URÍA
MENÉNDEZ

# Information Security Policy

# Information Security Policy

All information, especially that relating to clients, and the systems used to process it are critical assets for Uría Menéndez Abogados, S.L.P. (jointly with our branches and subsidiaries, "**UM**") and as such need to be properly protected (regardless of the storage methods used) so that UM can operate correctly, safeguard our business and the services we provide to our clients.

We manage our information systems according to this information security policy ("**Policy**"), which is based on three basic mainstays:

- Confidentiality: only authorised persons, processes and systems may access data and information assets to avoid unauthorised data disclosures.
- Integrity: unauthorised third parties must be prevented from manipulating information.
- Availability: authorised users must be guaranteed access to the information they need and UM have systems in place to recover data that are lost or corrupted due to a security breach.

To achieve our information security objectives, this Policy sets out procedures and measures that meet statutory requirements and are proportional in achieving a balance between the risks posed and an efficient use of resources.

The Policy applies to everyone at UM. It also applies to third parties directly or indirectly involved in any of the services UM provides. Our commitment to continually improve our information security management system is based on the following fundamental principles:

- Guaranteeing our information systems have the right level of security and resilience as proposed by the Information Security Committee.
- Putting in place minimal privilege mechanisms (in terms of content and number of people) designed to ensure users only have the access that is strictly necessary for them to perform their jobs.
- Having a default closed-access control policy, under which the information and the systems that process or store are closed and only opened when strictly necessary.
- Having a clearly defined set of information security roles and responsibilities that are reflected in UM's organisational chart and assigned in such a way that avoids conflicts of interest and limits access to information to those persons or processes that need it.

- Having tools and procedures in place to analyse, prevent, detect, respond to and recover from security breaches and adapt quickly to technological changes and new threats.
- Designing and implementing various levels of security according to each asset's risk analysis, to achieve effective defence in depth.
- Making everyone at UM aware of security risks and ensuring that we all have the necessary information security training and technological ability to protect our information systems.
- Working together with the corresponding authorities and agencies to improve our security and keep abreast of regulatory developments.
- Having readily accessible channels in place to report and promptly deal with security breaches.
- Reviewing and updating the security management model to ensure continued protection against new threats.

Our Information Security Committee approved this Policy on 14 June 2023.

In line with the principles of this Policy, UM's information security management system holds the ISO/IEC 27001 certification, with the firm therefore meeting international standards and following best practices in the field.

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED