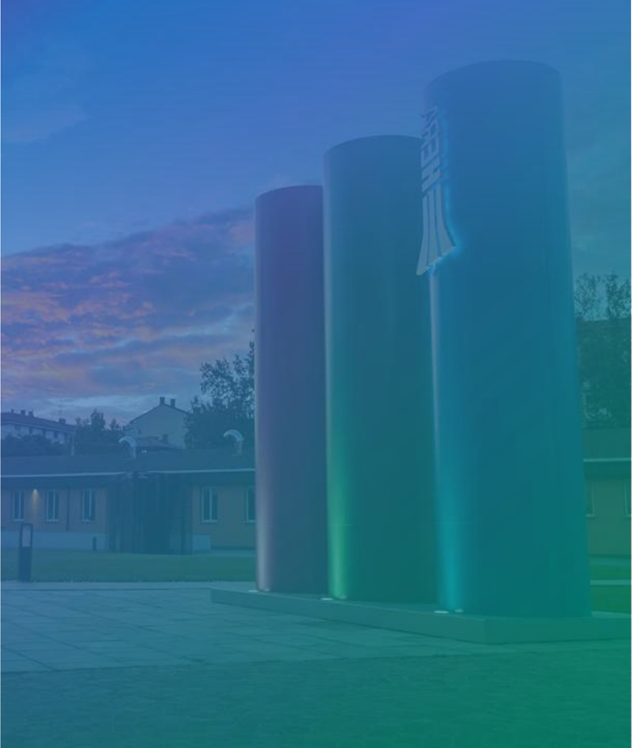
GRUPPO HERA

Information Security in Hera Group

Solid infrastructures for a long-term sustainable strategy

Photo by Silvia Camporesi: construction phase of the biomethane plant of Sant'Agata Bolognese

Information Security Governance



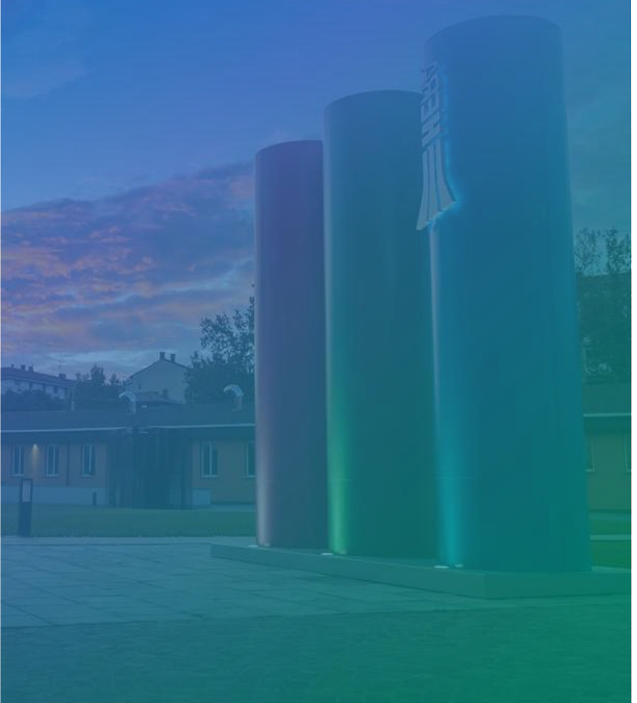
The management of information security in the Hera Group is integrated right from the design phases, adopting the principle of security by design to effectively protect company data, especially personal data, and achieve privacy by design. The governance of this area is embodied in a “multi-risk” approach to data and information processing aimed at increasing the resistance, with a certain level of reliability, of information and network systems to events that could compromise availability, authenticity, integrity or confidentiality. To this end, a business impact analysis is kept up to date on all of the Group’s information systems, supported by a continuously updated document system, including the Information security policy guidelines, the Personal data protection policy, and a series of information security policies that establish the guiding principles for all activities relating to information security, including the assignment of responsibilities to clearly defined organisational roles.

The company’s executive board members takes part in defining acceptable risk through the Risk Committee, which annually assesses information security and proposes mitigation initiatives, which are constantly monitored, based on the methodology of the national cybersecurity framework, in line with applicable regulations. Within the Control and Risk Committee a board member possesses expertise in IT security.

