ZAGREB
AIRPORT

INFORMATION SECURITY POLICY

Zagreb International Airport Jsc. establishes, implements, maintains and continuously improves an information security management system that is in accordance with the requirement IS.D.OR.200 (a)(1) of Commission Delegated Regulation (EU) 2022/1645, and with the requirements of the international standard ISO/IEC 27001:2022

To establish the general principles of the Company regarding the possible impact of risks on air traffic information security, International Zagreb Airport Jsc. is committed to:

- achieving compliance with applicable regulations and implementing relevant standards and best practices in the field of information security,
- implementing information security requirements in the organization's processes,
- continuously improving towards higher levels of maturity of information security processes,
- fulfilling applicable requirements regarding information security and its proactive and systematic management and ensuring adequate resources for implementation and enforcement,
- regularly promoting the Information Security Policy through training and awareness-raising activities for all employees, especially after changes,
- encouraging the implementation of a "just culture",
- encouraging the reporting of vulnerabilities, suspicious/abnormal events and/or information security incidents,
- developing employee awareness of their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance and the consequences of non-compliance with requirements, and
- communicating the Information Security Policy to all relevant parties.

This Policy assigns responsibility for information security in their area of responsibility to all persons holding management positions in the Company as one of their key responsibilities.

The scope of the ISMS includes all activities, processes, ICT systems that may have an impact on air traffic safety, and all other systems that ensure the safe operation of the airport as a key infrastructure.

The general principles of the Information Security Management System defined by this Policy are:

- information security risk management is aimed at preserving confidentiality, integrity, authenticity and availability of information whose compromise, disruption or loss could have a negative impact on air traffic safety,
- information security management system processes are aligned with the continuous improvement approach and take place within the planning, implementation, review and action cycle,
- information security risk management is an integral part of all organizational activities,

ZAGREB AIRPORT

- appropriate and timely involvement of stakeholders, consideration of their knowledge, views and perceptions to improve awareness and informed management of information security risks,
- all employees participate in the timely identification and reporting of information security events and incidents, and
- timely provision of appropriate information and communication technology resources and investment in the development and maintenance of competencies and organizational knowledge in the field of information security.

To ensure continuous improvement of the information security management system, this Policy defines general objectives and performance measures for information security management, as follows:

Goal	Performance measures
Confidentiality of information	0 incidents of unauthorized access; ≥95% access rights review; ≥90% MFA coverage
Data integrity	Error reduction; 100% integrity checking in critical systems; ≥95% successful backups
System availability	≥99.5% availability; recovery within RTO; 0 operational interruptions due to incidents
Security awareness	100% training completed; ≥80% test scores
Incident management	Response within SLA; ≥90% of incidents resolved within deadline; 0 repeat incidents
Compliance with regulations	Reducing non-compliance; ≥95% of examinations carried out; 100% corrective actions
Continuous improvement of ISMS	Annual improvements; positive management review results; reduction in overall risk level

This Policy must be available to every employee and relevant stakeholders, and its continued suitability is ensured through periodic reviews.

This Policy is published in the Company's document management system and is available on the Company website.

Velika Gorica, 24th April 2026

President of the Board	Board Member	Chief Operations Officer - Board Member
Hüseyin Bahadir Bedir	David Gabelica	Nicolas Duthilleul