accordé lors de la création de comptes d'utilisateurs conformément à la procédure de demande de compte et approuvé par la direction d'OCIM.

La procédure d'octroi, de révision et de suppression de l'accès doit être accompagnée des preuves de toutes les activations/désactivations et faire l'objet d'audits ou de révisions périodiques. La procédure d'octroi ou de suppression de l'accès doit être équipée d'un dispositif ou d'un mécanisme permettant de suivre l'approbation expresse des activations/désactivations, sous forme électronique ou sur papier. Par exemple : les courriers électroniques, les saisies dans un système de tickets informatiques, les formulaires signés et scannés au format électronique, les journaux ou tout autre élément qui peut prouver que l'autorisation d'accès appropriée a été accordée à l'utilisateur.

L'accès aux actifs informationnels sera limité aux personnes autorisées dont les responsabilités professionnelles l'exigent, et sera déterminé au moyen d'un processus d'approbation approprié, et à celles qui sont autorisées à y avoir accès en vertu d'une exigence légale ou réglementaire.

IX. POLITIQUE DE GESTION DU MATÉRIEL

Au fur et à mesure de l'évolution de la taille, de la portée et des opérations d'OCIM, le Responsable informatique, en collaboration avec les Services juridiques et de gestion des risques, déterminera les cas d'utilisation du matériel appropriés pour OCIM.

Appareils de l'entreprise

Les utilisateurs d'OCIM ne peuvent utiliser et s'identifier que sur des appareils approuvés par le Responsable informatique. Le Responsable informatique, ou son délégué, configurera l'appareil pour qu'il réponde aux normes minimales d'OCIM, notamment en ce qui concerne le type d'accès (par exemple, Active Directory ou accès local), les droits d'accès et de contrôle de groupe (par exemple, utilisateur normal, privilèges élevés, administrateur, etc.).

Appareils BYOD

OCIM autorise, mais déconseille, l'utilisation d'appareils personnels à des fins professionnelles. Les utilisateurs d'appareils personnels :

- Seront tenus responsables de toute perte de données ;
- Doivent consentir à l'installation de logiciels et de contrôles de sécurité supplémentaires, tels qu'identifiés par le Directeur de la technologie (par exemple, logiciel de balayage, surveillance de la gestion des appareils mobiles, etc.)
- Ne doivent accéder aux ressources en ligne d'OCIM que via le SaaS/Cloud.
- Ne doivent pas installer le logiciel propriétaire ou enregistré d'OCIM sur l'appareil ;
- Ne doivent pas se connecter à des lecteurs, ni les utiliser, ni les partager.

X. POLITIQUE DE GESTION DES RÉSEAUX ET DES SERVICES

Au fur et à mesure de l'évolution de la taille, de la portée et des opérations d'OCIM, le Directeur de la technologie, en collaboration avec le Service juridique, déterminera dans quels cas le réseau et les services appropriés d'OCIM peuvent être utilisés.

Le Directeur de la technologie, ou son délégué, veillera à ce que les actifs informationnels soient logiquement séparés et segmentés, afin de minimiser l'exposition aux risques (par exemple, séparation par site, politiques de groupe, sous-réseaux, etc.)

Le Directeur de la technologie conservera une documentation indiquant, au minimum, les éléments suivants :

- Les services utilisés ;
- Les flux de données ;
- L'emplacement des données.

Le Directeur de la technologie, ou son délégué, mettra en place des mesures de contrôle (par exemple, des dispositifs de pare-feu, des configurations, des systèmes d'alerte, etc.).

Le Directeur de la technologie peut utiliser une base de données de gestion de la configuration ou un outil similaire pour identifier, gérer et suivre les actifs, les appareils de réseau et les services.

