Croonus Technologies Ltd., Čačak

30 Kralja Petra Prvog St., Čačak, Serbia
Landline: +381 32 51 22 052
Phone: +381 66 25 24 23
VAT number: 111285459
ID number: 21455440
www.croonus.com

INFORMATION SECURITY POLICY

The data security policy's goal is to indicate in a clear and unambiguous manner the commitment of the company **Croonus Technologies Ltd., Čačak** to continually conduct and improve its operations in accordance with the **ISO/IEC 27001:2013** standard (Information Security Management Systems – ISMS), preserving the principle of maintaining confidentiality, availability, and integrity of information and information resources, thus securing and guaranteeing

- the protection of information and other information resources (people, processes, procedures, hardware, software, infrastructure, equipment...), from all internal and external, intentional or accidental threats (computer frauds, espionage, hacker attacks, viruses, floods, fires, earthquakes, etc.), through establishing, implementing, tracking, reevaluating, maintaining, and improving the ISMS;
- a continuity of business operations;;
- minimizing potential business damage by preventing security incidents, that is, decreasing their impact to the bare minimum;;

thus improving its corporate image, profitability, and competitive advantage.
The abovelisted is secured (implemented) through:

- The **Croonus Technologies Ltd., Čačak** founders' leadership stance toward engaging all employees, at all levels, in achieving company goals which, in total, result in a high level of security of information;
- Compatibility with strategic business plans and goals, relevant legal, regulatory and contract demands, as well as the ISO/IEC 27001:2013 standard;
    - A culture of safety and the employees' awareness regarding their role and responsibilities;
    - Acknowledging the interests of business partners, internal and external users, and other interested parties;
- Prevention of unauthorized access to information resources;
    - Maintaining and improving the security system for employees, clients, information, and property;
    - A clear organization and division of responsibility in terms of information safety;
- Risk management with the goal of decreasing security threats;
    - Crisis management;
    - Continued reevaluation and improvements..

All employees, consultants, external consultants, temporary employees, contractors, and subcontractors, as well as third parties with whom **Croonus Technologies Ltd., Čačak** does business with, need to be aware of their duties and responsibilities, defined within their job or contract description, and to act in accordance with this Policy.

They are responsible for maintaining confidentiality, availability, and the integrity of information and other information resources of **Croonus Technologies Ltd., Čačak** during all phases of their life cycle, as well as not to breach their security through their actions.

The founders of **Croonus Technologies Ltd., Čačak** are responsible for the application of the information security policy within their business processes, as well as its application on behalf of the employees.

Failing to adhere to the Information Security Policy entails disciplinary liability.

The founders of **Croonus Technologies Ltd., Čačak** ensure that this policy is understandable and conveyed to all interested parties, implemented and maintained at all levels within the company and revised at least one a year, in order to be correspond to any sort of changes regarding risk evaluation or the risk management plan.

This Policy was approved on part of the director of **Croonus Technologies Ltd., Čačak** and it provides a framework for setting of further relevant goals of the company and the basic principles for establishing an efficient information security management system (ISMS).

Čačak, March 11th 2022

Stefan Ćebić, Director