Gestamp

General Information Security Policy

Gestamp Automoción, S.A.

27 February 2023

TABLE OF CONTENTS

1. Introduction

In accordance with Article 249 bis of the Spanish Companies Act (‘**LSC**’ by its Spanish acronym) and Article 8 of the Regulations of the Board of Directors of Gestamp Automoción, S.A. (the ‘**Company**’), it is the responsibility of the Board of Directors to approve general Company policies.

By virtue of the foregoing, the Board of Directors of the Company, by means of the present General Information Security Policy (the ‘**Policy**’), aim to underline the Company and its subsidiaries' (‘**Gestamp**’ or the ‘**Group**’) commitment to complying with the highest information security standards.

2. Purpose and scope

The main purpose of this Policy is to establish a regulatory framework applicable to the Group, for the implementation of security measures that ensure the confidentiality, integrity, and availability of internal and third-party information in the possession of Gestamp.

To this effect, the scope of the present Policy includes both physical and digital security, ensuring the implementation of security measures on an organisational, technical, and staffing level, in order to uphold business continuity, prevent fraud, reduce the risk of suffering a cyber attack, and protect information from being damaged.

3. Scope of application

This Policy is applicable to the Gestamp Group globally. Therefore, it is applicable to all subsidiaries of the Group (notwithstanding the specific terms set out in the legislation applicable to each subsidiary), as well as to their infrastructure, networks, systems, industrial equipment, devices, and projects across all business areas. Likewise, compliance with this Policy is mandatory for all employees, external personnel, and collaborators of Gestamp who, for the purposes of carrying out their duties, need to handle information or operate systems belonging to Gestamp.

Consequently, the present Policy must be made accessible to all Group employees, external personnel and collaborators that are related with the Group through any of its processes.

4. Principles

The main information security principles undertaken by the Group are listed below:

Security by design and by default. The Management of Gestamp and each of the Group's subsidiaries commit to undertake, by design and by default, actions to establish, operate, monitor, maintain, review, and continuously improve information security measures, paying special attention to cybersecurity matters across the Group. In this respect, the Cybersecurity Area is in charge of defining information security goals and objectives, in order to protect the confidentiality, integrity, and availability of this information.

Legality, efficiency, co-responsibility, cooperation, and coordination. Gestamp must comply with the present Policy, all applicable legal, regulatory, statutory, and contractual requirements, as well as the requirements set forth by clients, partners, government bodies, investors, and other interested parties.

Proactive responsibility. The Group's subsidiaries, their employees, and their external personnel and collaborators must be able to demonstrate compliance with the Security Regulatory Framework. To do this, they will provide all necessary evidence.

Prevention and continuous improvement. Gestamp has established a preventive strategy for analysing risks to which the Company is exposed, by identifying these risks, implementing mitigation controls, and enforcing regulatory procedures for reassessment purposes. Throughout this continuous improvement process, Gestamp will oversee the definition of the accepted residual risk level (risk appetite), along with the company's tolerance thresholds.

Incident logging. All incidents or weaknesses that could or have already compromised the confidentiality, integrity, and/or availability of information must be logged and analysed so that the relevant corrective/preventive measures can be applied.

Information classification. Gestamp classifies information in order to enable access control, custody, and monitoring processes. Preventive measures and controls are established according to the information's assigned classification. The more sensitive the information in question, the more restrictive these controls will be.

Information handling limitations. The volume and type of information shared will be limited to that which is strictly necessary to perform the task for which the information was requested. Likewise, the use of any information provided will be limited to the purposes for which it was authorised.

Information access limitations. Access to information will be limited wherever possible, in order to ensure that it is only accessible to authorised individuals. The information owned by Gestamp or under the Company's custody must only be accessible to authorised individuals regardless of whether they belong to the Group.

Confidentiality and integrity. Information will be handled and disseminated in a way that guarantees its security, including protection against the unauthorised/illegal access and use, loss, destruction, or accidental damage of this information, by implementing the appropriate technical or organisational measures.

Availability. The availability of information must be guaranteed via the implementation of suitable backup and business continuity measures.

Training and awareness. Staff with information security responsibilities must be equipped with the necessary knowledge to perform their duties. As such, Gestamp will organise activities that are designed to strengthen the awareness level of all employees regarding the use of information and compliance with related security measures.

