Information Security and Privacy Policy
CETIN Bulgaria

	Position	Name	Signature
Approver	CEO	Petar Mudrinic	
Policy Manager	Security Director	Dimitar Korudzhiyski	
Policy Manager	Legal and Regulatory Director	Yoanna Ilchovska	

CETIN Bulgaria EAD is a technological company which offers a wide range of wholesale services such as: telecommunication infrastructure ensuring mobile and fixed voice and data, internet connectivity, etc. We at CETIN build and maintain the crucial technological infrastructure, which allows our clients to offer new services and products via innovative technologies, stimulating development, change and improvement. Therefore, information security and privacy are among the top priorities for the company.

The main objective of management of the information security and privacy, according to ISO 27001 and ISO27701, is to ensure the risk identification and management, the integrity and confidentiality of all assets and information of the company and of the clients, including personal data and to ensure business continuity and compliance with legal requirements for personal data protection.

The top management ensures that:

- Context of the organization is defined and all external and internal issues concerning the management of information security and privacy resolved;
- Any changes in the context of the organization and all external and internal issues are taken into account;
- Information security and privacy risks are identified and controlled;
- Integrity of information is maintained;
- Availability of information on all processes is maintained;
- Information is protected from unauthorized access;
- Confidentiality of information is assured;
- Criteria for assessing the risks are defined as the level of acceptable risk to which assesses the likelihood of threats and the severity of their impact on the company's assets and on the personal data subject;
- The legal requirements and internal requirements of the company are implemented;
- Procedures and policies for implementation of the information security and privacy policy are developed;
- Needed resources for the information security and privacy management system are available
- Training for all employees for management of the information security and privacy is provided;
- Information security and privacy awareness among employees is raised and maintained;
- All existing and potential breaches will be reported to the Management representative and Data Protection Officer and will be thoroughly investigated;
- Business Continuity and Disaster Recovery plans are created, implemented and maintained;
- Continually improve the effectiveness of the implemented Information security management system, through a policy of continual improvement.

In order to fulfil these objectives, and to provide the level of control and traceability, necessary to demonstrate compliance with recognized processes, it is the policy of the organization to maintain an efficient and effective Information security and Privacy management system based upon the requirements of the ISO 27001 Information security Management Systems Standard and ISO 27701 Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.

This Information Security and Privacy Policy and the management system shall be reviewed and where necessary revised as a minimum during formal annual review to ensure that they are continually improved.

The Management representative and the managers are responsible for implementing and maintaining the policy and providing full support.

Change Log

Version	Revision category (new requirement, update, wording)	Placement (chapter)	Description of main revisions	Date
1.0	New Policy		Policy creation and approval	20.10.2020
2.0	New requirements		Extension to ISO 27001 for privacy information management (ISO 27701)	1.03.2022