INFORMATION SECURITY POLICY OF AENA S.M.E., S.A.

Approved by the Board of Directors of Aena S.M.E., S.A. on 19 December 2023.

I. PURPOSE

Aena S.M.E., S.A. (hereinafter, "**Aena**" or the "**Company**") and any of the companies integrated in its group (hereinafter, "**Subsidiaries**"), under the terms established in article 42 of the Code of Commerce, (hereinafter, "**Aena Group**"), carry out their activity in the field of airport infrastructure management, and are responsible for managing the airports and their infrastructure, including their security, an activity that is carried out in coordination with the Security Forces and Corps.

However, the use of information technologies entails exposure to risks that threaten one of the most valuable assets for business processes: information.

Accordingly, the purpose of the Information Security Policy of Aena S.M.E., S.A. (hereinafter, the "**Policy**") is to establish the principles applicable to the processing of information in the Aena Group, guaranteeing the quality of the information security dimensions and the continuous provision of services, acting preventively, monitoring daily activity to detect any incident and reacting promptly to incidents in order to recover services as soon as possible.

This Policy also defines the mode of access, use, custody and safeguarding of IT assets.

II. SCOPE

This Policy is applicable to the Aena Group, and compliance with it is mandatory for the Board of Directors, executives and, in general, all employees of the Aena Group, without exception and regardless of their position, responsibility or geographical location.

Notwithstanding the foregoing, Subsidiaries registered outside of Spain may make the necessary adaptations to this Policy in order to comply with the local law applicable to them.

However, when within the scope of local law applicable to Subsidiaries registered outside of Spain there is a regulation in force, compliance with which requires the alteration or suppression of essential terms or principles of this policy, its adaptation shall require that, once it is approved in the form of an addendum by the Board of Directors of the corresponding subsidiary, it be submitted, together with a legal report justifying the mandatory nature of the local regulation, to the Board of Directors of Aena SME SA for its final approval. Once the addendum has been definitively approved, it will be published on the website, along with the rest of the policies, and will be communicated to the Aena Directors whose area of responsibility is related to this policy.

The Board of Directors of Aena shall approve a procedure regulating the steps to be followed to adapt corporate policies to the local law applicable to subsidiaries domiciled outside Spain in the cases referred to in the preceding paragraph.

III. PRINCIPLES

In accordance with the principles set out below, the Aena Group undertakes to always guarantee the confidentiality, integrity, availability, authenticity and traceability of the Aena Group's essential and critical information systems, respecting the legal framework in force and faithfully complying with the guidelines, procedures and access regulations established.

3.1. Prevention

To ensure that information and/or services are not adversely affected by security incidents, the Aena Group implements the necessary security measures, as well as any additional controls identified as necessary through a threat and risk assessment. These controls and the security roles and responsibilities of all personnel are clearly defined and documented.

3.2. Detection

The Aena Group establishes operational controls of its information systems with the objective of detecting information security anomalies in the provision of services and acting accordingly according to the principles of continuous monitoring and periodic reassessment. When a significant deviation occurs, the necessary detection, analysis and reporting mechanisms will be established to ensure that they reach those responsible on a regular basis.

3.3. Response

The Aena Group shall establish mechanisms to respond effectively to security incidents, designate a point of contact for communications with respect to incidents detected in other departments or other bodies, and establish protocols for the exchange of information related to the incident.

3.4. Recovery

The Aena Group shall have the necessary means and techniques to guarantee the recovery of the most critical services.

IV. GUIDELINES

This Policy is supported by the premises detailed below, which shall guide the development of the regulations, which will adequately expand the guidelines to each of the environments, situations and settings existing in the Aena Group:

4.1. Information processing

- The Aena Group forbids the disclosure, duplication, modification, destruction, misuse, theft and unauthorised access to information belonging to the Aena Group or to other companies and persons entrusted to it, and access must be granted only to the information necessary for the performance of its functions.
- The information held in the Aena Group's systems is protected in accordance with its importance.

4.2. Use of resources:

- The use of the Aena Group's IT resources (e-mail, Internet, office automation, portable and mobile devices, disk space, etc.) for purposes other than strictly professional ones, related to the normal performance of functions in the Aena Group, shall be regulated.
- Any activity related to information or material subject to intellectual property rights must consider the legal restrictions in this regard. Third party software shall only be used if it is licensed and/or authorised.
- Given the privileges involved in the use of harmful or unauthorised software, the installation of all applications that are not duly authorised or approved by the Aena Group is prohibited.

4.3. Access control to information assets:

- Access to the information stored in the Aena Group's information systems must always be carried out using the authentication systems implemented in the organisation, in addition to any other authentication mechanism accepted and validated by the organisation that may be implemented in the future.
- The authorisation of access to any information asset shall be determined by the need to use said asset for the performance of the different operational functions carried out.

4.4. Protection and security of information assets:

- The protection of the Aena Group's assets is a task that affects all those directly or indirectly linked to the Aena Group, and it is therefore the responsibility of each of them to preserve the confidentiality, integrity, availability, authenticity and traceability of the information, communicating to the competent areas, and through the established channels, any event or incident that affects the information systems.
- Adoption of an information security model that allows the Aena Group's business assets and processes to be protected against security risks of any nature and regardless of the place where they are likely to materialise.

- The Aena Group is committed to keeping its information systems in line with current legislation.

V. MONITORING AND CONTROL

The Audit Committee is responsible for identifying and assessing all the Company's non-financial risks, including operational and technological risks.

VI. EVOLUTION

All companies that make up the Aena Group must approve the internal policies required by the applicable regulatory framework on information security through the competent body.

Furthermore, these internal policies must be reviewed every two years or when significant changes occur that affect their content, application or scope, in such a way as to ensure their efficiency and effectiveness.

VII. VALIDITY

This Policy was approved by the Board of Directors of Aena at its meeting of 19 December 2023.

The previous Aena Information Security Policy approved by the Board of Directors of Aena at its meeting of 28 January 2020, and last updated at its meeting of 20 December 2022, shall remain in force until Aena approves an internal policy of the kind referred to in section VI. *EVOLUTION* of this Policy by the competent body in accordance with the applicable regulations on information security.