5. Structure of the Information Security Regulatory Framework

The Security Regulatory Framework is configured by all those internal information security policies, regulations, procedures, and guidelines applicable to the Group. The hierarchical structure of the Security Regulatory Framework is as follows:

- Level 1. General Information Security Policy. The present document constitutes the main component of the Security Regulatory Framework. It establishes high-level purposes and Gestamp's commitment to managing information security, as well as the key controls and principles required to keep this information secure. The other components of the Regulatory Framework are developed and based on this Policy.

- Level 2. Security procedures and regulations. A set of documents that support the purposes outlined in the Policy. This level describes the security requirements for each section or area included in the Policy in more detail.
- Level 3. Work instructions. These documents detail the set of specific tasks that will be carried out to support daily operations. These tasks are aligned with the security requirements established in the above procedures.

The present Policy, in addition to the requirements set forth in the information security procedures and work instructions that make up Gestamp's Security Regulatory Framework, must be complied with by all employees, and external personnel and collaborators of Group.

The Group's Security Regulatory Framework is based on information security best practices and regulations, such as ISO/IEC 27001, NIST, and Cyber Security Frameworks, and is subject to a yearly review and update process.

6. Information Security Governance

Strategy and operating model

Gestamp formalises the Company's strategic information security plan, which must be aligned with its strategic business plan.

The roles and responsibilities of the Group's employees in relation to information security are defined and assigned to the appropriate individuals. This way, Gestamp's strategy can be correctly structured and developed while demonstrating compliance with the Security Regulatory Framework. This guarantees an appropriate segregation of duties and avoids any potential conflicts of interest. To this effect, the following areas can be outlined:

- Gestamp's Corporate IT. This is the area in charge of handling, maintaining, supporting, and improving corporate and centralized infrastructures and systems, in addition to the connectivity between these components, by always applying the highest quality and security standards. Alignment with the business and the needs of each manufacturing plants and divisions is key to ensuring the delivery of the highest quality services.

- Cybersecurity Area. This is a sub-area of Gestamp's Corporate IT that is in charge of defining information security goals and objectives, with the aim of protecting the confidentiality, integrity, and availability of information and overseeing the execution of the strategy in order to manage information security. This will be done via the implementation of initiatives that allow processes and infrastructures to be protected against the growing number of cyber threats targeting the industry, following a range of international guides, regulations, and standards across Governance, Secure, Vigilant, and Resilient domains.

- Tactical Cybersecurity Committee. This Committee is in charge of making decisions, managing the cybersecurity strategy, and escalating information to the Senior Management. It is made up of the Chief Information Officer (CIO), Gestamp's Corporate IT Manager, and the Managers of the following sub-areas of Gestamp's Corporate IT: the IT Production Manager, the Cybersecurity Manager, and the GRC IT Manager.

Gestamp complies with all applicable legal, regulatory, and contractual requirements for which a control framework is available. This framework is associated with the Security Regulatory Framework in order to verify and monitor compliance levels.

An information security training and awareness strategy is in place to ensure that Gestamp employees correctly perform their duties.

Cyber secure culture

Gestamp fosters a security culture to tackle cyber risk across all levels and sends out regular announcements and messages about the cybersecurity strategy and its overarching objectives.

All Group employees receive cybersecurity training on a regular basis throughout their time at the Company.

Management of cyber risk, indicators, and reporting

Gestamp has a cyber risk management methodology in place that allows it to implement action plans when required. At the same time, it carries out cyber risk assessments and analyses in order to detect the cyber risks to which the Group is exposed and correctly manage and report them.

With the aim of reducing subjectivity and improving the precision of cyber risk monitoring and response activities, Gestamp boasts quantitative cyber risk measures (KPIs) that are included within operational risks.

7. Implementation of Information Security Controls

7.1. Access Control

Gestamp must regulate the access of internal and external personnel to company information systems, as well as the type of information processed or stored, according to the business needs of individuals. Access is granted on a strict need-to-know basis, meaning it is granted exclusively to the users who require the information or its functions for the correct execution of their tasks, in line with their role and profile.

Usernames must be unique and non-transferable. The principle of least privilege must be initially applied to all users, meaning they are granted the minimum access permissions required to perform their duties.

