URÍA
MENÉNDEZ

Information Security Policy

URÍA
MENÉNDEZ

Information Security Policy

Information, particularly that relating to clients − and the systems used to process it − are critical assets for Uría Menéndez Abogados, S.L.P. (collectively with our branches and subsidiaries, "**UM**"). As such, they must be properly protected (regardless of the type of information and the storage methods used) to ensure the proper functioning of our operations, safeguard our business and maintain the quality of services we provide to our clients.

We manage our information systems and assets according to this information security policy ("**Policy**"), which is based on three core principles:

- Confidentiality: ensuring that only authorised persons, processes and systems have access to information.
- Integrity: preventing unauthorised parties from altering, tampering with or corrupting information.
- Availability: ensuring that authorised users have access to information and the recovery of data lost or compromised due to a security incident.

To achieve our information security objectives, this Policy establishes procedures and measures that comply with legal and regulatory requirements, striking a proportionate balance between identified risks and the efficient use of resources.

This Policy applies to everyone at UM in Spain and Portugal, as well as all our branches and subsidiaries. It also applies to third parties directly or indirectly involved in any of the services UM provides; such third parties must comply with their contractual security and confidential obligations and their compliance will be regularly monitored. Our commitment to continually improve our information security management system is based on the following key objectives:

- Ensuring that our information systems maintain an appropriate level of security and resilience as recommended by UM's Information Security Committee.
- Implementing least privilege mechanisms (in terms of scope and number of users) to ensure that users have only the access strictly necessary to perform their job functions.
- Maintaining a default closed-access control policy under which the information and the systems that process or store the information are closed and only made accessible when strictly necessary, based on their classification level. This includes implementing data-lifecycle controls to ensure information is securely managed from creation to destruction.
- Establishing specific measures to ensure secure access through corporate devices and during remote work, including the use of VPNs, multi-factor authentication, encrypted devices, and minimum configuration controls, to protect information assets and systems against unauthorised access.
- Having a clearly defined set of information security roles and responsibilities, reflected in UM's

organisational chart and assigned in such a way to prevent conflicts of interest and ensure that access to information is limited to authorised individuals or processes with a legitimate need.

- Establishing analysis, prevention, detection, response, and recovery tools and procedures while adapting quickly to technological changes and emerging threats. This includes a systematic, documented, and continuous risk management process to identify, assess, treat, and monitor the risks that could impact the confidentiality, integrity, and availability of UM's information assets and systems.
- Designing and implementing appropriate levels of security based on the risk analysis of each information asset and the systems that store, process or manage information. This ensures a comprehensive security posture, enables business continuity during critical incidents or disasters, and ensures that security measures are proportionate to the identified risks.
- Promoting awareness of security risks at UM and ensuring that we all receive the necessary information security training and possess the technical capabilities to protect our information systems.
- Collaborating with the corresponding authorities and agencies to improve our security and keep abreast of regulatory developments.
- Establishing readily accessible reporting channels
- Regularly reviewing and updating our security management model to ensure continued protection against emerging threats that could impact UM and to guarantee its continuous effectiveness.

UM's Information Security Committee approved this Policy on 30 May 2025.

In line with the principles of this Policy, UM's information security management system is certified under ISO/IEC 27001:2022 and therefore adheres to international standards and recognised best practices in information security.

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED