GOVERNANCE POLICY

The management of Information Services JSC, represented by the Board of Directors and through the CEO, officially declares its **GOVERNANCE POLICY**, which is communicated and maintained to ensure it is understood and implemented at all levels of the company.

The Governance policy is aimed at offering high-tech solutions in the field of system integration, including the provision of supplies and services in the field of cybersecurity, the development and maintenance of national databases and electronic registries, software products, and authentication services, assembling and maintaining hardware systems, providing consultations in the field of hardware, software, and information technology that meet the requirements of our clients and partners under the most mutually beneficial terms and with the aim of safeguarding the security of information - both for clients and partners as well as for the company - in accordance with Bulgarian law.

As a National System Integrator and designated as the national operational centre for cybersecurity of the information environment, Information Services works toward building an information society in Bulgaria by providing the government, citizens, and businesses with the ability to acquire, use, protect, store, and disseminate in the most effective manner the information necessary for the normal conduct of administrative, civil, and business activities and services.

This Policy aims to ensure compliance with requirements for quality, information security, the provision of IT services, and anti-bribery, in accordance with the international standards ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 20000-1:2018, and ISO 37001:2025, and to ensure that all business conduct is honest and transparent, reasonably prudent, and that careful business judgment has been exercised in all actions.

Management demonstrates leadership and commitment by promoting and maintaining a culture of compliance and integrity and zero tolerance for bribery as a key factor in the effectiveness of the anti-bribery system.

For the effective implementation of the Governance policy, management establishes the following **key quality management objectives**:

- To maintain its leading position as a company in the field of delivery, installation, and maintenance of information systems of national importance, through technical and software solutions, development of application software, and staff training, in compliance with the effective regulatory requirements.
- To contribute, in its capacity as a National System Integrator, to the development of an information society in Bulgaria.
- To maintain a consistent level of quality (including timely delivery) of:
  - developed application software, in accordance with customer requirements
  - software and hardware installation and maintenance;
  - comprehensive IT services;
  - the local and remote networks under construction;

  - training of IT specialists;
  - subscription and post-warranty service for computer and communication equipment and peripheral devices;
  - management of information system projects of national significance;
  - consulting services in the field of software and information technology;
  - development and maintenance of information and communication security systems.
- Effective use of material, human, and financial resources in accordance with the needs of customers and stakeholders.
- Continuous improvement of core company processes through the maintenance and implementation of modern technological solutions in the fields of computer hardware, software products, and communications.
- Enhancing staff qualifications and motivation for effective work, and fostering an internal mindset focused on consistent and measurable results.

To implement this Governance policy, management has established the following key **objectives for information security management:**

- To ensure the confidentiality, integrity, and full access to all physical and electronic information assets, both of the company and of customers and stakeholders, provided to Information Services in the course of fulfilling contractual obligations, through the implementation and maintenance of adequate organizational and technical measures for their protection based on risk analysis;
- To establish and apply clearly defined and documented risk assessment criteria that comply with the requirements of the international standards ISO/IEC 27001:2022, ISO/IEC 27701:2019, EN 31010:2019, ISO 31000:2018, as well as applicable regulatory and contractual obligations and the company's strategic interests.
- To periodically review and update information security measures following an objective and competent systematic assessment and reassessment of their effectiveness;
- To identify emerging threats to information assets and to promptly implement adequate protection mechanisms and controls;
- To plan and take appropriate actions to ensure business continuity by maintaining and testing up-to-date contingency plans;
- To conduct adequate verification and investigation of identified and suspected breaches of the company's information security.

The Governance policy provides a framework for defining, reviewing, and achieving the key **objectives, principles, and requirements for personal data protection:**

- Ensuring the lawful personal data processing;
- Defining roles, responsibilities, and principles for personal data processing;
- Ensuring the protection of the rights and freedoms of data subjects;
- Reducing the risk of personal data security breaches;
- Personal data shall only be processed for specific, clearly defined, and lawful purposes, including: fulfilment of contractual obligations, compliance with legal and regulatory requirements, human

resources management, customer and supplier administration, information and physical security, and marketing activities (where there is an applicable legal basis).

The management of Information Services defines information security management as a mechanism to ensure the proper functioning and continuity of processes, enhance the company's competitiveness, and protect business interests by preventing or minimizing the impact of potential incidents related to information security.

The scope of this Policy includes information owned by the company and its customers in any form or format, whether on paper, digital, video, or audio media; the company's information systems that process and store data, the communication systems that transmit data, and all services provided by Information Services.

The management of Information Services strives to enhance employees' qualifications regarding information security. The management is committed to supporting each team member understand their responsibility and contribution to ensuring information security by providing appropriate general and role-specific training in accordance with their position and responsibilities.

The management of Information Services aims to demonstrate its capabilities in managing the service lifecycle, including planning, design, transition, delivery, and improvement, and to this end defines key **objectives for IT service management:**

- The IT services provided by the company should stand out from those of competing companies;
- Service delivery should follow the latest and best practices in IT service management;
- Effective management, measurement, and improvement of service management processes;
- Ensuring transparency of IT services to customers;
- Increase the satisfaction of internal and external customers with the services used;
- Expanding sales opportunities by achieving compliance with ISO/IEC 20000-1:2018, as a business requirement.

This Governance policy provides a framework for defining, reviewing, and achieving the key **management objectives for anti-bribery**:

- Meeting the requirements of ISO 37001:2025 and applicable legal and other obligations (national and international) related to anti-bribery;
- Establishing and maintaining a professional culture of integrity, transparency, openness, and compliance with applicable requirements, including through clear rules of conduct, training, and communication;
- Zero tolerance for bribery and any form of unethical business conduct, including in relationships with third parties and business partners;
- Management of conflicts of interest through rules for disclosure, assessment, and taking action (including recusal from decision-making) where applicable;
- Risk-based due diligence for business partners, subcontractors, and other relevant third parties, proportionate to the identified risk of bribery and in the event of significant changes in relationships / scope of activities;

- Channels for reporting/whistleblowing on suspicions or violations, ensuring the possibility of confidentiality (where applicable) and protection against retaliation for individuals who report in good faith, in accordance with internal rules;
- Establishment and maintenance of an anti-bribery function with clearly defined responsibilities, authority, and the necessary independence to support, monitor, and report on the effectiveness of the system;
- Periodic assessment and update of the risk of bribery, including an assessment of whether climate change is a relevant issue in the context of the organization and regarding the risk of bribery/vulnerabilities in the supply chain and relationships with third parties (where applicable);
- Building public trust and strengthening business relationships while enhancing the organization's reputation through consistent policy implementation and effective controls.

A unified Financial Management and Control System has been established at Information Services, comprising a set of policies, procedures, internal rules, and instructions systematized in accordance with management accountability and the elements of financial management and control in the public sector. In accordance with the regulatory requirements, the following have been adopted: Rules for Performing Preliminary Control and Implementing a Dual-Signature System, Rules for Managing and Assigning System Integration Activities at Information Services JSC, Internal Rules for the Management of the Public Procurement Cycle at Information Services JSC, Rules for Conducting Tenders and Competitions, and for Concluding Lease Contracts with Workers and Employees of Information Services JSC, Rules for the Selection of a Registered Auditor to Perform an Independent Financial Audit and Certify the Annual Financial Report of Information Services JSC and Rules for the Selection of a Contractor to Provide Financial Services by Credit or Financial Institutions to Information Services JSC, Internal Rules for the Receipt, Registration, and Review of Reports of Violations Addressed to Information Services JSC, Code of Ethics, and other in-house acts.

Strict compliance with the established rules and procedures, as well as the preliminary and subsequent control of actions and decisions, ensure the high-level functioning of processes designed to support management in the performance of its functions and powers.

The Financial Management and Control System at Information Services is updated in a timely manner in response to various factors affecting current operations - changes in the regulatory framework governing commercial relations, company ownership, relations with tax, social security, supervisory, and statistical authorities, employment relations, occupational health and safety, fire and emergency safety, cybersecurity, and others, as well as factors related to the relevance of climate change to operations and the risk of bribery.

This Policy applies to all employees of Information Services JSC, as well as to any person associated with the company who provides services on its behalf and for its account, including subcontractors, their personnel, and business partners.

It is the responsibility of Information Services employees to ensure the effective functioning of the management systems implemented in the company through the strict application of the Governance policy.

This Governance policy is communicated at all levels within the company and is available to all stakeholders on the Information Services website.

Failure to comply with the Governance policy and applicable regulations by company employees will be considered a disciplinary violation, and when committed by third parties, it shall constitute grounds for termination of employment, commercial, and other types of relationships.

Information Services conducts a careful assessment of the ethical conduct and reliability of each employee or business partner and will take serious measures against those who violate the Governance policy.

The Governance policy and governance objectives are subject to annual review and, if necessary, update.

The management of Information Services has established the necessary conditions, provides the necessary resources, and exercises control to ensure strict compliance with the requirements of the implemented management systems, which comply with the international standards ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 20000-1:2018, ISO 37001:2025, and the applicable regulations, and is committed to direct participation and responsibility for the implementation of the announced **GOVERNANCE POLICY,** ensuring the company's prosperity.

IVAYLO FILIPOV
CHIEF EXECUTIVE OFFICER
INFORMATION SERVICES JSC