The individuals in charge of handling information assets are responsible for defining access levels and authorising any exceptional access permissions, in line with the guidelines of the authorising party or managers of the information in question or, where appropriate, the process or business owners.

7.2. Software Development Security

Security requirements are applied throughout the entire software development life cycle in place at Gestamp, both in terms of in-house and third-party software. They are applied during the analysis of requirements and feasibility, the phases in which these requirements are outlined and assessed, as well as during design, testing, implementation, acceptance, and subsequent maintenance phases.

To correctly develop software, Gestamp has established a security testing plan that includes secure code reviews, data protection mechanisms, etc. Likewise, pentesting and vulnerability scanning can be carried out on software developments before they are deployed.

Gestamp ensures that information security is an integral part of its processes and procedures for selecting, developing, and implementing applications, products, and services.

Gestamp informs software developers about the present Policy and its objectives, as well as other internal regulations that make up the Security Regulatory Framework.

7.3. System Security

Gestamp has formally established responsibilities and documented procedures in order to ensure that information systems are correctly configured, managed, operated, and monitored.

In addition, Gestamp has implemented protection measures on information systems in order to prevent attacks and data leaks. These measures also help to guarantee the segregation of duties when assigning responsibilities, with the aim of preventing the unauthorised use of information systems.

To ensure the security of systems, Gestamp has a patch management process in place that includes the software base, availability, applicability, acquisition, validation, and deployment phases for the identified assets.

Gestamp performs system hardening in order to correctly implement the Security Regulatory Framework, as well as harden and clearly define user privileges, groups, roles, and service configurations.

7.4. Malware Protection

Gestamp has measures in place to detect, eradicate, and protect its information systems against different types of known malware. Assessments are carried out at least once a year in order to identify and study any new threats that have emerged. This way, the company can confirm which new systems could be exposed to these threats and which ones are prepared to contain them. As a result, all Gestamp information systems boast updated solutions for malware protection.

Gestamp has installed End Point Protection (EPP) software on all servers and computers that is automatically updated. Users are strictly prohibited from disabling or modifying EPP mechanisms or tools, unless they are authorised to do so and have been given the required technical authorisation by the Cybersecurity Area.

7.5. Network Security

Gestamp correctly manages and controls networks with the aim of protecting the company against threats and upholding the security of systems and applications that use the network. This includes network access control, which is designed to protect all information that is sent via these elements/environments.

The information sent and received via both public and private communication networks is effectively protected by security mechanisms that uphold the confidentiality, integrity, and availability of information. The necessary controls are established in order to prevent sender spoofing and the modification or loss of any information sent in communications with both internal network systems and any external parties with which Gestamp collaborates.

A set of technologies and controls have been established for connecting remotely to Gestamp networks depending on individual user profiles.

The guest Wi-Fi network is isolated from the other networks and is protected by security measures involving authentication, monitoring, encryption, etc.

All connections to Gestamp corporate networks must comply with the technical requirements established by the Group and any exceptions must be reviewed and authorised by the Cybersecurity Area in advance.

7.6. Security of End-user Devices

Gestamp has established usage and handling guidelines for corporate devices that leverage information services belonging to the Group.

Users cannot be local administrators for corporate devices to which they have access for work purposes and they must not alter hardware or configuration settings. The installation of software that has not been approved by Gestamp's Corporate IT is forbidden.

7.7. Human Resources Security

Security responsibilities are taken into account throughout the recruitment process and the preparation of contracts. Employees are then informed of these responsibilities once the contract is in force, in order to reduce the risk of fraud or the inappropriate use/tampering/theft of information.

In this regard, Gestamp's information security policies and regulations are reflected in the contractual obligations of employees. The terms and conditions discuss matters such as confidentiality, legal rights, and responsibilities for complying with the Security Regulatory Framework and handling third-party information. The actions to be taken in the event of non-compliance with security requirements are also detailed.

Likewise, Gestamp informs all employees of the information security responsibilities that are applicable from the moment they are hired until after they have officially left the company.

All Group personnel participate in information security training and awareness activities and are correctly informed of their roles and responsibilities in this area.

