SECURITY INFORMATION AND PRIVACY, IT SERVICES AND BUSINESS CONTINUITY MANAGEMENT POLICY

The application of security information and privacy, IT services and business continuity management policy aims to controlled and secure access to documents, information and premises, both for employees and users of services and products of the company Saga d.o.o. Beograd (hereinafter Saga). The subject and area of application refers to the field of work related to design and execution of works of telecommunication networks and systems, products and services based on information technologies in the field of infrastructure, technological services and solutions. The purpose of the policy is to protect information as a valuable asset of the company from all internal, external, accidental or intentional threats and to indicate the possibilities of the process for controlling organizational activities and resources with the aim of improving and increasing the value of the service, as well as to enable the functioning of the company in predefined capacities during a possible disruption due to a disaster.

Security of information is one of the basic values of the organization, bearing in mind that the security of information and privacy, as well as preservation the basic security principles of confidentiality, integrity and availability are critical to the organization's operations and are directly correlated with the strategy of the company. The organizational approach in the management of security of information objectives is realized by Saga in compliance with current regulations and laws, stakeholder requirements, current and projected environmental threats for security of information and privacy. Each data generated on Saga's information systems is considered the property of Saga company.

By establishing, implementing and enforcing, monitoring and reviewing, maintaining and continuously improving the management system, we strive to improve the quality of services, increase the satisfaction of interested parties, reduce costs, use the resources better, increase awareness of the nature of importance and significance of maintaining security of information, managing the risks of deteriorating the quality of IT services and compromising security of information by detecting vulnerabilities and dangers and taking measures to reduce risk levels.

The top management of Saga company is aware of its responsibility to ensure the high quality in all business segments and this is manifested through the establishment of service management system and security of information and privacy management system in order to maintain the quality of support level for business goals and processes, as well as through assigning responsibilities through clearly defined roles. The security of information and privacy, IT services and business continuity policy is compliant with the regulations and requirements of the series of ISO 20000-1, ISO 27001 and ISO 27701, but also serves as a response measure in case of emergencies, including disasters in accordance with the requirements of ISO 22301. All principles of information security apply to the security and protection of personal data, which are a subset of information security. The top management is focused on the well-being of each individual in the overall business, where the personal safety of employees is the highest priority. Saga is also aware that the protection of personal data is one of the fundamental human rights and takes all measures to ensure that all its employees take the data privacy seriously.

With this Policy, the organization expresses its readiness and obligation to maintain continuous improvement of the management system by finding improvements in processes and products in order to increase quality and reduce losses, with defined goals through:

- providing a secure environment for achieving business goals,
- minimizing risks in terms of information security and privacy, as well as business continuity,
- improvement of the portfolio of security and other services,
- maintaining the reputation of Saga company and its leadership position in the field of information security.

The success of the entire management system of IT services and security of information is achieved by implementing the adopted principles for handling all activities related to security of information and privacy of the organization, through the established scope and implemented controls of defined sub-policies in accordance with applicable laws and regulations. Regular training and motivating employees to perform quality work in the field of IT services, security of information and privacy, as well as and business continuity, aims to raise awareness and encourage employees to act preventively, change their habits and get involved in the organization's efforts to improve its performance. In order to conduct permanent informing on the basics of security, as well as informing on emergencies, a Log'on policy has been established with the aim of informing employees in a timely manner about their basic responsibilities and obligations.

The business continuity management framework clearly defines procedures and designates emergency teams, as well as responsibilities for the activities outlined in the plans. The activities of the business continuity management framework oblige to create a Business Continuity Plan and a Disaster Recovery Plan. Incident response involves taking action by the authorities in a way that demonstrates responsible command and control in times of crisis.

Business continuity planning procedures, as well as disaster recovery activities, are based on the performed business impact analysis, with special emphasis on:

- Identifying critical business processes, resources and services;
- Assessment of all identified risks, determination of acceptable level of risk and planned risk treatment;
- Creating and maintaining backups and synchronization of data between the primary and backup center in the manner specified in the Disaster Recovery Plan;
- Adopting detailed Recovery Plans and determining responsibility for their implementation;
- Compliance with legal requirements, contractual obligations and expectations of all stakeholders;
- Intensive communication with all stakeholders.

The business continuity management framework of Saga organization clearly defines the procedures and teams, ie responsibilities in case of crisis situations based on defined Recovery Plans. Response to disruptions and disasters involves taking actions in a way that demonstrates responsible command and control in times of crisis.

The organization conducts trainings in order to ensure that all employees are aware of their roles and responsibilities in case of emergencies. The organization undertakes review and, where planned, a testing of plans and supporting documents at least once a year and harmonizes them with any changes in business, technology, environment or changes that need to be implemented in accordance with test results, as well as after any adverse event or major changes, in order to improve and maintain the relevance and integrity of business continuity management framework.

The organization is committed to continuous improvement of the business continuity process in accordance with the established integrated procedures of continuous improvement with other management systems. The policy completely supports the vision of the organization as a responsible IT company. Saga undertakes to respect the stated security and organizational principles, both within it and when providing IT services to external users.

This policy is accepted by the top management and is binding on all employees in the organization, as well as all engaged subcontractors and project consultants who are responsible for its implementation. The policy is applied integrated with the Quality Management System Policy, as well as other policies in the organization.

Director,