The Leadership of Telepoint LTD officially declares its **MANAGEMENT POLICY**, which is announced and maintained in order to be understood and applied at all levels of the organization.

The management policy is aimed at developing, implementing and maintaining services, which comply fully with the requirements of the organization's clients and partners and bringing long-term satisfaction to all stakeholders.

TELEPOINT operates Carrier Neutral Data Centers for colocation, ensuring high level of service quality, informational security and guaranteeing business continuity. The colocation we offer provides the clients with the possibility of eliminating the investments and lowering their operational expenses for up keeping a data center for their own equipment.

The fully redundant data center systems, the business continuity management and the implemented systems for quality management and information security allow the company to provide 99.999% continuity of service.

As a company we implement special measures that ensure the on-going legal conformity and the execution of the applicable requirements of the international standards, legislative directives and regulations.

By placing our focus on our clients, we are intolerant to any risks. Therefore, we manage over 97% of all identified risks, while having taken the necessary measures for protection, access control and confidentiality.

For the effective implementation of the Management policy, the Leadership defines the following main

QUALITY CONTROL GOALS:

- Constant improvement of the quality control management system and increasing the quality of our colocation services in regards to the span of the defined context of the company;
- Reaching the strategic quality aims that define the main framework of the concrete measurable quality targets;
- Full satisfaction of the needs and expectations of the clients and the stakeholders;
- Reaching a high level of competitiveness for "Telepoint" LTD, by providing innovative and accessible solutions to the clients;
- Maintaining all applicable to the company Bulgarian laws, normative acts and international standards, as well as the agreed upon obligations towards the clients;
- Recruitment, training and development of the human resources with the aim of achieving the best possible results.

BUSINESS CONTINUITY MANAGEMENT GOALS:

- Improving the infrastructure's continuity and the systems and processes, which are responsible for providing the services, which fall within the scope of the Integrated Management System;
- Constant improvement of the Business Continuity Management System, part of IMS;
- Periodic (no less than once per year) business impact analysis and risk assessment;
- Ensuring the necessary resources for achieving service continuity;
- Development, implementation and maintenance of plans for service continuity that are based on the conducted business impact analysis, identified risks and strategic targets of the company;
- Appropriate personnel training that is linked to the process of ensuring the continuity of service.

INFORMATION SECURITY MANAGEMENT GOALS:

In order to be able to protect the clients' sensitive information we offer many types of physical protection and access control, part of which are 24/7 on-site personnel, armed security officers and constant video surveillance of all areas. Every person, which is employed by Telepoint has been recruited after a strict HR research process through a severe competition. We constantly develop our employees' professionalism, moral values and work ethics with modern trainings under on-going control.

- Ensuring the necessary resources for implementing and maintaining an effective informational safety management system;
- Guaranteeing the confidentiality, integrity and availability of the information – by implementing pre-approved administrative and technical controls (safeguards);
- The identifying of the risks for the informational assets and the implementation of measures with which to mitigate the risk of threat realization.
- Development and maintaining a methodology for risk assessment that includes quantitative and qualitative assessment methods;
- Development and integration of a security awareness program, which would serve to inform the employees about their responsibility in regards to information security;
- Developing, integrating and maintaining a system for monitoring, which would identify and record incidents related to information security in regards to the effective incident management of those assets;
- Applying special measures, which ensure the constant legal conformity and application of the international standards' requirements, as well as the legal directives, norms and regulations.

Payment Card Industry Data Security Standard (PCI DSS) Compliance:

In constant aspiration for improving the internal operational processes and adding value for its clients, Telepoint LTD has developed and maintains a policy regarding the information security for bank cards operations and cardholders' data – PCIS DSS.

The standard contains 12 sections, which cover all processes connected to the storage, dissemination and operations with card/cardholder data. As a colocation services supplier, Telepoint complies with section 9 and section 12 from the last version of the standard – 3.2.

The main accents in the strategy of the information security management for operations with bank cards and cardholders' data are:

- Existence of documented policies and processes, which include all aspects of the safekeeping of the information security;
- The company's employees undergo specially designed recruitment process and interviews, which comply with the requirements of PCI DSS;
- All employees undergo initial and periodic briefings and trainings in regard to informational security;
- A procedure for managing the information security has been developed. Rights and responsibilities for managing and maintaining the system have been delegated to specific individuals. The results from the management and development of the informational security system are being tracked and assessed periodically;
- A compulsory information assets risk assessment for the organization is being conducted, including in itself the clients' equipment, which is also defined as an information asset. Plans for mitigating and counteracting the risk have been developed and applied.
- Plans for business continuity have been developed, which are being role-played periodically by employees and their performance is being assessed.
- Special procedures for incident management in relation to informational security have been created and are acted upon.
- The relevance and applicability of the informational security strategy is being inspected and assessed periodically, in order for it to be fully compliant with the latest requirements of the PCI DSS standard.
- A shared responsibility matrix is available on demand, containing detailed information regarding the exact articles of the standard, which Telepoint complies with.

The Leadership holds the responsibility to exact from all employees of "Telepoint" LTD to be well informed with the requirements of the documents for the Quality control system, the informational security control

system and the business continuity management system as part of the integrated system for management and to control their application.

The present policy will be revised annually by the Leadership in order to achieve full applicability.

Date: 07.01.2021

General Manager:

/A. Zlatev/