Information Security Policy

V.1

01/01/2023

APPROVALS AND REVISION HISTORY

The Company has approved this Information Security Policy and will periodically review and update, as necessary.

Effective Date	Version	Changes Made	Signatures
1 Jan 2023	1.0	Creation of Information Security Policy	Laurent Mathiot, CEO Arnaud Lapière, CTO

Table of Contents

I. INTRODUCTION

OCIM Finance ("OCIM") is a privately held group of companies headquartered in Paris and is owned and funded by the Mathiot family. The family's initial interests in real estate have since diversified into a series of other activities, including but not limited to precious and strategic metals financing and trading through OCIM. The expansion of the group's financial activities has also driven a geographical expansion, with a subsidiary in Geneva.

OCIM functions as the group holding company; OCIM Metals & Mining SA ("OMM") and Electrum SA ("Electrum") are two of the main group subsidiaries. OMM is a metals merchant and financier focused on gold, silver, and platinum metals with a presence in Paris and Geneva, while Electrum provides a proprietary trading capability to support the group activities, primarily for hedging and risk management purposes, with teams in Paris and Geneva.

II. PURPOSE

OCIM, their affiliates and related entities (hereinafter known as the "Company" or "OCIM") is committed to achieving the highest standards of professionalism in its operations and services and expects its Representatives (e.g., management, employees, related third parties, etc.) to conduct their business according to the highest ethical standards of conduct and to comply with all applicable laws.

This Information Security Policy (this "Policy") is intended to increase awareness of issues pertaining to information security and establish rules to manage, govern, and enforce the information security management program. This Policy is intended to supplement but not replace any applicable laws governing information security requirements applicable to the Company and its subsidiaries.

The purpose of this Policy is to set forth the underlying tenets, framework, and reasoning for the OCIM 's information security practices.

The OCIM Information Security Policy framework defines baseline control measures that everyone at OCIM is expected to be familiar with and to follow consistently. The intent of the security framework and its related policies is to define minimum acceptable levels of security to the Company and to implement them consistently across the Company.

The minimum level is set to prevent most anticipated security risks, while still offering the Company and its subsidiaries the ability to customize local standards and procedures to meet their day-to-day security needs.

Moreover, the policy is set to prevent most anticipated risks based on the Company's existing operations and size. Therefore, the policy must be regularly updated as the Company modifies its operations and size. Any material change in the Company's size, scope, business, operations, or information assets should initiate a review and update of this policy. A record for proper versioning and history, as the standards, must also be maintained to remain consistent with technology advances. This record shall be maintained in the repository with all other related OCIM policies and record keeping activities.

II.A. EXCEPTIONS

Requests for exceptions to this Policy's requirements or the Policy itself must be submitted in formal writing to the Chief Technology Officer ("CTO") for review. The exception request **must** include:

- The business reason for making the request; and
- The specific policy requirement or section requested to be modified or to be excepted from.

The CTO will engage with the appropriate stakeholders, including by not limited to Legal and Risk stakeholders, to determine if further review and assessment is required.

Exceptions are time-based for a reasonable duration, reflective of the business need and level of risk involved. If the exception has a requirement for greater than one (1) year, updates and/or modifications to policies and procedures should be considered.

At expiration of an exception, the risk must be reviewed, and an extension or further action will be determined by the CTO or the Legal department/counsel.

III. SCOPE

This Policy is applicable to employees, officers, managers, directors, senior executives, temporary employees, contractors, consultants, temporaries, and any other workers, of OCIM, as well as any vendors and third parties that create, receive, store, use, encounter or transmit OCIM Information. This Policy covers information that is stored or shared via any means including electronic and paper information, and information shared orally or visually (such as telephone and video conferencing). For purposes of this document, the scope of infrastructure components is limited to OCIM infrastructure required to support the business.

IV. DEFINITIONS

A **"policy"** is a mandatory, definite course or method of action selected by senior management to guide and determine present and future decisions. Policy is independent of technologies or specific solutions. Security, compliance, and various technology specific subject matter experts update all policies, at a minimum, on an annual basis.

A **"practice"** is a mechanism for carrying out the policy direction of senior management. Practices will reference the necessary standards and procedures used when carrying out a policy.

A **"standard"** is a set of mandatory, specific requirements for satisfying high-level objectives defined in a policy. OCIM must identify common industry practices applicable to its business and subsidiaries and align security controls to those requirements or use the requirements as a base framework for standards, followed by customization to meet the organizational policy requirements. In rare cases, departments may request exceptions to standards provided they follow a formal exception procedure.

A **"procedure"** is a set of specific, systematic instructions that describe how to comply with requirements described in a standard or guideline. These documents change frequently based on the technology and/or the team/individual performing the task.

A **"guideline"** is a set of optional recommendations that support a specific standard. OCIM reviews guidelines on an as needed basis.

A **"legal agreement"** or **"contract"** refers to any and all written instruments, agreements, documents, execution of deeds, powers of attorney, transfers, assignments, contracts, obligations, certificates and other instruments of whatever nature entered into by OCIM (e.g., MSAs, NDAs, SOWs).

This document delineates authorities. Each authority is characterized by one of the following words:

- **shall** or **must** indicates an activity or function which the role is obligated to perform and cannot refuse or delegate.
- **should** indicates an activity or function for which the role is accountable, although specific performance may be delegated.
- **may** indicates an activity or function which the role is capable of performing among its other duties.

V. ROLES AND RESPONSIBILITIES

OCIM shall use the following classifications for persons using OCIM digital assets:

User: any person utilizing OCIM information assets for legitimate business purposes, including external third parties, such as vendors and contractors. A user is required to abide by the requirements set out in this policy. All users are obligated to report instances of non-compliance with this policy. Every user must maintain the confidentiality of information assets even if technical security mechanisms fail or are absent.

IT Manager: any individual(s) explicitly assigned to be responsible for maintaining the operations and security of OCIM information assets. The IT Manager, or their assigned delegate, must ensure the requirements set out in this policy are enforced. The IT Manager must inform Management of any violations to this policy and take corrective action. Corrective action must be taken within a reasonable amount of time based on the risk and in agreement with Management.

Management: any individual(s) explicitly assigned to be responsible for the operations and fiduciary duty of OCIM. Management is required to provide oversight and direction for the information security program and approve this policy.

Visitor/Guest: any individual(s) requiring temporary access to OCIM information assets for limited or non-business purposes (e.g., Guest Wi-Fi or printer access). Visitors and/or Guests will not be granted access to any information outlined in the Data Identification and Classification Policy. The IT Manager will configure the information assets in a manner such that a Visitor and/or Guest cannot access any internal OCIM information (e.g., segmentation of systems, guest-only networks, etc.). Visitors and/or Guests will not be issued OCIM user accounts.

VI. DATA IDENTIFICATION AND CLASSIFICATION POLICY

The Data and Identification Classification Policy defines OCIM's objectives for establishing specific standards to identify, classify, and label OCIM information assets. This policy provides a practice to protect data critical to the organization and all employees should be aware of these classifications and handling procedures.

Data classification will be based on sensitivity, criticality, and value. Data must be classified in one of four (4) tiers: Restricted/Proprietary, Confidential, Sensitive, or Public. All data require some level of protection, but as sensitivity, criticality, and value increase, so should security controls. Security controls must be implemented commensurate with the data value, sensitivity, risk, and according to legal and regulatory requirements.

Tier I: Restricted/Proprietary

Information of a strategic, proprietary, or mission critical nature. Loss or damage to this information would likely result in **serious or catastrophic** adverse impact to the organization's ability to continue operations, **serious or catastrophic** adverse impact to the reputation of the organization, **serious or catastrophic** adverse impact to personnel or assets of the organization. This data is intended for use within the organization and those who have a legitimate business need to it. Any intentional external release of this information for legitimate business use (e.g., regulators, strategic investors, external counsel, etc.) should be coordinated by the Legal and Risk departments.

Tier II: Confidential

Information whose unauthorized access, compromise, or destruction would result **severe** damage to OCIM, its customers, or employees (e.g., ID numbers, dates of birth, health information, financial information, etc., or collectively, "personally identifiable information" or "personal information"). This data is intended for use within the organization and those (internally or externally) who have a legitimate business need to it.

Tier III: Sensitive

Information that must be guarded due to ethical or privacy considerations. Unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to OCIM's reputation, or violate an individual's privacy rights. This includes information confined for use only within purposes related to its business.

Tier IV: Public

Public information is information that is not publicly disseminated, but assessable to the general public through legitimate release. This type of information is either explicitly defined as public information, intended to be readily available to individuals, or not specifically classified elsewhere in the protected data classification standard. Knowledge of public information does not expose OCIM, its assets, or its people to financial, reputation, or other types of harm.

VII. CUSTOMER DATA POLICY

Customer Data Retention

To ensure fair processing, Customer Data will not be retained by OCIM for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which OCIM needs to retain Customer Data should be outlined in legal and contractual requirements, where possible. In the absence of a legal, regulatory, and contractual requirement, OCIM will retain Customer Data based up a published industry best practice standard **applicable to OCIM's businesses**. All Customer Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Customer Data Protection

OCIM will adopt physical, technical, and organizational measures to ensure the security of Customer Data, including but not limited to personally identifiable information. This includes the prevention of loss or

damage, unauthorized alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures adopted are meant to:

- Prevent unauthorized persons from gaining access to data processing systems in which Customer Data is processed.
- Prevent individuals entitled to use a data processing system from accessing Customer Data beyond their needs and authorizations.
- Ensure that Customer Data during electronic transmission cannot be read, copied, modified, or removed without authorization.
- Ensure that access logs are in place to establish whether, and by whom, the Customer Data was entered into, modified on, or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor (e.g., a third party other than OCIM), the data can be processed only in accordance with the OCIM Information Security Policy.
- Ensure that Customer Data is protected against undesired destruction, loss, or corruption.
- Ensure that Customer Data collected for different purposes can and is processed separately, based on business needs and requirements.
- Ensure that Customer Data is not kept longer than necessary.

VIII. INFORMATION ASSET PROTECTION POLICY

The Information Asset Protection Policy defines OCIM objectives for establishing practices to protect the confidentiality, integrity, and availability of OCIM information assets. The policy defines objectives for properly managing OCIM Information Technology infrastructure, including networks, systems, and applications that store, process, and transmit information assets. For this policy, assets may include but are not limited to the following types:

- Endpoints (e.g., Provisioned and managed by OCIM computing devices that include but are not limited to laptops, smartphones, tablets, servers, networking equipment).
- BYOD devices (e.g., Devices not owned by OCIM but used for OCIM business).
- Data and information (e.g., Source code, project plans, customer provider availability).
- System accounts (e.g., ProtonMail administrator accounts, AWS Console, AWS Linux, service accounts).
- Application accounts (e.g., HRIS, Confluence, GitHub.
- Software (e.g., Slack, GSuite).
- Social media accounts (e.g., OCIM Twitter account, Facebook, Instagram, etc.).
- Private networks (e.g., Assets used for development testing).
- Public network connections to OCIM private networks (e.g., VPN).
- Office facilities.

The minimum level of access required to meet an approved business need will be granted to OCIM resources after proper approval is obtained from the IT Manager and Management, or their assigned delegates. Access is given through the establishment of user accounts in accordance with the account request process and approved by OCIM management.

The procedure for granting, reviewing, and removing access must include evidence of all provisioning transactions and be made available for periodic audits or reviews. The procedure for granting or removing access must include a facility or mechanism to track the express approval for the transaction, either in electronic or hard copy format. Examples include but are not limited to email, entries in a ticketing system, signed and scanned forms in electronic format, logs, or other items that can show evidence the proper authorization was granted for provisioning user access.

Access to information assets will be limited to authorized persons whose job responsibilities require it, as determined by an appropriate approval process, and to those authorized to have access by legal or regulatory requirement.

IX. HARDWARE MANAGEMENT POLICY

As OCIM's size, scope, and operations change, the IT Manager, in conjunction with the Legal and Risk departments, will determine the appropriate hardware use cases for OCIM.

Corporate Devices

All OCIM users may only acquire and register devices approved by the IT Manager. The IT Manager, or their delegate, will configure the device to meet OCIM minimum standards, including but not limited to access type (e.g., Active Directory versus local access), access and group control rights (e.g., normal user, elevated privileges, administrator, etc.), and monitoring and scanning software.

BYOD Devices

OCIM permits, but discourages, the use of personal devices for business purposes. Users of personal devices:

- Must accept responsibility for, and liability of, any data loss.
- Must accept additional software and security controls, as identified by the CTO (e.g., scanning software, mobile device management monitoring, etc.).
- Must only use web access to SaaS/Cloud-based OCIM resources.
- Not install OCIM owner or registered software on the device.
- Not connect to or use and share/cloud drives.

X. NETWORK AND SERVICES MANAGEMENT POLICY

As OCIM's size, scope, and operations change, the CTO, in conjunction with the Legal department, will determine the appropriate network and services use cases for OCIM.

The CTO, or their delegate, shall ensure information assets are logically separated and segmented, to minimize risk exposure (e.g., separate by site, group policies, subnets, etc.).

The CTO will maintain documentation outlining, at a minimum:

- Services in use.
- Data flows.
- Data locations.

The CTO, or their delegate, shall institute control measures (e.g., firewall appliances, configurations, alerting systems, etc.) to protect information security assets.

CTO may use a configuration management database, or similar tool, to identify, manage, and track assets, network appliances, and services.

XI. SOFTWARE INSTALLATION AND HARDWARE CONNECTION MANAGEMENT POLICY

All software installed on, or hardware connected to, OCIM information assets must be evaluated by the CTO prior to installation or connection. Installation or connection may be done at the direction of the CTO, their delegate, or explicit instruction to the user. Users are not permitted to install software or connect to hardware without permission. Tampering with security controls to circumvent this policy is a violation.

XII. ACCOUNT PROTECTION POLICY

The Account Protection Policy defines OCIM objectives for establishing practices for user accounts and their protection.

User Accounts Characteristics

All OCIM user accounts must be unique and traceable to the assigned user. OCIM will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by the CTO **and** Management, or their delegates.

User Account Privileges

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user's manager, and the evaluation of the information system owner. The information system owner will have final determination as to the level of a user's access to their system.

Inactive Accounts

Accounts will be disabled after thirty (30) days of inactivity. Users planning to deploy to field operating locations or to be away from the office for other approved periods of extended absence should coordinate their absence with the manager to ensure proper disposition of the account.

Temporary User Accounts

All requests for temporary user accounts should provide an expiration date to be applied at the time the account is created. Where this is not possible, a manually controlled mechanism can be used. The system owner will monitor temporary access to ensure activities comply with the intended purpose.

Password Characteristics

All passwords must be constructed using minimal complexity standards. For best practices, OCIM may reference external standards, such as *NIST Special Publication 800-63b, Digital Identity Guidelines*, or similarly related standards or guidance.

OCIM may deploy a password management solution to all users to allow for regular rotation of passwords and uniqueness per service.

The CTO will configure controls to ensure minimal complexity standards are met and reasonable expiration durations are implemented.

Password Reset

OCIM will establish a procedure for verifying a user's identity prior to resetting their password.

Automatic Logon

The use of automatic logon software to circumvent password entry shall not be allowed, except with specific written approval from the CTO **and** Management, or their delegates.

User Account and Password Safekeeping

Each individual assigned a user account and password is responsible for the actions taken under said account and must not divulge that account information to any other person for any reason.

Management Access to User Accounts

Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of OCIM information resources.

Transfers of Roles or Responsibilities

Personnel transferring from one role or area of responsibility to another shall have their access privileges modified to reflect their new job responsibilities.

User Access Cancellation

Voluntary Resignation. Within 24 hours, OCIM will cancel account access and physical access for users whose relationship with OCIM has concluded.

Involuntary Termination. OCIM will cancel account access and physical access immediately upon notification from the legal and/or human resource departments for users whose relationship with OCIM has concluded.

The CTO must coordinate user data and account retention requirements with the appropriate legal and human resource departments before purging, deleting, or modifying and data or user information of a departing employee or user.

User Session Time-out

User sessions will time-out after 20 minutes of inactivity unless otherwise specified as part of the system or application security plan. This includes user connections to the Internet, or to specific applications.

Sensitive Information Access

As part of OCIM's commitment to the protection of Sensitive Information, background checks will be conducted for all final candidates being considered for employment. These individuals will be subject to the provisions of OCIM policies and procedures to protect and safeguard such information from unauthorized disclosure. Background checks may include, but are not limited to, criminal history checks.

XIII. ACCEPTABLE USE POLICY

The Company's information assets shall not be used as a forum to promote religious or political causes, or any illegal activity. Offensive or improper messages or opinions, transmission of sexually explicit images, messages, cartoons, or other such items, or messages that may be construed as harassment or disparagement of others based on race, color, age, national origin, religion, sex, veteran, disability, or any other status protected under applicable international, federal, state, regional, and/or local law are also prohibited on the Company systems.

Employees are responsible for exercising good judgment in the personal use of Company Systems. In the absence of specific policies regarding personal use of Company systems, employees should consult their supervisor or manager for guidance.

There is no guarantee of privacy while using OCIM's infrastructure. Information created or stored on OCIM equipment is considered the intellectual property of OCIM. Management reserves the right to monitor computer activity and examine incidents on any equipment at any time.

Communication Tools and Data Storage

OCIM recommends users solely employ communication tools that support end-to-end encryption and data-at-rest encryption.

The CTO shall make available to users a list of authorized communication tools. This list shall be reviewed periodically.

Users will limit the use of mobile messaging and chat applications for business purposes if a corporate solution is not readily available.

Data will only be stored in approved tools by the CTO. The CTO shall make available to users a list of authorized data storage solutions. The solution must use the most reasonable current day encryption methods and standards.

Data will be tagged in accordance with the Data Identification and Classification Policy while in use and storage.

Access to OCIM data storage solutions by third parties must be minimized and employ the "least privilege" methodology if there is a legitimate business use for external access.

Prohibited Use

The following list of items is prohibited from usage or storage on OCIM assets:

- Use of any USB drives or similar removal media (e.g., hard drives, wireless storage devices, etc.) to download or upload any information or content from or to any OCIM asset.
- Items which may constitute a violation of copyright, trade secret, patent, or other intellectual property laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by OCIM.
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws.
- Introduction of malicious software into the network, or in any other manner which may interfere, harm, or hamper the security or integrity of any OCIM asset.
- Circumventing or bypassing Endpoint Security Policy requirements on devices (e.g., jailbreaking, disabling features, removing monitoring, etc.).
- Revealing account password to others or allowing use of account by others.
- Giving or loaning a company asset to another individual without written consent from authorized management.
- Using a company asset (any device or host on a OCIM network) to actively engage in procuring or transmitting material that is in violation of harassment or hostile workplace OCIM policies or laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any company account.
- Disruption of network communications.
- Circumventing user authentication or security of any host, network, or account.
- Forging or spoofing of identity, including but not limited to email, accounts, or voice.
- Use of messaging or social media services to misrepresent OCIM or otherwise in violation related company policies.
- Use of OCIM assets for personal purposes or benefit, other than incidental use or benefit, or in violation of any agreement between user and OCIM, such as the employee handbook or employee non-disclosure agreement.
- Forwarding or use of messaging services to engage in ponzi, chain, or pyramid schemes.
- Forwarding OCIM emails, documents, software, internal and proprietary information to personal email accounts.

XIV. **INCIDENT RESPONSE POLICY**

OCIM will conduct incident response activities in accordance with the Incident Response Plan ("IRP"). The IRP will be jointly developed and managed by the IT Manager, Legal Department, and Risk Department. The IRP shall:

- Describe the structure and organization of OCIM's incident response capability.
- Identify roles and responsibilities of internal and external stakeholders.
- Align with the unique requirements of organization, including by not limited to risk tolerances, mission, vision, strategy, and operations.
- Definitions for a reportable incident, including but not limited to evidence of unauthorized access, evidence of leaked data, evidence of malware or malicious code, evidence of service attacks or disruptions, evidence of sustained attack patterns.
- Define resources and management support needs to effectively manage and maintain the incident response program and active incidents.
- Define technical requirements to effectively manage and maintain the incident response program and active incidents.
- Identify contingency planning activities and resources required in the event of an incident.

- Include criticality ratings to assist responders and evaluators to determine scope and impact.
- Include a method to properly document and archive system incidents with appropriate audit trail evidence. Storage durations shall comply with the established records retention policy.
- Be periodically updated to align with the organization's changes.
- Be approved by Management.