XI. POLITIQUE D'INSTALLATION DES LOGICIELS ET DE GESTION DES CONNEXIONS MATÉRIELLES

Tous les logiciels installés sur les actifs informationnels d'OCIM ou le matériel connecté à ceux-ci doivent être évalués par le Directeur de la technologie avant leur installation ou leur connexion. L'installation ou la connexion se fera sous la direction du Directeur de la technologie, de son délégué ou sur instruction explicite de l'utilisateur. Les utilisateurs ne sont pas autorisés à installer des logiciels ou à se connecter à du matériel sans autorisation. Toute altération des contrôles de sécurité dans le but de contourner la présente Politique constitue une violation.

XII. POLITIQUE DE PROTECTION DES COMPTES

La Politique de protection des comptes aide OCIM à définir des pratiques relatives aux comptes d'utilisateurs et à leur protection.

Caractéristiques des comptes d'utilisateurs

Tous les comptes d'utilisateurs OCIM doivent être uniques, traçables et associables à l'utilisateur concerné. OCIM prendra les mesures appropriées pour protéger la confidentialité des informations de l'utilisateur associées aux comptes d'utilisateur. L'utilisation de comptes et de mots de passe de groupe n'est pas autorisée, sauf approbation expresse du Directeur de la technologie **et** de la direction, ou de leurs délégués.

Privilèges du compte d'utilisateur

Les utilisateurs se verront accorder l'accès minimum nécessaire à l'exécution de leurs tâches spécifiques. L'octroi des niveaux d'accès aux ressources est basé sur le principe du moindre privilège, des responsabilités professionnelles et de la séparation des tâches. L'octroi du niveau d'accès minimal est soumis à la recommandation du responsable de l'utilisateur et à l'évaluation du propriétaire du système d'information. Le propriétaire du système d'information déterminera en dernier ressort le niveau d'accès d'un utilisateur à son système.

Comptes inactifs

Les comptes seront désactivés après trente (30) jours d'inactivité. Les utilisateurs qui prévoient de partir sur le terrain ou de s'absenter du bureau pendant toute période approuvée d'absence prolongée doivent informer leur responsable de leur absence afin de s'assurer que le compte sera correctement géré.

Comptes d'utilisateurs temporaires

Toutes les demandes de création de comptes d'utilisateurs temporaires doivent comporter une date d'expiration à appliquer au moment de la création du compte. Lorsque cela n'est pas possible, un mécanisme à commande manuelle peut être utilisé. Le propriétaire du système contrôlera l'accès temporaire pour s'assurer que les activités sont conformes à l'objectif visé.

Caractéristiques du mot de passe

Tous les mots de passe doivent être créés selon des normes de complexité minimale. Pour suivre les meilleures pratiques en la matière, OCIM peut s'appuyer sur des normes externes, telles que la publication spéciale 800-63b du NIST, *Digital Identity Guidelines*, ou des normes ou orientations similaires.

OCIM peut déployer une solution de gestion des mots de passe pour tous les utilisateurs afin de permettre

une rotation régulière des mots de passe et de veiller à leur unicité par service.

Le Directeur de la technologie configurera les contrôles pour s'assurer que les normes de complexité minimale sont respectées et que des durées d'expiration raisonnables sont mises en œuvre.

Réinitialisation du mot de passe

OCIM mettra en place une procédure pour vérifier l'identité d'un utilisateur avant de réinitialiser son mot de passe.

Connexion automatique

Toute utilisation d'un logiciel de connexion automatique pour contourner la saisie d'un mot de passe est interdite, sauf accord écrit spécifique du Directeur de la technologie **et** de la direction, ou de leurs délégués.

Conservation des comptes d'utilisateurs et des mots de passe

Chaque personne à qui un compte d'utilisateur et un mot de passe ont été attribués est responsable des actions effectuées depuis ce compte et ne doit pas divulguer les informations relatives à ce compte à une autre personne, pour quelque raison que ce soit.

Accès de la direction aux comptes d'utilisateurs

L'accès de la direction aux comptes d'utilisateurs sera limité à des fins professionnelles uniquement, par exemple en cas d'urgence ou de situation impérieuse, en cas d'absence prolongée d'un utilisateur ou d'utilisation abusive par un utilisateur des actifs informationnels d'OCIM.

Transferts de postes ou de responsabilités

Le personnel qui passe d'un poste ou d'un domaine de responsabilité à un autre verra ses privilèges d'accès modifiés pour tenir compte de ses nouvelles responsabilités professionnelles.

Suspension de l'accès d'un utilisateur

> **Rupture de la relation de travail volontaire.** Dans un délai de 24 heures, OCIM suspendra l'accès au compte et l'accès physique des utilisateurs dont la relation avec OCIM a pris fin.
>
> **Rupture de la relation de travail involontaire.** OCIM suspendra immédiatement l'accès au compte et l'accès physique des utilisateurs dont la relation avec OCIM a pris fin sur notification du Service juridique et/ou du Service des ressources humaines.
>
> Le Directeur de la technologie doit collaborer avec le Service juridique et le Service des ressources humaines concernés au sujet des exigences en matière de conservation des données et des comptes des utilisateurs avant de purger, de supprimer ou de modifier les données ou les informations des utilisateurs d'un employé ou d'un utilisateur qui quitte l'entreprise.

Délai d'attente de la session utilisateur

Les sessions utilisateur sont interrompues après 20 minutes d'inactivité, sauf indication contraire dans le cadre du plan de sécurité du système ou de l'application. Cela concerne notamment les connexions des utilisateurs à Internet ou à des applications spécifiques.

Accès aux informations sensibles

Dans le cadre de l'engagement d'OCIM en matière de protection des informations sensibles, les candidats finaux dont l'embauche est envisagée feront l'objet d'une vérification de leurs antécédents. Ces personnes seront soumises aux dispositions des politiques et procédures d'OCIM visant à protéger ces informations contre toute divulgation non autorisée. Les vérifications d'antécédents peuvent inclure, mais sans s'y limiter, la vérification des antécédents criminels.

XIII. POLITIQUE D'UTILISATION ACCEPTABLE

Les actifs informationnels de la Société ne doivent pas servir à promouvoir des causes religieuses ou politiques, ou toute activité illégale. Les messages ou opinions offensants ou inappropriés, la transmission d'images, de messages, de dessins animés ou d'autres éléments de ce type qui seraient sexuellement explicites, ou les messages pouvant constituer une forme de harcèlement ou de dénigrement d'autrui fondé sur l'origine raciale, la couleur, l'âge, l'origine nationale, la religion, le sexe, le statut d'ancien combattant, le handicap ou tout autre statut protégé par la législation internationale, fédérale, nationale, régionale et/ou locale applicable sont également interdits sur les systèmes de la Société.

Les employés sont tenus de faire preuve de bon sens dans l'utilisation personnelle des systèmes de la Société. En l'absence de politiques spécifiques concernant l'utilisation personnelle des systèmes de la Société, les employés doivent consulter leur superviseur ou leur responsable afin d'obtenir tout conseil.

L'utilisation de l'infrastructure d'OCIM n'offre aucune garantie de confidentialité. Toute information créée ou stockée sur les équipements d'OCIM est considérée comme la propriété intellectuelle d'OCIM. La direction se réserve le droit de surveiller l'activité informatique et d'examiner les incidents sur tout équipement à tout moment.

Outils de communication et stockage des données

OCIM recommande aux utilisateurs de n'employer que des outils de communication qui prennent en charge le cryptage de bout en bout et le cryptage des données au repos.

Le Directeur de la technologie mettra à la disposition des utilisateurs une liste des outils de communication autorisés. Cette liste sera révisée régulièrement.

Les utilisateurs limiteront l'utilisation des applications de messagerie mobile et de chat à des fins professionnelles en l'absence de solution d'entreprise facilement accessible.

Les données ne seront stockées que sur des outils approuvés par le Directeur de la technologie. Le Directeur de la technologie mettra à la disposition des utilisateurs une liste des solutions de stockage de données autorisées. La solution doit utiliser les méthodes et les normes actuelles de cryptage les plus raisonnables.

