Parque Tecnológico de Vigo, Calle C, Nave C7
36315 Vigo (Pontevedra), Spain
T/ +34 986 410 091
www.optaresolutions.com

ISMS Security Policy

05-2026-1.0 | Author | securityl@optaresolutions.com | Access Level: Público

Confidentiality

This document is classified under the following access level: Público

Regardless of the confidentiality level, the content of this document is the property of Optare Solutions, S.A. and must be treated in accordance with its classification. Its use, reproduction, or disclosure, in whole or in part, must have the express authorization of Optare Solutions, S.A.

The recipient of this document agrees to respect these conditions and, in the case of a Confidential level, not to copy or disclose the information by any means without the prior and explicit consent of Optare Solutions, S.A.

Purpose and Scope

This document establishes the framework for the Information Security Management System (ISMS) of **Optare Solutions S.A.**, defining its purpose and scope, and formalizes the organization's commitment to information protection. The intended scope of **Optare Solutions S.A**.'s ISMS covers the design, research, and development activities of all types of computer and telecommunications systems, services, and equipment, which correspond to the company's main activity. This policy will apply to all processes, employees, and information assets involved in these activities, ensuring a homogeneous and comprehensive approach to information security management across the organization.

Policy

Optare Solutions is currently **implementing an ISMS in accordance with the ISO/IEC 27001:2022** standard and aligning its security controls with the best practices contained therein, with its formal **certification currently in progress**. This fact reflects the organization's firm commitment to information security management and compliance with international standards. Although the ISO/IEC 27001:2022 certification has not yet been obtained, **Optare Solutions** works proactively to ensure that all requirements of the standard are met, establishing and integrating the necessary measures to protect the confidentiality, integrity, and availability of information from the design phase of its services and products. The company thus demonstrates its determination to protect the information it handles and to create a solid security culture through a continuous improvement process aimed at meeting the requirements of the standard and the expectations of clients and stakeholders.

The **Security Policy of Optare Solutions** (in the ISMS implementation phase) is structured around the following fundamental principles:

- **Commitment to continuous improvement:** Develop and implement the ISMS by providing the necessary resources and promoting continuous improvement, with a special focus on achieving the company's information security and business objectives. Management commits to defining clear security objectives, monitoring compliance, and adjusting processes when necessary, so that the ISMS constantly evolves and improves.

- **Legal and regulatory compliance:** Ensure compliance with all applicable laws, regulations, and contractual obligations regarding information security. From the outset, **Optare Solutions** adopts policies and procedures aligned with the requirements of **ISO/IEC 27001:2022**, anticipating regulatory compliance even before formal certification, and ensuring that obligations to clients, suppliers, and third parties are fully satisfied.

- **Proactive risk management:** Systematically identify and evaluate information security risks in all projects and operations. Establish controls and risk treatment measures in accordance with **ISO/IEC 27002:2022** to mitigate threats and minimize potential impacts on the confidentiality, integrity, and/or availability of information assets. Risk management-based decision-making is encouraged, preventing security incidents and strengthening the resilience of **Optare Solutions**' processes.

The **Management of Optare Solutions** actively supports and drives the adoption of the ISMS, ensuring that information security is embedded into the organizational culture and strategic planning. Metrics and monitoring mechanisms are established to evaluate the performance of the ISMS during its implementation, allowing any deviations to be corrected in a timely manner and ensuring compliance with the certification criteria.

Optare Solutions declares its commitment to obtaining **ISO/IEC 27001:2022** certification in the short term, viewing this effort as an investment in the trust of its clients and the excellence of its services. Being in the certification process means that the company already operates in accordance with international information security standards, providing assurance to stakeholders that the necessary measures are being taken to protect critical data and services. Once obtained, this certification will confirm **Optare Solutions**' continuous alignment with

internationally recognized information security requirements, consolidating its position as an organization committed to quality and security in the telecommunications and information technology sector.

Approval and Validity

This Information Security Policy (ISMS) reflects the organization's commitment to the proper protection and management of its information assets.

This policy has been reviewed, endorsed, and formally approved by the Board of Directors and the Management Committee of Optare Solutions S.A., which assume the commitment to provide the necessary resources for the maintenance and continuous improvement of the Information Security Management System, as well as to ensure compliance with it.

This regulation is mandatory for all personnel, collaborators, and third parties involved in the company's processes, and it covers all activities carried out at our facilities.

Luis A. Alvarez-Sestelo, CEO of Optare Solutions S.A., on behalf of the Board of Directors and the Management Committee of Optare Solutions S.A., at Parque Tecnológico y Logístico Rúa C, Nave C-7, 36315 Vigo, Pontevedra, on May 29, 2026.