



WMC

Confidentiality
Policy

Confidentiality Policy

Effective date: 1 December 2022

Review period: Every two years

Version: 1 (Approved 1 December 2022)

Policy owner: Compliance Officer

Related document(s): NA

Public document: Yes

1.0 POLICY STATEMENT

WMC commits to safeguard confidential information possessed and received by WMC and to handle all confidential information in a sensitive and professional manner.

2.0 EXECUTIVE SUMMARY

WMC possesses confidential information about its business, employees and contractors, including personal data. WMC also receives confidential information from agents, suppliers, business partners and other counterparties. The purpose of this policy is to set guidelines on how such confidential information should be treated and protected.

3.0 SCOPE

This policy is applicable to all of WMC's employees and third parties acting on behalf of WMC (Personnel).

This policy is binding on Personnel even after they have left WMC's employment or have stopped working as WMC's contractor.

4.0 PROCEDURES

4.1 Obligations under this policy

Breaches of confidentiality could lead to reputational damage and could have legal consequences. As such, WMC Personnel are not allowed to share any confidential information unless they have received approval from management or when disclosure is required by law.

Personnel are expected to handle confidential information with care. To ensure desired conduct and avoid the (unintentional) disclosure of confidential information, Personnel are obliged to adhere to the following rules:

Do

- Access and use confidential information solely for the purposes of performing your duties as an employee and/or third party acting on behalf of WMC.
- Only view confidential information on protected WMC devices and do not replicate or store confidential information on insecure or personal devices.
- Change passwords periodically to prevent security breaches and unauthorized access.
- (Regularly) Dispose of confidential documents by (i) with respect to hard copies (paper), shredding, and (ii) with respect to digital information, deleting from your devices, when such documents are no longer needed to perform your duties.
- Dispose of confidential information containing personal data when the data is no longer required (as required by Dutch privacy laws).
- Leave working spaces free of business documents, notes, etc. to prevent information theft and security breaches.
- When communicating confidential information both internally and externally, emphasise and repeat the confidential nature of such information in email exchanges and other forms of communication. If necessary, use codes for the projects/clients (as it is also used in the financial sector).
- Ahead of external calls, actively discuss internally what information can and cannot be shared with the external party and discuss whether a non-disclosure agreement should be entered into with the third party, if there is not currently one in place.
- Be aware of WMC's contractual non-disclosure and non-use obligations to third parties under applicable non-disclosure agreements and other contracts, including with whom confidential information can be shared.

Don't

- Distribute confidential information to WMC Personnel who do not need to know the information for the performance of their duties or to external parties unless permitted, either in accordance with the terms of the applicable non-disclosure agreement or contract or by the Compliance Officer.
- Discuss confidential information with others unless permitted, either in accordance with the terms of the applicable non-disclosure agreement or contract or by the Compliance Officer.
- Use confidential information for any other objective than what is set out in the applicable non-disclosure agreement or contract or the purpose for which the information was collected.
- Use public networks (e.g., restaurants, coffee shop, etc.) to access confidential information.
- Leave WMC hardware unattended in unprotected or public places.
- Use WMC's equipment, documents, or other confidential (intellectual) property for personal use or pass it on to third parties.

4.2 Confidential Measures

To ensure that confidential information is handled sensitively and with the strictest confidence internally and externally, the following measures have been put into place by WMC to encourage Personnel behaviour in accordance with this policy:

- Giving permissions to have access to the confidential folders and shared mailbox only to authorised staff.
- Providing secure passwords and encrypting sensitive data.
- Assigning an internal employee to advise on non-disclosure agreements, including addressing (i) what constitutes confidential information, (ii) what can be disclosed to third parties under the non-disclosure agreement without prior approval, and (iii) asking for consent to disclose confidential information under a non-disclosure agreement when required.
- Having in-depth discussions about what can and cannot be shared and clearly communicating it internally and in writing.
- Fostering an open culture which stimulates honesty within the team in case confidential information is shared by WMC Personnel. Reporting should be rewarded (and not punished); this way the others can be prepared, learn and improve.

4.3 Training and Awareness

WMC ensures the protection of confidential information by regularly reviewing and updating this policy as well as continuously enforcing the compliance of this policy within WMC. As well, WMC requires all Personnel to sign a confidentiality agreement.

This policy will be provided to Personnel and made available on the WMC Intranet.

Training is available for Personnel regarding compliance of this policy upon request.

4.4 Monitoring and Reporting

This policy is regularly monitored by the Compliance Officer.

Following an incident or complaint, the Compliance Officer will report to the WMC Board with an update and recommended action on how best to proceed and/or how best to develop preventative measures for future.

5.0 DEFINITIONS

CONFIDENTIAL INFORMATION

Confidential information refers to all non-public information regarding WMC, its business activities, its employees and counterparties. It includes, but is not limited to, information regarding WMC's business activities (e.g., financial transactions) and strategies, employee's personal data, sensitive customer information, supplier lists, information from third parties disclosed to WMC, information relating to and embedded in WMC software or hardware, etc.

PERSONNEL

WMC employees and third parties acting on behalf of WMC.

WMC

WMC Energy B.V. and its affiliates.

6.0 POLICY VIOLATIONS

WMC Personnel who violate this policy and/or willfully share confidential information will be subject to appropriate disciplinary measures which could lead to dismissal or legal action. This also applies to employees even after they have left WMC's employment.

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

7.0 OTHER

7.1 Related Information

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

7.2 Policy History

Version 1 Effective 1 December 2022