Les données seront étiquetées conformément à la Politique d'identification et de classification des données pendant leur utilisation et leur stockage.

L'accès aux solutions de stockage de données d'OCIM par des tiers doit être restreint au minimum et répondre au principe du « moindre privilège » si l'accès externe est requis dans le cadre d'un usage professionnel légitime.

Utilisation interdite

Les éléments suivants ne devront en aucun cas être utilisés ou stockés sur les actifs d'OCIM :

LM AL

- L'utilisation d'une clé USB ou d'un support d'extraction similaire (par exemple, disque dur, dispositif de stockage sans fil, etc.) pour télécharger ou téléverser toute information ou tout contenu depuis ou vers un actif d'OCIM ;
- Les éléments qui peuvent constituer une violation des droits d'auteur, des secrets commerciaux, des brevets ou d'autres lois ou règlements sur la propriété intellectuelle, y compris, mais sans s'y limiter, l'installation ou la distribution de produits « piratés » ou d'autres produits logiciels qui ne font pas l'objet d'une licence appropriée pour être utilisés par OCIM ;
- L'export de logiciels, d'informations techniques, de logiciels de cryptage ou de technologies, en violation des lois internationales ou régionales sur le contrôle des exportations ;
- L'introduction de logiciels malveillants dans le réseau, ou de toute autre manière susceptible d'interférer, de nuire ou d'entraver la sécurité ou l'intégrité de tout actif d'OCIM ;
- Le contournement des exigences prévues par la Politique de sécurité des points de terminaison sur les dispositifs (par exemple, jailbreaking, désactivation des fonctions, suppression de la surveillance, etc.) ;
- La divulgation de mot de passe de compte à d'autres personnes ou l'octroi d'autorisation à d'autres personnes leur permettant d'utiliser le compte ;
- Le don ou le prêt d'un actif de la Société à une autre personne sans l'accord écrit de la direction autorisée ;
- L'utilisation d'un actif de la Société (tout appareil ou hôte sur un réseau OCIM) dans le but d'obtenir ou de transmettre du matériel qui enfreint les politiques ou les lois d'OCIM en matière de harcèlement ou de lieu de travail hostile dans la juridiction locale de l'utilisateur ;
- La formulation d'offres frauduleuses de produits, d'articles ou de services depuis un compte de la Société ;
- La perturbation des communications du réseau ;
- Le contournement de l'authentification de l'utilisateur ou de la sécurité d'un hôte, d'un réseau ou d'un compte ;
- La falsification ou l'usurpation d'identité, y compris, mais sans s'y limiter, le courrier électronique, les comptes ou la voix ;
- L'utilisation de services de messagerie ou de réseaux sociaux pour présenter OCIM de manière trompeuse ou en violation des politiques de la Société ;
- L'utilisation des actifs d'OCIM à des fins ou bénéfices personnels, autres qu'une utilisation ou un bénéfice accessoire, ou en violation de tout accord entre l'utilisateur et OCIM, tel que le manuel de l'employé ou l'accord de non-divulgation de l'employé ;
- Le transfert ou l'utilisation de services de messagerie pour participer à des systèmes de ponzi, de chaîne ou de pyramide ;
- Le transfert de courriers électroniques, de documents, de logiciels et d'informations internes et exclusives d'OCIM vers des comptes de messagerie personnels.

