Information Security Policy

Daikin Applied Europe's Information Security Policy is intended to provide a framework for people in the organization and stakeholders regarding information security objectives.
This translates into the safeguarding of the parameters of:
Confidentiality: the information must not be accessible to unauthorized parties;
Integrity: the information must not be modified by unauthorized parties, must not be corrupted, and must be reliable;
Availability: Information must be accessible to authorized parties promptly.

To ensure that these parameters are respected, the organization undertakes to make available the resources necessary to meet the **applicable requirements** of the ISO/IEC 27001 standard, so that the operating procedures defined by the Information Security Management System (ISMS), the policies and all the controls applicable to the perimeter as defined by the **SOA** – (Statement Of Applicability) – are followed and implemented.

In particular, Daikin Applied Europe's Information Security Management System (ISMS) aims to ensure:

- full knowledge and assessment of the criticality of the information managed, through appropriate **risk analysis activities**;
- **secure logical access** to information under the "Need to know" principle;
- full **awareness** of all parties involved in information security processes;
- that **the organization and any third parties** involved collaborate in the processing of information by adopting procedures aimed at complying with adequate levels of security, by procedures and policies of the ISMS;
- the **timely recognition** of events, anomalies, and vulnerabilities so that their correct management ensures the protection of information and the minimization of impacts on business processes and stakeholders.
- that **physical access to the** premises and areas is only by authorized personnel;
- compliance with legal requirements and security commitments set out in contracts with stakeholders;
- the **continuity of business processes** through the definition and application of suitable Business Continuity Plans that include adequate Disaster Recovery Plans;
- that the staff and third parties involved in the processing are appropriately **trained** in the field of information security, gaining the necessary awareness for the correct management of data and information.
- that suppliers are appropriately verified, as applicable, through contractual clauses, audits, monitoring activities, sharing of plans, and improvement actions;
- that in **the design phase, in the creation of products, and in the provision of services,** security requirements are appropriately considered from their design according to the principle of Security & Data Protection by design.
- that **events** and **incidents** related to information security are promptly identified, analyzed, assessed, and processed in order to prevent or reduce their impacts, balancing them with business risk, its sustainability, and its predisposition to innovation;
- that every opportunity for **improvement** is identified and analyzed so that it can be seized;
- that the **processing of personal data** takes place in compliance with the European Regulation on the Protection of Personal Data (GDPR) 679/2016.

The organization has defined a **risk assessment** methodology based on the guidelines of ISO/IEC 27005 and the appropriate **objectives** (KPIs) and related monitoring parameters for the management of the performance of the ISMS have been identified.

The information security management system is constantly monitored and updated to ensure its **continuous improvement**, also with the help of periodic audits to which all interested parties are periodically subjected, in order to maintain a high level of awareness on the issue of information security.

This policy is shared and made available to the organization and all interested parties through the intranet system and specific **communication channels**.

The organization has also defined precise **responsibilities** for the definition and management of the ISMS, in particular by providing for a specific role assigned to the Information Security Manager.

In general, in terms of information, Daikin Applied Europe has among its primary objectives:

- address the growing risks related to the civil or legal liability of the organization and management as a result of inaccurate information or the lack of due care in its protection or non-compliance with mandatory regulations;
- ensure policy compliance;
- increase predictability and reduce uncertainty in business operations by bringing risk to definable and acceptable levels;
- provide a level of assurance that critical decisions are not based on incorrect information;
- provide a solid foundation for efficient and effective risk management, process improvement, rapid incident response, and continuity management;
- improve trust in relationships with customers and partners;
- protect the reputation of the organization;
- enable new and better ways to process electronic transactions;
- assign responsibilities for safeguarding information in the performance of business activities, business recovery processes, and in response to regulations;
- effective and efficient management of resources dedicated to information security.

In summary, implementing an effective information security strategy can add value to the organization by reducing losses that result from information security events and providing assurance that security incidents and breaches are not catastrophic.

This Information Security Policy is periodically reviewed by the Management to ensure that it is continuously updated in line with the evolution of the context in which Daikin Applied Europe S.p.A. operates.

Ariccia, 09/01/2024

Francesco Aruta
Information Security Representative

Claudio Capozio
Chief Executive Officer
Daikin Applied Europe S.p.A