ZADAR AIRPORT

MANAGEMENT POLICY FOR INFORMATION SYSTEMS SECURITY

Zadar Airport (IATA identification code ZAD) is one of the nine airports in Croatia. It was founded in 1968 near the village of Zemunik Donji and is located 7 km east of Zadar. It is located at an altitude of 88 m. It is the largest aviation center in Croatia. Due to its two runways (in vertical relations) it is able to accept aircraft regardless of weather conditions. It is specialized in the reception and maintenance of firefighting aircraft (Canadair and Air tractors), of which it is also the home port. At the same time, the base of the Croatian Air Force is authorized for the education and training of professional pilots.

Security is an integral part of all business processes and principles of operation and management at Zadar Airport. All employees, business partners and service providers and all other persons who are in any way involved in business processes, or access information owned by Zadar Airport are required to meet the requirements arising from this document.

The goal of information security management at Zadar Airport is to ensure the security of all information at Zadar Airport, additional confidentiality and level of security for customers, clients and suppliers, and raising the level of awareness and quality in everyday business. The goals of information security management are in line with the company's business policy.

The goals of information security at Zadar Airport are to protect information assets, legal and business interests of the company, from damage and losses caused by internal or external, intentional or accidental actions, to reduce the impact of security incidents and ensure business continuity.

The objectives are achieved on the basis of risk assessment and through adopted preventive measures, detection and correction measures and response to possible incidents, in accordance with the relevant legislation, contractual obligations and other business requirements.

The implementation of security programs and the application of established security measures are harmonized with all applicable legal and contractual obligations, international norms and good practice, and above all legal regulations and acts.

All users of the system (employees and business partners who are in any way involved in the business processes of the Company) are required to familiarize themselves with the security practices prescribed by this document and other internal acts governing information security and the proper use of the system.

Information security policy is implemented through organizational, procedural and technical security measures as well as control of their implementation.

The aim of the policy is to ensure that all data and information of the Company, customers and users are protected from unwanted destruction, alteration or loss.

Passwords and user accounts are confidential and may not be disclosed. Any disclosure or sharing of passwords and user accounts is considered the most severe violation of the Security Policy.

The classification of information will be carried out for the business processes, information and systems in the business system of the company. Confidentiality levels and classification classes will be determined by appropriate acts.

Information security management is carried out on the basis of risk assessment, assessment of the company's resources and assets, and the impact and risk they have on the security of information in the company. Threats and vulnerabilities are identified for each resource or information. The aim of risk assessment is to determine the value of individual assets for the company, and the consequences for the company in the event of threats to these risks. Based on the value of individual assets and impacts, the level of risk for the company is calculated.

The manner of implementing the Policy is additionally regulated by the accompanying documents governing information security (policies, methodology, regulations, procedures, instructions, guidelines).

Non-compliance with this Policy or other acts regulating information security, the laws of the Republic of Croatia and all other internal acts of the Company shall be sanctioned in accordance with legal and internal regulations.

General Manager
Josip Klišmanić