XIV. **POLITIQUE DE RÉPONSE AUX INCIDENTS**

OCIM mettra en place un processus de réponse aux incidents conformément au plan de réponse aux incidents (« PRI »). Le PRI sera élaboré et géré conjointement par le Responsable informatique, le Service juridique et le Service de gestion des risques. Le PRI :

- Décrira la structure et la coordination de la capacité de réponse aux incidents d'OCIM ;
- Identifiera les rôles et les responsabilités des parties prenantes internes et externes ;
- Sera cohérent avec les exigences propres à l'organisation, y compris, mais sans s'y limiter, la tolérance au risque, la mission, la vision, la stratégie et les opérations ;
- Décrira l'incident à signaler, y compris, mais sans s'y limiter, la preuve d'un accès non autorisé, la preuve d'une fuite de données, la preuve d'un logiciel malveillant ou d'un code malveillant, la preuve d'une attaque ou d'une interruption de service, la preuve d'un schéma d'attaque durable ;
- Définira les besoins en matière de ressources et d'aide à la gestion pour gérer et maintenir efficacement le programme de réponse aux incidents et les incidents en cours ;
- Définira les exigences techniques pour gérer et maintenir efficacement le programme de réponse aux incidents et les incidents en cours ;
- Identifiera les activités de planification d'urgence et les ressources nécessaires en cas d'incident ;
- Inclura des notes de criticité pour aider les intervenants et les évaluateurs à déterminer la portée et

l'impact de l'incident ;

- Prévoira une méthode permettant de documenter et d'archiver correctement les incidents de système à l'aide de journaux d'audit appropriés. Les durées de stockage doivent être conformes à la politique de conservation des documents établie ;
- Sera périodiquement mis à jour pour rester cohérent aux changements de l'organisation ;
- Sera approuvé par la direction.

XV. POLITIQUE DE SUIVI, DE TESTS PÉRIODIQUES ET D'ÉVALUATION DES RISQUES

Pour mieux protéger en permanence ses actifs informationnels, OCIM mettra en place des capacités raisonnables et appropriées d'évaluation et de surveillance des menaces dans l'ensemble de son infrastructure et de ses dispositifs. En outre, OCIM effectuera des tests périodiques de ses actifs informationnels et examinera régulièrement sa position en matière de risques liés à la sécurité de l'information.

Évaluation et surveillance des menaces

OCIM identifiera, analysera et classera périodiquement par ordre de priorité les menaces pesant sur les actifs informationnels et s'appuiera sur les conclusions des activités d'évaluation des menaces, le cas échéant, pour améliorer la sécurité des actifs informationnels d'OCIM.

Sur la base du caractère raisonnable, des menaces et de la tolérance au risque, OCIM effectuera une surveillance en temps réel de la détection des intrusions et une analyse périodique de la détection des intrusions afin de détecter les menaces et les intrusions sur les segments critiques du réseau sur la base des résultats de l'analyse des menaces.

Évaluation et gestion de la vulnérabilité

Au fur et à mesure de l'évolution de la taille, de la portée et des opérations d'OCIM, le Responsable informatique, en collaboration avec les Services juridiques et de gestion des risques, déterminera les mesures appropriées pour mener des évaluations de la vulnérabilité. Au minimum, OCIM effectuera des analyses trimestrielles de ses actifs informationnels afin d'identifier les vulnérabilités, ou à tout autre intervalle régulier adapté à la taille, à la portée et aux opérations d'OCIM actuelles.

Au minimum, OCIM effectuera chaque année un test de pénétration externe de son réseau et de ses actifs pertinents.

OCIM mettra en place un processus formel pour identifier, suivre, remédier ou atténuer les vulnérabilités techniques en utilisant les résultats de l'analyse des vulnérabilités, des tests de pénétration, de la réponse aux incidents et des activités d'évaluation des risques. Pour mener à bien ces activités, OCIM mettra en place une procédure ou un programme formel de gestion des correctifs.

Dans les cas où OCIM ne peut pas procéder à une analyse ou à un test sur le système (par exemple, s'il est géré par un tiers), OCIM demandera au responsable une attestation, une validation ou une certification indiquant que son environnement est régulièrement analysé pour détecter les vulnérabilités, que les vulnérabilités sont corrigées et qu'un programme formel de gestion des correctifs a été mis en place.

