Gestamp
TOOLING DIVISION

INFORMATION SECURITY POLICY

Gestamp Tooling Division dedicated to the engineering process, design, manufacturing and setting up of metal stamping dies for the automotive sector is committed to maintaining measures to ensure that the knowledge of product development and technologies of the Gestamp and of our clients are safe within our organization.

To meet the requirements established by our clients, an Information Security Management System has been created, which includes all the requirements of the VDA-ISA Information Security Assessment model, which are based on the ISO 27000 family standards and the good sectoral practices.

Basic Principles of the Gestamp Information Security Policy:

a) Protection and secure use of information assets to enable sharing of information

It is the organization's policy that the information assets are appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

b) Information Security, a strategic goal in our company

Protection and secure use of information assets are priorities in our organization

c) Establishing Risk assessment

To determine the appropriate levels of security measures applied to information systems, a process of risk assessment is carried out for each system to identify the probability and impact of security failures.

d) Security policies and guidelines

- This policy, ISMS procedures shall comply with regulatory and contractual requirements.
- Provide all employees with regular information security training to increase their information security awareness.
- A disaster contingency plan has been developed.
- Employees must comply with the policies and procedures of the ISMS. An employee who violates any of these regulations shall be involved in disciplinary process in accordance with the employee rules and regulations.

e) Responsabilities

- It is responsibility of the Tooling Division Director to manage and regularly review this policy.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments
- It is a duty of any staff member to immediately report any information incident

f) Documented system

This Security Policy is supported by more detailed procedures and subsidiary policies that develop and assist in its implementation.

Alatz Aurtenetxe
Gestamp Tooling Division Director