In 2024, a priority project was launched to adapt the Group companies to the NIS2 Directive, which strengthened cybersecurity obligations and expanded the number of sectors and parties involved, also involving the supply chain. Again, with a view to improving the protection of data availability, the Group launched a modular ISO 22301 certification project, the international standard developed to guide organisations in identifying potential threats to their business processes and in building effective backup systems and processes to safeguard their interests and those of stakeholders. In this context, particular and specific focus was given to the continuity of the IT systems of critical processes.
Particular attention is also paid to the impacts of the adoption of artificial intelligence solutions within the Group, also in light of European Regulation 2024/1689 and which led to the adoption of a specific Group policy in the use of artificial intelligence.

The Hera Group has had a cybersecurity department since 2020, headed by a Chief Information Security Officer who reports directly to the Chief Innovation Officer and the Executive Management Team.

Information Security Policy



Policy statement

The Hera Group's Executive Board considers the protection of information a fundamental value, including both business-critical information and personal data. The loss of Confidentiality, Integrity, and Availability could cause significant financial losses and harm to the company's market image. The Group's reputation is directly tied to how it manages corporate information, particularly through information systems. To make the Information Security Management Process effective and efficient, the approach to Information Security must be a collective effort, involving the participation and support of all Hera Group employees and its suppliers.

The purpose of this document is to define the strategy of Privacy & Security by design and provide a guideline to all corporate functions for continuously improving information security and complying with the current Privacy regulations (particularly GDPR 2016/679 and privacy code), in implementation of the Hera Group's "Policy for the protection of personal data" and in line with the Information Security Management System, according to the ISO/IEC 27001 standard. This Guideline contains the references for the design and maintenance of privacy and information security management systems and allows for a comprehensive and uniform protection system across the various technological, logistical, and organizational areas of the Hera Group. The lack or non-application of these references, which direct all corporate functions on their roles in the corporate security building process and privacy compliance, results in a lack of uniformity in the level of protection and privacy compliance.

Area of application

This guideline is applied in Hera S.p.A. and all its controlled companies, which will implement it through their own documentation system. All Group companies must comply with the Parent Company's requirements.

Implementation procedures

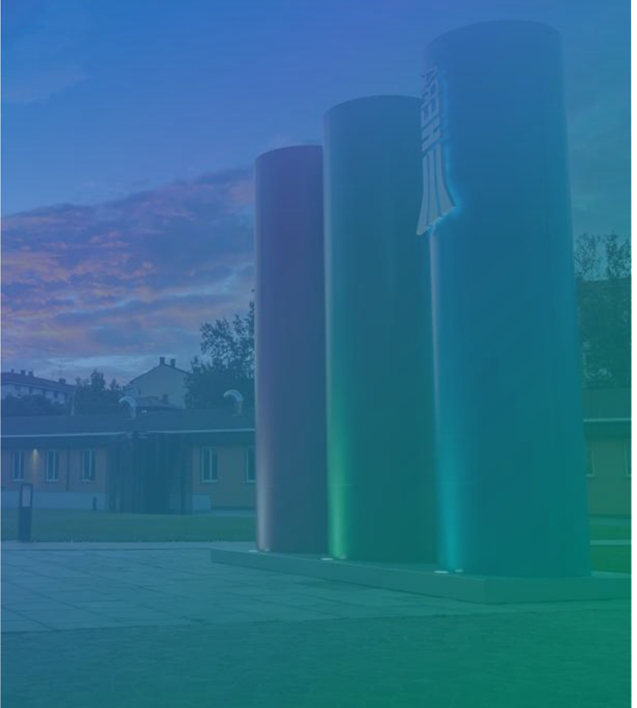
Information and particularly personal data must always be protected and controlled, considering their nature and the specific characteristics of their processing. Information security is implemented by adopting measures to protect confidentiality, integrity, and availability to minimize the risks of destruction or loss, even accidental; unauthorized access; and unapproved operations. The management processes necessary to ensure the effectiveness and efficiency of these measures must be implemented. Within the Hera Group, it must be ensured that:

1. There is full knowledge of the managed information and an assessment of its criticality to facilitate the implementation of appropriate protection levels;
2. The organization and third parties collaborating on information processing adopt procedures that ensure adequate security levels and are fully aware of security-related issues;
3. Anomalies and incidents impacting the information system and corporate security levels are promptly recognized and managed through effective prevention, communication, and reaction systems to minimize the impact on business, customers, and individuals;
4. Access to company premises, individual company areas, and information is exclusively by authorized personnel, to protect area security and prevent unauthorized processing;
5. Business Continuity and Disaster Recovery are ensured through the application of formalized security procedures.

