

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

The goal of information security is to protect the informational assets of **MONSSON OPERATION SRL**, of customers and partners, to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents. The information security policy is approved by the management and reflects the commitment of **MONSSON OPERATION SRL** management to implement and maintain an Information Security Management System, through which we can protect the informational assets of the organization from all threats, whether internal or external, deliberate or accidental.

Through compliance with **ISO IEC 27001: 2006**, we make sure that:

- Information will be protected against unauthorized access;
- Confidentiality will be maintained;
- Information integrity will be preserved;
- Availability of information will be provided when business processes require;
- Requirements of applicable laws and regulations are met;
- Business Continuity Plans will be drawn up, maintained and tested;
- All staff will be trained in information security;
- All security incidents, real or suspected, will be reported to and investigated by the Information Security Manager.

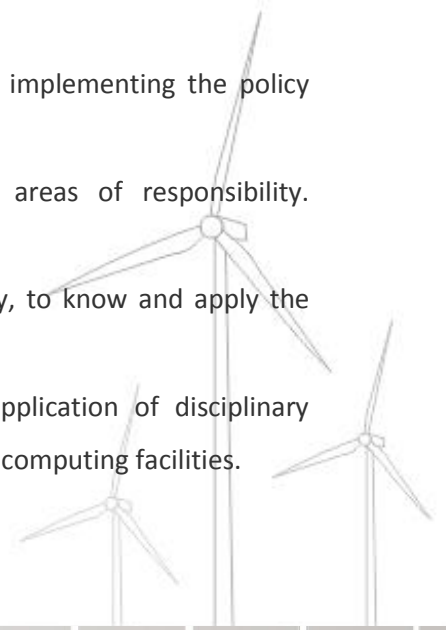
In order to apply the policy, information security procedures have been implemented. Business requirements regarding the availability of information and informational systems will be met.

Information Security Management Representative is directly involved in implementing the policy regarding support and guidance delivery for its implementation.

All managers are responsible for implementing the policy in their areas of responsibility.

It is every organization employee's responsibility to adhere to this Policy, to know and apply the procedures from the Information Security Management Manual.

Failure in respecting the Information Security Policy will entail the application of disciplinary measures (for employees) and recalling of access rights to information and computing facilities.



In some cases, alteration, disclosure or destruction of company's informational assets will lead to legal actions (civil or penal) against natural or legal persons responsible for security incidents.

As a legal representative, I engage to ensure the continuous improvement of the Information Security Management System, to provide the necessary resources to achieve the set goals and to apply the information security policy. The appointed Management Representative for Information Security has the necessary authority to manage the Information Security Management System; this representative provides support and guidance for its implementation within the organization.

CEO

Ana – Mihaiela Aldea



30.01.2018