7.8. Physical and Environment Security

The Group's facilities, including offices and production plants, at which business operations take place, as well as internal or third-party facilities at which the Group's information systems are located, are suitably protected through the use of perimeter access controls, CCTV, and accident prevention measures, with the aim of preventing security and/or environmental incidents from occurring.

Gestamp has established security measures to protect physical assets, along with procedures for storing, handling, transporting, and destroying sensitive information in both paper and digital format, in order to mitigate the risk of unauthorised access and theft.

7.9. Information Management

Gestamp has security measures in place for all of the phases of the information life cycle, including creation, distribution, handling, storage, and deletion/destruction.

Gestamp has established procedures and time periods for retaining, storing, and destroying information, which are reviewed and updated according to applicable regulations.

Gestamp classifies corporate information in order to simplify access control, custody, and monitoring processes. Preventive measures and controls are established according to the information's assigned classification. The higher the confidentiality level of the information in question, the more restrictive these controls will be.

7.10. Data Privacy

There are special privacy requirements in place for systems and applications that handle sensitive or personal information, in order to prevent this data from being stolen, disclosed, or accessed without proper authorisation.

In regard to outsourcing Gestamp processes that require personal or sensitive data to be accessed or handled, data processing contracts and non-disclosure agreements are established with external service providers in order to ensure that data remains private throughout its life cycle.

To this effect, Gestamp has a Data Protection Policy in place that details the applicable guarantees and principles in this area, along with a set of additional regulations, guidelines, and procedures designed to thoroughly implement the former. Gestamp has adopted technical and organisational measures to ensure the security of personal data and prevent their unauthorized alteration, loss, processing, or access, taking into account the state of technology, the nature of the data stored, and the risks to which they are exposed.

7.11. Cloud Security

Gestamp requests all of the information related to security controls and measures from Cloud service providers and checks that these controls are aligned with the Cloud security standards stipulated by Gestamp.

As a result, Gestamp ensures that Cloud service providers have the necessary mechanisms in place to report security incidents affecting the confidentiality, integrity, and availability of information, in accordance with applicable legislation.

In addition, incident management and business continuity plans cover services that are outsourced to Cloud service providers. The necessary audits are also carried out to ensure the protection of the Cloud environment.

The information stored in private Cloud environments has the same security level as information that is usually stored on infrastructures belonging to the Group.

The information stored in public Cloud environments is assessed in advance by the Tactical Cybersecurity Committee, which defines the specific security measures to be implemented, taking into account a range of techniques for encrypting, anonymising, obfuscating, and tokenising information.

7.12. Third-party Risk Management

Gestamp places special emphasis on assessing the criticality level of services that could be potentially outsourced, which helps to identify those that are relevant from an information security perspective due to their nature, the sensitivity of the data to be processed, or their dependence on business continuity.

Recruitment processes, contractual requirements, service level monitoring, and the security measures implemented by these service providers are all prioritised by Gestamp. In addition, it is mandatory to present evidence demonstrating that the service provider in question complies with current tax and labour regulations. The controls to which these service providers are subject are reviewed on a yearly basis.

Gestamp has formal processes in place for terminating contractual relationships with service providers, which include specific contract clauses to ensure that information is kept private and returned to the company once the service has been delivered.

7.13. Vigilant

Pentesting and vulnerability scanning

Gestamp carries out vulnerability scanning in line with the yearly planning, with the aim of analysing the security of systems and applications and developing remediation plans. The scope, methodology, and coverage of these tests are adjusted according to the risk level of systems and functions, along with the criticality of the assets in question.

Pentesting is carried out with a range of service providers, in order to alter methodologies while ensuring that improvements are monitored to make before and after comparisons. A risk assessment process is carried out during the phase in which the relevant pentests are selected.

Cybersecurity analysis

Gestamp has processes in place for analysing user behaviour in order to detect anomalies and attack patterns. In addition, processes have been defined for detecting potentially harmful, fraudulent activity. These processes generate alerts that are sent to the Incident Response team.

Moreover, Gestamp networks and systems are monitored in order to detect anomalous behaviour.

Security event monitoring

Gestamp boasts an alert management and event logging, correlation, and monitoring service. All critical activity is logged and monitored by security devices.

Log collection and correlation is carried out on a 24/7 basis and is used to support investigations, carry out forensic analyses, and provide evidence of regulatory compliance.