To fulfill these commitments, the Hera Group follows "Risk-Based" principles for correctly identifying and assessing risk and opportunity factors through:

- The adoption of a systematic, structured, and proactive approach to risk management, also in terms of Business Impact Analysis;
- The identification and implementation of actions to reduce undesired effects by identifying factors that could create criticalities in processes, thus governing the achievement of planned business objectives;
- Strengthening resilience to cyber threats by creating a unified Group approach to information and personal data security.

Information Security Policy



Compliance Management with the Current Regulatory Framework

Monitoring Regulatory Sources: the Hera Group must comply with applicable laws. To ensure this compliance, regulatory sources must be constantly monitored. Particular attention must be paid to laws governing:

- Aspects directly related to corporate business activities (Authority provisions);
- Privacy protection (EU Regulation No. 2016/679; Legislative Decree 196/03 updated by Legislative Decree 101/2018 of 10/08/2018; General Provisions issued by the Privacy Guarantor published in the Official Gazette);
- Intellectual property protection.

Updating Security Procedures: the Procedural Body must be continuously updated based on:

- The technological scenario;
- Security incidents;
- Auditing and Risk Management activities;
- Regulatory changes**.**

Compliance Obligations with Copyright

The Hera Group commits to aligning its software management processes with copyright protection laws, requiring suppliers to respect the same obligations.

Audits and Controls

Periodic and continuous audits on the management and protection of personal data, Penetration Tests, and Vulnerability Assessments of the Hera Group's information security must be planned to monitor whether the current state aligns with Corporate Policies, regulations, and existing procedures. These activities will help evaluate the effectiveness of the adopted countermeasures and controls.

Audits must also be systematically carried out on all organizational components of the company, particularly management processes, including outsourced ones, and processes involving personal data processing.

Internal and Third-Party Personnel Management

Hera Group personnel are required to comply with the Information security guidelines, as well as to report any operational anomalies of the control systems established and improvement opportunities identified in the use of corporate systems.

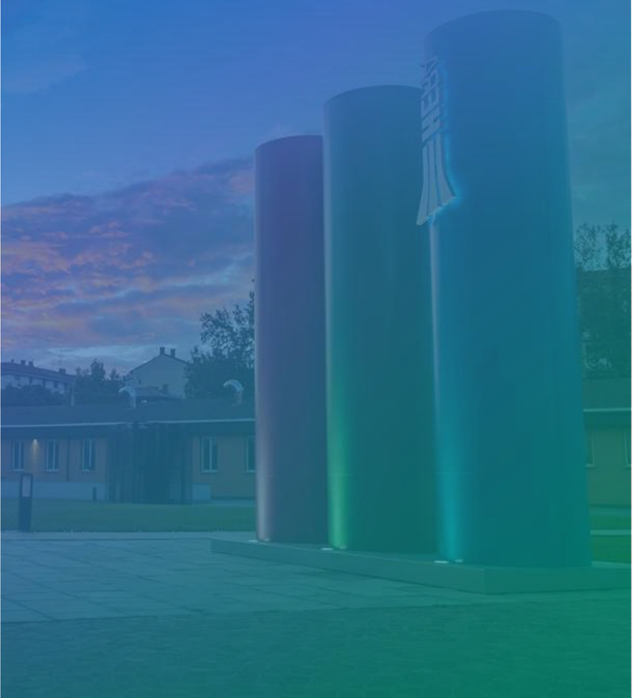
All personnel involved in managing corporate information must receive training and be aware of the strategic importance of an Information and Data Protection Management System. All personnel must be informed and trained on security aspects and data protection through the dissemination of a precise and defined awareness program. The effectiveness of these programs must be periodically verified. Employees needing access to corporate information must respect confidentiality and non-disclosure agreements specified in the employment contract, the Code of Ethics, and corporate Privacy provisions. The presence of external personnel who may come into contact with corporate information for a defined period or due to work needs could create vulnerabilities in the Information and Data Protection Management Process. Therefore, an adequate level of control must also be applied to suppliers that must comply with the requirements set forth in this policy. To this end, specific clauses on information security and personal data protection must be explicitly included in contracts. These clauses must include:

- Definition of responsibilities regarding security aspects;
- Definition of responsibilities for processing personal data, always identifying the Data Controller and/or the Processor;
- Signing specific confidentiality and non-disclosure agreements (NDA - Non-Disclosure Agreement) that provide for penalties in case of agreement violations.

Control methods

The application of this Guideline will be verified during internal audits conducted by the competent corporate structures.

Information Security Management Programs



In 2024, the initiatives related to improving the Group's cyber security continued, with ongoing coordination between the initiatives of individual IT and OT managers and the centralised Group initiatives.

In 2024, in light of the ever-increasing development of cloud and multi-platform environments, a specific solution was introduced for monitoring cyber security in the cloud with alarm integration at the Group's Security Operations Centre, the hub for aggregating and monitoring all internal and external information relating to cyber security. As regards the trend of events monitored by the Security operation centre, in 2024 there was a slight decline in the unusual events analysed compared with 2023, a positive trend due to the continuous improvement of the event correlation rules despite the increase in attacks from outside and the extension of the monitoring perimeter. Still in relation to the cyber security operations, in 2024 the quarterly vulnerability assessment continued, and was extended to any part of the company exposed to the Internet.

In the process area, in 2024, to combat the issue of Shadow-IT (i.e. systems not formally managed by an IT manager), a specific procedure and an online platform were introduced for cataloguing all the systems involved, as well as a related analysis in terms of cyber security.

On the people side, awareness-raising continued via awareness campaigns and trainings extended to the whole company and incident simulation exercises for more technical profiles.

Hera Group personnel are required to comply with the Information security guidelines, as well as to report any operational anomalies of the control systems established and improvement opportunities identified in the use of corporate systems.

Company personnel must collaborate with IT/OT Managers and competent company structures, and in particular report IT security incidents to a dedicated email address, according to the procedures detailed in the ICT Security Incident Management procedure. These incidents include any event, generated by IT tools, that threatens or could threaten information security, understood as loss of data confidentiality, data damage or integrity, malicious interruption of data availability, regardless of its severity.

In 2024, four cyber incidents were recorded, none of which had significant impacts on the company's operations or involved customers' personal data. One of the incidents was related to the malfunctioning of the CrowdStrike solution that impacted many companies around the world. For the Hera Group, the impact was reduced thanks to the limited use of this solution on the Group's systems.

The cybersecurity posture, which refers to an organisation's overall strength and readiness in defending against cyber threats, is monitored using sector indicators and benchmarks. The focus on the Group's IT service providers, during the selection, assignment and control phases, is subject to continuous improvement, especially in light of new mandatory regulations.

As regards cybersecurity, the Group's Security operation centre (SOC) is active, i.e. the centralised service for realtime monitoring of events affecting information systems, IT infrastructures and industrial areas (OT). In operational terms, this service works through the use of hardware probes and software agents, and sees a continuous increase in alerts coming both from external factors (continuous increase in attacks and their level of sophistication), and from the increase in the perimeter analysed due to the increase in computer and industrial systems belonging to the Group.

This service is constantly being developed in terms of the new correlation and regulation rules put in place, to counter false positives and not lose effectiveness in detecting anomalous events in the early stages of possible chains of compromise. In addition to the SOC service, as every year, vulnerability assessment activities continued, to continuously assess the level of penetrability of exposed systems and network security, through an analysis of the Group's perimeter exposed on the Internet. As regards the human factor risk, awareness-raising campaigns intended for all Group employees continued, in addition to periodic ethical phishing simulations and technical exercises intended for IT specialists. During 2024, actions aimed at ensuring the confidentiality, integrity and availability of Hera systems continued to be implemented. For example, in the context of industrial plants, ongoing development went to the converging cyber security monitoring model between the IT (information technology) and OT (operation technology) areas. In order to detect any vulnerabilities on systems or applications that could be exploited by an attacker, vulnerability assessment activities has been carried out also by third party, including the activities related to simulated hacker attacks (penetration tests).

Risks arising from cybercrime, which Hera also assesses in terms of their impact on service continuity, are also given increasing attention. Information security incident response procedures are in place and are tested every year. Coherently with the Information Security Policy, information security systems are periodically internal audited. Furthermore, independent external audits have been carried out on our data centers based on the following standards: ISO 27001, ISO 27017 and ISO 27018 (set of rules comprising the data security management system), ISO 27701 (privacy certification) and Tia-942 Rated 3 (international standard that evaluates configuration and maintenance of data centre highlights) and Csp (Cloud service provider at the National Cybersecurity Agency).