

INFORMATION SECURITY POLICY

AIGO BS Ltd. Belgrade has an approach to information security based on an inviolable information flow and the protection of information and material assets from all possible external and internal threats, be they accidental or deliberate, using an established information security system in accordance with the requirements of the international ISO/IEC 27001:2013 standard in order to ensure continuous fulfillment of this approach.

It is the responsibility of top management and all other employees to perform their business activities in the area of trading in computers, printers, printer supplies, office supplies, computer, printer and photocopier servicing, data processing and variable data printing, wholesale – import, export, procurement, storage and medical equipment distribution, as well as daily expert consulting and operational communication, and to preserve the integrity, confidentiality and availability of all material and electronic information assets of the company. This kind of obligation is a prerequisite for profitability, compliance with legal, regulatory and contractual requirements, achieving competitive advantage and a successfully sustained corporate identity of the company

The implemented international ISO 27001 standard provides consistent frameworks for constant improvement of information security. The primary principles that the company adheres to, listed in the defined frameworks for attaining a sustainable improvement of information security include:

- ❖ meeting the requirements of clients and other stakeholders in the domain of information security;
- ❖ meeting the set goals pertaining to the company's information security;
- ❖ protecting all information assets from unauthorized access;
- ❖ controlled protection of the integration of documents and information by creating backup copies;
- ❖ regular updates to software packages, antivirus programs and user access;
- ❖ controlled access to the secured video surveillance system;
- ❖ educating employees and raising their awareness of the importance of information security;
- ❖ detailed investigation and analysis of security information incidents;
- ❖ continuous alignment with regulations, laws, contractual obligations and stakeholders' expectations;
- ❖ abiding by the rules of confidentiality, personal data protection, as well as copyright and licensed rights;
- ❖ regular assessment of the information security management system based on the designated employees' adequate reporting;

In order to implement the formulated Information Security Policy, we expect full support and maximum commitment from all employees.

In Belgrade, 05.02.2020.



Director