Logs are stored by the system for at least two years so that they can be viewed by the staff that have been authorised by the Group.

In this respect, logs can only be accessed by employees for work-related purposes. In addition, the files that store these logs are protected in order to prevent unauthorised modifications from being made, and backups are created for all logs.

Monitoring of Information and Communications Technology (ICT) devices and resources

Gestamp owns a range of ICT devices and resources that are made available to managers and the rest of the Group's employees. The company also owns the information stored on these components.

These ICT devices and resources and the information they store can only be used by Gestamp managers and employees to carry out work-related duties. This information must never be used for personal/recreational matters or to carry out illegal activities.

Gestamp has the freedom to process, store, monitor, delete, or destroy any data permanently or temporarily stored on ICT devices and resources under the ownership of the Company, while at all times respecting privacy or intellectual/industrial property rights, or any other legitimate interests or rights stipulated in applicable legislation.

7.14. Resilient

Incident management

Gestamp has defined an information security incident response process for correctly managing all threats that could materialise within the Company. This process includes the monitoring, classification, and remediation of incidents.

All incidents that could or have already compromised the confidentiality, integrity, and/or availability of information are logged and analysed so that the relevant corrective/preventive measures can be applied in accordance with Gestamp’s Incident Management Procedure.

All internal and external employees are responsible for reporting any suspicious activity, incidents, or crimes that could compromise the security of information assets belonging to the Group to the Company's security managers.

In addition, a yearly incident simulation plan has been established in order to train and raise awareness among the Group’s employees.

Business continuity management

Gestamp has defined a business continuity plan in order to ensure that essential services can continue to be delivered and any impacts on business are appropriately managed in the event of a crisis. This is achieved by providing a reference framework that defines how to proceed under these circumstances.

This plan does not only discuss information system contingency plans, but also physical dependencies, the individuals that support business operations, and the resources that may be required by these individuals to ensure that Group operations are kept up and running and services can be provided to clients.

The contingency plan is developed and implemented to ensure that critical business processes can be reestablished as soon as possible. It includes controls designed to identify and reduce risks, limit the consequences of incidents, and determine the response time of essential operations. The training assigned to the Crisis Management team, simulation exercises, and regular reviews of the defined response procedures are all fundamental to this plan.

This plan is published and reviewed on a yearly basis or in response to important changes such as the inclusion of new real estate, technology, or organisational assets.

All sensitive, confidential, and personal information is stored in backups, which are managed in line with the security measures defined by Gestamp.

8. Compliance

Gestamp must ensure compliance with this Policy on a yearly basis.

The Management of Gestamp will undertake to encourage and support the implementation of technical, organisational, and control measures that ensure the authenticity, confidentiality, integrity, availability, and auditability of information.

The management of this Policy corresponds to the Cybersecurity Area, which must, therefore, interpret any doubts that may arise in its application, as well as proceed to review it when necessary or required, to propose updating its content. The Group's Internal Audit Management is entitled to carry out as many analyses and checks as it deems appropriate in order to confirm that this Policy is being correctly implemented.

The Audit Committee will oversee compliance with this Policy on a yearly basis and report any findings to the Board of Directors.

Disciplinary actions may be taken in the event of Policy violations. All internal and external employees are responsible for reporting any event or situation that could result in non-compliance with this Policy to the Cybersecurity Area.

9. Exceptions

The Cybersecurity Area must be informed of any exceptions to this Policy so that they can be approved prior to implementation and appropriately logged.

10. References

The present Policy complies with the following international information security standards and regulations:

- ISO/IEC 27001 'Information technology - Security techniques - Information security management systems - Requirements'.
- ISO/IEC 27002 'Information technology - Security techniques - Code of practice for information security controls'.
- General Data Protection Regulation (GDPR).
- Cybersecurity Framework.

11. Approval and review

This Policy has been approved by the Company's Board of Directors and any modifications made to this Policy must be approved by the former upon proposal of the Audit Committee.

This Policy will be reviewed on a yearly basis by the Tactical Cybersecurity Committee in conjunction with the Cybersecurity Area.

Version	Issuing party	Supervising party	Approving party	Entity	Approval date
1.0	Corporate IT	Audit Committee	Board of Directors	GESTAMP AUTOMOCIÓN, S.A.	27 February 2023