Gestion des risques

Les évaluations des risques liés à la sécurité de l'information doivent identifier, quantifier et hiérarchiser les risques en fonction de critères d'acceptation des risques et d'objectifs pertinents pour OCIM. Les résultats doivent guider et déterminer les actions et priorités appropriées de la direction pour gérer les risques liés à la sécurité de l'information et pour mettre en œuvre les contrôles sélectionnés permettant de se protéger contre ces risques.

L'évaluation des risques liés à la sécurité de l'information doit inclure une approche systématique de l'estimation de l'ampleur des risques (analyse des risques) et le processus de comparaison des risques estimés avec les critères de risque afin de déterminer l'importance des risques (évaluation des risques).

Les évaluations des risques liés à la sécurité de l'information doivent être effectuées de manière

méthodique, afin de produire des résultats comparables et reproductibles. Pour être efficaces, les évaluations des risques liés à la sécurité de l'information doivent avoir un champ d'application clairement défini et doivent, le cas échéant, être associées à des évaluations des risques dans d'autres domaines.

OCIM procédera au moins une fois par an à une évaluation des risques en matière de sécurité de l'information.

XVI. FORMATION, APPLICATION, POLITIQUE D'ACTION CORRECTIVE

Au fur et à mesure de l'évolution de la taille, de la portée et des opérations d'OCIM, le Responsable informatique, en collaboration avec les Services juridiques et de gestion des risques, déterminera les activités et les exigences appropriées en matière de formation, d'application et d'action corrective.

Formation

Tous les utilisateurs qu'OCIM examineront et auront connaissance de la présente Politique de sécurité de l'information ainsi que des politiques, normes et lignes directrices pertinentes. Après toute mise à jour et tout examen, OCIM communiquera les changements aux utilisateurs.

Les utilisateurs auront accès à la Politique de sécurité de l'information et aux politiques, normes et lignes directrices pertinentes par le biais de la solution de stockage de données partagé d'OCIM.

Tous les utilisateurs devront attester avoir lu et compris les politiques sur une base annuelle et dans le cadre du processus d'accueil et d'intégration.

Tous les nouveaux utilisateurs ou les nouveaux employés doivent recevoir une formation appropriée en matière de sensibilisation à la sécurité au moment de leur embauche. À l'issue de la formation, les nouveaux utilisateurs d'OCIM et les personnes nouvellement embauchées devront attester par écrit qu'ils ont bien suivi la formation.

OCIM conservera un registre des formations de sensibilisation à la sécurité suivies.

Application de la loi

Le non-respect des politiques, normes, lignes directrices et procédures du programme de sécurité de l'information d'OCIM peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement pour les employés ou à la rupture de contrats pour les entrepreneurs, partenaires, consultants et autres entités. OCIM se réserve également le droit d'intenter une action en justice en cas de violation des règlements et lois applicables.

Action corrective

Tout utilisateur d'OCIM qui constate une violation des Politiques de sécurité de l'information d'OCIM est tenu de la signaler immédiatement à son responsable, au Directeur de la technologie ou au Service des ressources humaines. Lors de l'application de mesures correctives, la direction ou les RH suivront les politiques pertinentes d'OCIM.

ANNEXE A : PAGE DE SIGNATURE

RÉCEPTION ET PRISE DE CONNAISSANCE

Je reconnais par la présente avoir reçu, lu attentivement et compris la « Politique de sécurité de l'information » d'OCIM et j'accepte de me conformer à tous égards à toutes les procédures de ce type auxquelles je suis soumis(e).

Je comprends que le Directeur général peut répondre à toutes les questions que je me pose concernant la Politique de sécurité de l'information du groupe OCIM.

5 nov 2024

boxSIGN 4PZX277R-1VPP66YJ

Signature

Date

Laurent Mathiot

Nom (en caractères d'imprimerie)

boxSIGN 19Z23P84-1VPP66YJ

5 nov. 2024

Signature

Date

Arnaud Lapiere

Nom (en caractères d'imprimerie)