Cybersecurity and Digital Resilience

In a constantly evolving digital landscape, characterized by increasingly sophisticated threats, data protection and system resilience represent an essential prerequisite for OVS S.p.A. to guarantee the trust of customers, partners, and shareholders.

Cybersecurity is a strategic priority and is integrated into corporate processes and organizational culture through a structured, proactive, and risk-based approach. We constantly update strategies, technologies, and training programs to mitigate emerging risks, ensure business continuity, and guarantee secure and responsible information management.

Governance and Management Oversight

Cybersecurity is fully integrated into the corporate governance system, and responsibility for the strategy starts at the top management level.

The Board of Directors receives periodic updates on the main technological and cyber risks, while the competent Committees (Risk and Audit) oversee the effectiveness of the internal control system. Top management monitors the implementation of security strategies and the evolution of the corporate risk profile.

The Information Security function, led by the Chief Information Security Officer (CISO), is responsible for defining the security strategy, policies, and controls, as well as coordinating threat response. The CISO reports periodically to the control bodies, ensuring constant alignment between cyber risk management and business objectives.

This model guarantees structured oversight, information transparency, and a clear attribution of responsibilities.

Operational Excellence and Incident Management

We aim to prevent threats, but we are prepared to manage and mitigate any adverse event to ensure business continuity.

- **Cyber Incident Response:** We have a dedicated team for protection and intrusion detection. Our Incident Response Plan follows international standards and is divided into four key phases:
    1. Proactive prevention and protection of corporate infrastructures and data;
    2. Detection and Analysis, with continuous monitoring to promptly identify any anomalies;
    3. Containment and Eradication, with a structured response for incident management;
    4. Recovery and Remediation;
    5. Post-Event Analysis for continuous improvement.
- **System Resilience:** We constantly invest in advanced defense technologies and redundant backup systems to minimize the impact of any incidents on our operations.

Collaborations and External Assessments

We believe that security is a collective effort. For this reason, we constantly validate our defenses through:

- **Audit and Penetration Testing:** We collaborate with leading consulting firms in the sector to carry out independent verifications, intrusion tests, and audits on the robustness of our controls.
- **Information Sharing:** We actively participate in industry networks and Information Sharing and Analysis Centers (ISACs) to exchange information on threats and vulnerabilities, contributing to the security of the entire digital ecosystem.

Third-Party Risk Management

Our security also depends on that of our partners. We apply rigorous IT Due Diligence processes in the selection of suppliers and technological partners. We regularly assess the cyber risk profile of third parties to ensure that our protection standards are maintained throughout the value chain.

The Culture of Security: People Training

People are our first line of defense. We promote a culture of digital responsibility through:

- **Mandatory Training:** Every employee and collaborator participates annually in cybersecurity and data protection training programs.

- **Phishing Simulations:** We regularly run advanced phishing tests to educate staff to recognize social engineering attempts and the most sophisticated cyber threats.
- **Continuous Awareness:** We send periodic communications to update colleagues on new risk trends and best practices to adopt both in the office and when working remotely.

A Responsible and Sustainable Approach

Cybersecurity is an integral part of our ESG commitment. Protecting data, ensuring operational resilience, and preserving stakeholder trust contributes to sustainability and long-term value creation.

We continue to invest in skills, technologies, and processes to maintain high security standards and responsibly address the challenges of the digital landscape.