XV. MONITORING, PERIODIC TESTING, AND RISK REVIEW POLICY

To better protect its information assets on an ongoing basis, OCIM will institute reasonable and appropriate threat assessment and monitoring capabilities across its infrastructure and devices. Furthermore, OCIM will conduct periodic testing of their information assets and review its information security risk posture on a regular basis.

Threat Assessment and Monitoring

OCIM will periodically identify, analyze, and prioritize threats to information assets, and will integrate findings from threat assessment activities, as appropriate, into the improving the security posture of OCIM's information assets.

Based on reasonableness, threats, and risk tolerances, OCIM will perform real-time intrusion detection monitoring and periodic intrusion detection analysis to detect threat and intrusion activity on critical network segments based on threat analysis results.

Vulnerability Assessment and Management

As OCIM's size, scope, and operations change, the IT Manager, in conjunction with the Legal and Risk departments, will determine the appropriate measures to conduct vulnerability assessments. At a minimum, OCIM will perform quarterly scans of OCIM information assets to identify vulnerabilities, or at some other regular interval appropriate to OCIM's current day size, scope, and operations.

At a minimum, OCIM will conduct an external penetration test of its network and relevant assets annually.

A formal process shall be established to identify, track, remediate, or mitigate technical vulnerabilities using the findings identified from vulnerability scanning, penetration testing, incident response, and risk assessment activities. To support these activities, OCIM will establish a formalize patch management procedure or program.

In instances where OCIM cannot perform a scan or test on the system (e.g., managed by a third party), OCIM will seek from the responsible some type of attestation, validation, or certification, that their environment is scanned regularly for vulnerabilities, vulnerabilities are remediated, and some type of formal patch management program is in place.

Risk Management

Information Security Risk assessments must identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to OCIM. The results are to guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

Information Security Risk assessments must include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

Information Security Risk assessments are to be undertaken in a methodical manner capable of producing comparable and reproducible results. Information security risk assessments should have a clearly defined scope to be effective and should include relationships with risk assessments in other areas, if appropriate.

At a minimum OCIM will conduct an Information Security Risk Assessment annually.

XVI. TRAINING, ENFORCEMENT, CORRECTIVE ACTION POLICY

As OCIM's size, scope, and operations change, the IT Manager, in conjunction with the Legal and Risk departments, will determine the appropriate training, enforcement, and corrective action activities and requirements.

Training

All users OCIM assists will review and acknowledge this Information Security Policy and relevant policies, standards, and guidelines. Upon regular update and review, OCIM will communicate changes to users.

All users will have access to the Information Security Policy and relevant policies, standards, and guidelines through OCIM's shared data storage solution.

All users will be required to attest to having read and understood the policies on an annual basis and as part of the onboarding process.

All new users or new hires must be provided with the appropriate security awareness education and training upon hiring. Upon completion of training, OCIM new users and new hires will be required to sign off that training has been completed.

OCIM will maintain a repository of security awareness training completion and acknowledgement.

Enforcement

Failure to comply with any of the OCIM Information Security Program policies, standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. OCIM also reserves the right to take legal action in cases that involve violations of applicable regulations and laws.

Corrective Action

Any OCIM user that identifies a violation of the OCIM Information Security Policies is required to report the violation to their manager, the CTO, or Human Resources immediately. When applying corrective actions, management or HR shall follow relevant OCIM policies.

EXHIBIT A: SIGNATURE PAGE

RECEIPT AND ACKNOWLEDGEMENT

I hereby acknowledge that I have received, carefully read, and understand the "Information Security Policy" of OCIM and agree to comply in all respects with all such procedures to which I am subject.

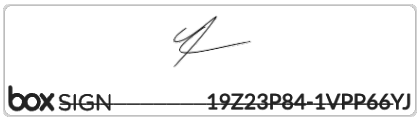
I understand that the CEO is available to answer any questions I have regarding the OCIM Group Information Security Policy.

5 nov. 2024

Signature Date

Laurent Mathiot

Name (Please print)



5 nov. 2024

Signature Date

Arnaud Lapiere

Name (Please print)