



DANMON GROUP  
SYSTEMS

## Information Security Policy Statement

Danmon Group UK Ltd, as a provider of professional broadcast, audiovisual, and media systems integration services, is committed to delivering secure, resilient, and compliant solutions to all clients.

To support this commitment, Danmon has implemented an Information Security Management System (ISMS) aligned to ISO/IEC 27001, with the objective of ensuring business continuity, protecting information assets, and maintaining the confidentiality, integrity, and availability of information across all operations.

Our approach is underpinned by compliance with applicable UK legislation and best practice, including UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and Guidance issued by the National Cyber Security Centre (NCSC)

To this end, it assumes its commitment to information security and establishes the following principles:

- Competence and leadership on the part of management as a commitment to developing the Information Security Management System.
- Determine the internal and external stakeholders that are relevant to the Information Security management system and meet their requirements.
- Understand the organization's context and determine its opportunities and risks regarding information security as a basis for planning actions to address, assume, or deal with them.
- To ensure the satisfaction of our clients, including stakeholders in the company's results, in all matters relating to the performance of our activities and their impact on society.
- Establish objectives and goals focused on evaluating performance in Information Security, as well as continuous improvement in our activities, regulated in the Management System that develops this policy.



## DANMON GROUP

---

SYSTEMS

- Compliance with the requirements of the legislation applicable and regulations to our activity, the commitments made to clients and interested parties and all those internal rules or guidelines to which the company is subject.
- Ensure the confidentiality of the data managed by the company and the availability of information systems, both in the services offered to clients and in internal management, preventing undue alterations to the information.
- Ensure the ability to respond to emergency situations, restoring the operation of critical services in the shortest possible time.
- . Establish appropriate measures for the treatment of risks arising from the identification and assessment of assets.
- Motivate and train all personnel working in the organization, both for the correct performance of their job and to act in accordance with the requirements imposed by the reference standard, providing a suitable environment for the operation of the processes.
- . Maintaining fluid communication both internally, between the different levels of the company, and with clients.
- Evaluate and guarantee the technical competence of the staff for the performance of their functions, as well as ensure the adequate motivation of the staff for their participation in the continuous improvement of our processes.
- . Ensure the proper condition of the facilities and the appropriate equipment, so that they correspond to the activity, objectives and goals of the company
- Ensure continuous analysis of all relevant processes, establishing appropriate improvements in each case, based on the results obtained and the objectives set.

These principles are adopted by the General Management, who provides the necessary means and equips its employees with sufficient resources for their fulfillment, embodying them and making them publicly known through this Information Security Policy.