# Confidentiality Policy

| | |
|---|---|
| Date of inception: | 1 December 2022 |
| Review period: | Every two years |
| Approval date: | #2 (Approved 10 February 2025) |
| Policy owner: | Compliance Officer |
| Related document(s): | Information Technology Policy |
| Public document: | Yes |

## 1. Policy Statement

WMC commits to safeguarding all Confidential Information (as defined in Section 7) possessed and received by WMC in the course of its business activities and to handle all such information in a sensitive and professional manner.

## 2. Purpose

WMC possesses Confidential Information related to its business operations, including sensitive information about employees. WMC also receives similar information from business partners and other counterparties. This policy establishes guidelines for the treatment, handling and protection of all such Confidential Information to prevent unauthorized disclosure or misuse, as this could lead to legal consequences and reputational damage.

## 3. Scope

This policy applies to all of WMC's Personnel and remains binding even after their employment or contractual relationship with WMC ends, for as long as the information in their possession qualifies as Confidential Information under this policy or applicable laws.

Capitalized terms used herein shall have the meanings ascribed to them in Section 7.

## 4. Procedures

### 4.1 Obligations

WMC Personnel is strictly prohibited from sharing any Confidential Information unless they have received approval from the Compliance Officer or when disclosure is required by law. WMC Personnel are expected to handle all Confidential Information with care. To ensure desired conduct and avoid the (unintentional) disclosure of Confidential Information, WMC Personnel are obliged to adhere to the following rules:

**Do's**

- **Access and Use**: Solely access and use Confidential Information necessary for performing Personnel duties.
- **Secure Viewing**: Only view WMC documents, especially Confidential Information, on protected WMC devices and through WMC-approved Microsoft Teams platforms as per the WMC Information Technology Policy. Do not replicate or store Confidential Information on unsecure or personal devices.
- **Password Security**: Change passwords periodically or as directed by WMC's Data and IT division, to prevent security breaches and unauthorized access.
- **Disposal of Documents**: Securely dispose of confidential documents and information containing personal data regularly, when asked, or when no longer needed to perform Personnel duties. This means: shredding hard copies (paper) and deleting digital information.
- **Workstation Security**: Lock desktops/laptops when away (even for a short break), and keep workspaces clear of business documents, notes and other sensitive materials to prevent theft or unauthorized access.

- **Communication and Confidentiality**: When communicating Confidential Information (both internally and externally), emphasise and repeat the confidential nature of such information in the respective email and other forms of communication. In addition,
- If necessary, use project/client codes.
- Include the WMC-required confidentiality notice at the bottom of all Personnel email signatures.
- **External Disclosure Precautions**: Before external calls, actively discuss internally what information can and cannot be shared with the external party and discuss whether an NDA is required, if one is not already in place.
- **Contractual Awareness**: Be aware of WMC's contractual non-disclosure and non-use obligations under Contracts, especially NDAs, as well as who is authorized thereunder to receive Confidential Information.

**Don't**

- **Share Without Need**: Do not share or discuss Confidential Information with Personnel who do not need to know the information to perform their duties or with external parties unless explicitly permitted under the applicable Contract or by the Compliance Officer.
- **Use for Unapproved Purposes**: Do not use Confidential Information for any purpose other than the one set out in the applicable Contract or for which it was collected.
- **Access on Public Networks**: Do not use public networks (e.g., restaurants, hotels) to access Confidential Information.
- **Leave Hardware Unattended**: Do not leave WMC hardware unattended in unprotected or public places.

### 4.2 Confidentiality Measures

To ensure that Confidential Information is managed and handled sensitively and with the strictest confidence both internally and externally, WMC has, *inter alia*, implemented the following measures to encourage Personnel behaviour in accordance with this policy:

- **Restricted Access to Confidential Information**: Only authorised staff who require access for their roles have permission to access specific folders, shared mailboxes, and databases.
- **Secure Data Protection Practices**: Use of secure passwords and encryption of sensitive data, along with other data security measures outlined in WMC's Information and Technology Policy.
- **Legal Guidance on Disclosure Obligations:** Providing access to the legal department for guidance on Contracts, including:
- defining what constitutes Confidential Information;
- identifying what may be disclosed to third parties under the Contract without prior approval;
- obtaining consent to disclose Confidential Information under a Contract when required.
- **Clear Communication of Confidentiality Standards**: Having discussions with Personnel about what can and cannot be shared and clearly communicating these standards both verbally and in writing.
- **Active Reporting and Improvement**: Encouraging and rewarding the reporting of violations to improve confidentiality practices, enhance processes and create learning opportunities.

### 4.3 Training and Awareness

Training on this policy and its contents is provided to WMC Personnel at the discretion of the Compliance Officer (which will include regular periodic training as well as training upon the occurrence of any significant compliance incidents). As well, contracts of WMC Personnel contain confidentiality obligations and WMC requires all its employees to sign its Code of Conduct which contains such obligations.

Additional training is available for WMC Personnel upon request.

This policy will be provided to all WMC Personnel through the WMC Intranet.

### 4.4 Monitoring and Reporting

This policy is regularly monitored by the Compliance Officer.

Following an incident or complaint, the Compliance Officer will conduct an investigation and provide the WMC Board with a report, including findings, recommended actions, and preventative measures to mitigate future risks.

## 5. Policy Violations

To report non-compliance (or suspected non-compliance) of this policy, please contact the Compliance Officer—who will evaluate what action is required and appropriate.

WMC Personnel who violate this policy, or do not report violations of this policy, will be subject to appropriate disciplinary measures which could include legal action and/or termination of their employment or contract.

## 6. Other

### 6.1 Related Information

Additional information regarding WMC's values and guidelines on the acceptable behaviours of its Personnel is provided in further detail in WMC's Code of Conduct.

Information regarding the Information Technology Policy for WMC Personnel is available on WMC's Intranet.

Questions or comments pertaining to this policy may be directed to the Compliance Officer.

### 6.2 Policy History

| | |
|---|---|
| Version 1 | Effective 1 December 2022 |
| Version 2 | Effective 10 February 2025 |

## 7. Definitions

| | |
|---|---|
| CONFIDENTIAL INFORMATION | Confidential Information refers to all non-public information concerning WMC, its business operations, employees, counterparties or other related matters. This includes, but is not limited to:<br>Business information such as strategies, plans, financial data, trade secrets and intellectual property;<br>Supplier, customer and other counterparty information, including agreements, transaction structures, commercial terms (including pricing), communications, negotiations and other sensitive data;<br>Third-party information disclosed to WMC under confidentiality obligations, including information shared under Contracts;<br>Personal data of Personnel, including employment details or compensation;<br>Technology-related information, such as proprietary software, hardware specifications, technical designs, and systems architecture.<br>Confidential Information encompasses any such information in any form, including written, electronic, oral, or visual, whether or not marked as "confidential." |
| CONTRACT | A written agreement that establishes legally binding obligations between WMC and another party. This includes, but is not limited to, agreements related to the purchase or sale of goods or services, NDAs, memoranda of understanding (MOUs), supplier agreements, customer agreements, joint venture agreements, and any other legally enforceable commitments that impose confidentiality obligations on WMC. |
| NDA | A non-disclosure agreement, confidentiality agreement or other Contract primarily focused on confidentiality obligations. |
| PERSONNEL | WMC employees and third parties acting on behalf of WMC. |
| WMC | WMC Group B.V. and its affiliates. |