NETERRA telecommunications

Kambanite Green Offices, fl. 3,
9 Vitoshki Kambani str., 1766 Sofia, Bulgaria,
Phone: +359 2 975 16 16,
neterra.net

INFORMATION SECURITY, PRIVACY AND BUSINESS CONTINUITY POLICY of NETERRA EOOD

The primary objective of information security, privacy, business continuity, information technology, and IT service management is to ensure the integrity and confidentiality of both company and customer/data subject information. It further aims to guarantee business process continuity and maintain heightened attention to detail across all activities involving consulting, designing, engineering, implementing, provisioning, and supporting systems and solutions in the fields of telecommunications, radio and satellite connectivity, audio and video services, colocation, IT services, cloud services, network infrastructure, managed services, and network security.

This policy applies to all employees, contractors, and third parties who have access to our information assets or are involved in processing, storing, transmitting, or managing information within our organization.

Within NETERRA EOOD, **"Information Security"** entails the application of a combination of technical, administrative, and physical controls designed to protect information assets. Its purpose is to safeguard against a wide range of threats, including unauthorized access, data breaches, cyberattacks, malware, insider threats, and other vulnerabilities that could compromise the security and reliability of information and information systems.

Our **information security and business continuity objectives** are as follows:

a. Protecting information confidentiality by ensuring that access is restricted to authorized individuals and preventing unauthorized disclosure.

b. Protecting information integrity by maintaining its accuracy, completeness, and reliability throughout its entire lifecycle.

c. Ensuring the availability of information resources and IT systems to support the business strategy and stakeholder requirements.

d. Complying with applicable legal, regulatory, and contractual requirements related to information security.

e. Managing current and projected information security risks and threats by implementing appropriate controls and continuously improving our security posture.

f. Fostering information security-conscious culture through training, awareness programs, and regular communication.

g. Enhancing disaster resilience through the continuous improvement of business continuity systems and measures.

h. Reducing recovery time following disruptions.

i. Preparing personnel for disaster response.

Kambanite Green Offices, fl. 3,
9 Vitoshki Kambani str., 1766 Sofia, Bulgaria,
Phone: +359 2 975 16 16,
neterra.net

Information Security and Business Continuity Management Principles at NETERRA EOOD:

Confidentiality: Protecting information from unauthorized access or disclosure to preserve its secrecy.

Integrity: Ensuring the accuracy, completeness, and reliability of information by safeguarding it against unauthorized alteration or deletion.

Availability: Ensuring timely and reliable access to information and IT systems for authorized users.

Risk Management: Identifying, assessing, and mitigating information security and business continuity risks to protect against potential threats and vulnerabilities.

Compliance: Adhering to applicable laws, regulations, and contractual obligations related to information security.

Awareness and Training: Fostering a culture of information security awareness through education and training programs for all personnel.

Incident Response: Establishing effective incident response procedures for the rapid detection of, response to, and recovery from information security and business continuity incidents.

Business Continuity: Developing and maintaining business continuity plans to ensure the availability and timely recovery of critical information assets and IT systems.

Principle of Least Privilege: Granting individuals only the access rights necessary for their specific roles and responsibilities to minimize the risk of unauthorized access.

Monitoring and Continuous Improvement: Regularly reviewing and enhancing information security and business continuity measures to adapt to evolving threats and technologies.

Security by Design: Integrating security considerations throughout the entire lifecycle of systems, applications, and processes—from design to deployment and maintenance.

Accountability: Ensuring individuals take responsibility for their actions and comply with information security and business continuity policies and procedures.

Data Protection: Respecting the right to privacy and protecting personal data in accordance with relevant privacy laws and regulations.

Collaboration: Promoting cooperation and information sharing among stakeholders to enhance the overall security posture and address emerging threats.

Exception and Deviation Management: Establishing procedures and guidelines for handling exceptions and deviations from standard information

Kambanite Green Offices, fl. 3,
9 Vitoshki Kambani str., 1766 Sofia, Bulgaria,
Phone: +359 2 975 16 16,
neterra.net

security practices to minimize risks and maintain the overall effectiveness of the Information Security and Business Continuity Management System.

Allocation of Responsibilities: Assigning tasks, roles, or functions related to information security and business continuity.

Building Recovery Capacity: Maintaining recovery plans and the capability to restore operations quickly and effectively following disruptions.

Testing and Simulations: Conducting tests and simulations of business continuity plans to prepare personnel for real-world scenarios.

We shall achieve these objectives and principles by maintaining and continually improving an operational Management System in accordance with the requirements of **ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 20000-1:2018, and ISO 22301:2019**.

Department heads and the Management and Security Group are responsible for implementing and maintaining the Information Security, Privacy, and Business Continuity Policy, providing full support in communicating it to stakeholders.

All managers are directly responsible for deploying the Information Security, Privacy, and Business Continuity Policy and ensuring compliance by all subordinates.

The Information Security, Privacy, and Business Continuity Policy is reviewed at least once a year during the management review process.

Upon request and where necessary, the Information Security, Privacy, and Business Continuity Policy shall be shared with external stakeholders in an appropriate manner adopted by the company.

DECLARATION

I, in my capacity as CEO of NETERRA EOOD,

Hereby declare my personal involvement and responsibility for the implementation of the stated Information Security, Privacy, and Business Continuity Management Policy regarding protection against internal, external, intentional, and accidental threats, as well as potential risks to the associated information assets.

I declare my commitment and support for the continuous improvement of the information security, privacy, and business continuity management system.

Signed by Neven Petkov Dilkov (No:109915)
Date: 20.10.2026 . 13:11:28 +03:00

Sofia

CEO.....

/N. Dilkov/