



Security Policy of the Information Systems of the Acerinox Group

Classification of the Information:

| | |
|-------------------------------|-----------------------|
| Document Level | General Documentation |
| File Name | SecurityPolicy.docx |
| Type | PUBLIC |
| Scope of Dissemination | PUBLIC |
| Responsible | IT Manager |

**Documentación general****Security Policy of the Information Systems of the Acerinox Group**

Versión: 2.0

Fecha: 16/12/2019

Página 2 de 7

AMENDMENTS CONTROL

| Description | Version | Date |
|---|---------|------------|
| Document's preliminary version. | 1.0 | 05/11/2018 |
| Auditory requirement included: review periodicity.. | 2.0 | 16/12/2019 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

The paper copies of this document will be solely and exclusively INFORMATIVE. For the purposes of compliance with procedures, the only valid reference will be the document in electronic format available in the repository intended for that purpose.



INDEX OF CONTENT

| | |
|---|---|
| INTRODUCTION | 4 |
| SCOPE | 4 |
| Employees | 4 |
| Information Systems | 4 |
| Third Parties | 4 |
| APPROVAL, MAINTENANCE AND POLICY REVIEW | 5 |
| POLICY DISTRIBUTION | 5 |
| PENALTIES | 5 |
| INFORMATION SYSTEMS SECURITY POLICY | 5 |



1. INTRODUCTION

This document shows the principles where Acerinox Group Security Policy is held. These sets of fundamental principles have been formulated based on valid business needs, added value acknowledgment of those systems to be protected and understanding those risks related to these systems.

2. SCOPE

2.1. Employees

Information Systems Security is a collective effort. It requires the involvement and participation of all organization members working with the Information Systems Department / Management. For this reason, every employee should meet the Security Policy requirements and its associated documentation. Those employees, who intentionally or by negligence do not comply with the Security Policy, may be subject to disciplinary actions as appropriate.


2.2. Information Systems

This Policy concerns all Information assets of the company, both personal equipment or servers, nets, applications, Operating Systems, company processes which belong and/or are managed by Acerinox Group.

This policy meets those aspects more directly related to responsibility and proper use by the staff.

2.3. Third Parties

The current Security Policy is of extensive acknowledgment and compliance for any external person belonging to third entities that perform any type of work hired by Acerinox Group and those third supplier companies hired for the execution of professional services in the appropriated fields, in the case of performing any activity involving access or processing to any system or information owned by Acerinox Group and so will be contractually defined.

| | | | |
|---|--|-------------------|---------------|
|  | Documentación general | | |
| | Security Policy of the Information Systems of the Acerinox Group | | |
| | Versión: 2.0 | Fecha: 16/12/2019 | Página 5 de 7 |

3. APPROVAL, MAINTENANCE AND POLICY REVIEW

Acerinox Group Management is responsible for the approval of Information Security Policy.

The person responsible for the Information Security should build, maintain and publish the Information Security Policy.

Any change or development which affect or may affect the Information Security Policy will be recorded in a new signature of the approval document.

A maximum periodicity of two years is established for the review of the validity and reasonableness of this policy, in which the improvements, adaptations or modifications required will be carried out depending on the applicable organizational, technical or regulatory changes.

4. POLICY DISTRIBUTION

The distribution of this document, Policy of Information Security, and its disseminations will be made according to the existing measures and depending on the receiver.

5. PENALTIES


Any intentional, culpable or negligent infringement of security policies and rules and which implies a potential harm, accomplished or not to Acerinox Group, will be sanctioned in accordance with the provisions of the management of the ACERINOX GROUP and the applicable collective agreements.

Any actions which may negatively affect Acerinox Group's Security and which are not provided in this policy should be reviewed both by the Management and Information System Security Responsible and Governing Bodies according applicable law.

Those disciplinary actions in response to non-compliance of Information System Security Policy are Acerinox Group Management's responsibility and the rest of the governing bodies according to applicable law.

6. INFORMATION SYSTEMS SECURITY POLICY

In response to the new technological environment where convergence of informatics and communications are providing a new paradigm of productivity for the companies, Acerinox

| | | | |
|---|--|-------------------|---------------|
|  | Documentación general | | |
| | Security Policy of the Information Systems of the Acerinox Group | | |
| | Versión: 2.0 | Fecha: 16/12/2019 | Página 6 de 7 |


Group is highly committed to maintain a competitive service providing a responsible business model based on permanent search of economic, social and environmental balance where best practices development in Information Security is essential to achieve the confidentiality, integrity availability goals and legacy of all information managed.

As a result of the above, Acerinox Group defines the following application principles to be considered in the Information Security Frame:

- **Confidentiality:** The information managed by Acerinox Group will be exclusively known by authorized persons, prior identification, at the time and by the enable means.
- **Integrity:** The information processed by Acerinox Group will be complete, exact and valid, being its content provided by those individuals affected without any type of manipulation.
- **Availability:** The information processed by Acerinox Group will be available and usable by authorized users and identified at any time, being guaranteed its own persistence before any foreseen contingency.
- **Legality:** Acerinox Group will guarantee the compliance of all applicable existing legislation or contractual requirement which may be applicable. And specifically, those regulations in force concerning data processing of personal nature.

Acerinox Group, for the proper development of its business functions is based and makes use of the different types of data processing and information supported by those systems, programs, communication infrastructures, files, databases, computer files, etc., being one of main assets of Acerinox Group, therefore, their damage or loss impact on its services development and may endangering the organization's continuity. To prevent that, it has been designed an Information Security Policy whose main goals are:

- **Guarantee** the proper functioning of all assets related to information security.
- **Protect** assets against those threats which may lead to security incidents.
- **Relieve** those effects of security incidents.
- **Establish** a classification system for information and data to protect critical assets.
- **Develop** a set of **rules, standards and procedures** applicable to employees, partners, external services suppliers, etc.

| | | | |
|---|--|-------------------|---------------|
|  | Documentación general | | |
| | Security Policy of the Information Systems of the Acerinox Group | | |
| | Versión: 2.0 | Fecha: 16/12/2019 | Página 7 de 7 |

- **Properly request the necessary training actions to user concerning security management.**
- **Observe and comply with the current legislation** in terms of data protection, intellectual property, labour, information company's services, criminal, etc., which affects Acerinox Group's assets.
- **Protect the Organization's intellectual capital**, so that it not spread or being illegally used.
- **Reduce** the possibilities of unavailability by properly use of organization assets.
- **Defend** the assets before internal or external attacks so that they do not turn into security incidents.
- **Control the security measures functioning**, finding out the number in incidences, their nature and effects.

Acerinox Group Management assumes the responsibility to support and promote the establishment of those organizational, technical and control measures for the accomplishment of the current Information Security Policy and providing those necessary resources to solve, as quickly and effectively as possible, those nonconformities and information security incidents which may arise, and setting up those necessary measures so that they do not happen again.

This Policy will be maintained, updated and adequate to organization ends, lining up with the context of the organization risk management. For that purpose, it will be reviewed at planes intervals or whenever there are significant changes, to ensure its suitability, adequacy and efficiency.

All policies and procedures included in the security policy will be approved and promoted by Acerinox Group Management.

APROVED BY:

Name:

Signature:



Date: 16/12/2019