INFORMATION SECURITY MANAGEMENT POLICY

TELEPOINT is carrier neutral colocation Center, providing a high level of information security. The customers benefit from the infrastructure, thereby reducing operational costs and eliminating the investment expenditures for colocatin facility to host their equipment.

The redundancy of the datacenter, the quality control and the information security systems alow for 99.999% availability of the services.

To be able to protect sensitive information of our customers, we apply a number of means of physical protection and access control, which include 24/7 duty engineers, armed guards and constant surveillance of all areas. All personnel within Telepoint were selected after a very thorough investigation in a major competition (1:1000), constantly developing their professionalism, ethical values and work habits with advanced training under constant control.

Telepoint applies constant measures to ensure continued compliance and enforcement of applicable international standards, directives and legal requirements.

Being customer-centric company, we are intolerant to risk. We manage over 95% of all identified risks and we have taken the necessary precautions, ensuring availability, integrity and confidentiality.

Payment Card Industry Data Security Standard (PCI DSS) Compliance

In constant strive of improving internal processes and adding value to its clients Telepint Ltd. has developed and maintains policy regarding the security of the information and customer`s data regarding the bank cards payments - PCI DSS.

The standard consists of 12 chapters covering all processes related to the storage and distribution of card (and cardholeder`s) data. As a provider of collocation services, Telepoint is certified under section 9 and section 12 of the latest version of the standard - 3.2.

The main highlights of the strategy for managing information security when paying with bank cards are:

- Documented policies and processes that include all aspects of information security protection;
- Employees in the company undergo a specially designed selection process and interviews that comply with PCI DSS requirements;

- All employees undergo initial and periodic training related to information security;
- An information security management procedure has been developed. The rights and responsibilities for managing and maintaining the system are delegated to specific people. The results of the management and development of the information security system are monitored and evaluated periodically;
- Mandatory risk assessment of the organization's information assets is conducted. Customers` equipment, is also considered an information asset. Risk mitigation plans have been developed and implemented;
- Business continuity plans are developed and all personnel undergo trainings and assessment of their performance.
- Special procedures for handling information security incidents have been established and followed;
- The timeliness and applicability of the information security strategy is reviewed and evaluated periodically to make it consistent with the latest PCI DSS requirements.
- Shared responsibility matrix is available upon request. In this matrix all responsibilities of Telepoint as a service provider have been described in details.

Successful audit review of compatibility means that the data (whether cardholder`s or other) is secure in Teleponet so that you, our partners, can concentrate on that part of the business processes that has the most value for you!

Date: 07.2019

General Manager**:**

/A. Zlatev/