NETERRA telecommunications
20A, A.Saharov Blvd., 1784 Sofia, Bulgaria,
Phone: +359 2 975 16 16, Fax: +359 2 975 34 36
www.neterra.net

Information Security Responsibilities Policy and Procedures

The information in this document is internal for Neterra Ltd. The levels of access are as follows:

Level Access	Authorized Person	Storage Place	Electronic copy sending	Paper Copy Access
Internal Access : Free **Internal:All**	*This document and the information in it is intended for use by employees of Neterra Ltd.*	*In electronic mode the document can be kept on all servers, work stations, notebooks and portable storage devices in the company.*	*The document can be sent on the official e-mails (neterra.net, neterra.tv) of the employees.*	*Free access to the current document on paper copy have all employees of Neterra LTD.*
External Access: Free **External-All**	*There are no restrictions of access to this document and the information in it.*	*There are no restrictions regarding the place of storage of the document.*	*There are no restrictions of sending an electronic copy of the document and storing it in electronic form.*	*There are no restrictions for the storage of this document on paper copy.*

Table of Contents

20A, A.Saharov Blvd., 1784 Sofia, Bulgaria,
Phone: +359 2 975 16 16, Fax: +359 2 975 34 36
www.neterra.net

1. Overview

Ensuring the safety and security of organizational assets begins by defining information security responsibilities and assigning such responsibilities to relevant personnel within **Neterra Ltd.**. Information security must be embraced by all employees within an organization for ensuring its success and business processes continuity, thus identifying and assigning relevant roles and responsibilities is absolutely critical.

In accordance with mandated organizational security requirements set forth and approved by management, **Neterra Ltd.** has established a formal information security policy and supporting procedures. This policy has been implemented along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on an annual basis, in the Management Review, for ensuring its adequacy and relevancy regarding **Neterra Ltd.**'s needs and goals and covering all policies and procedures.

2. Purpose

The aim of ensuring the security of information, information technology and services of **Neterra Ltd.** is to determine its risks related to the context of the organization and assets and their protection from internal, external, premeditated and accidental threats.

This policy and applicable supporting procedures are designed to provide **Neterra Ltd.** with a documented and formalized process for ensuring information security responsibilities are clearly identified and assigned to appropriate personnel. Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of **Neterra Ltd.**'s system components.

3. Scope

This policy and supporting procedures encompasses all system components that are owned, operated, maintained, and controlled by **Neterra Ltd.** and all other system components, both internally and externally, that interact with these systems and the business processes for **Consulting, Design, Construction, Implementation, Provisioning and Maintenance of systems and solutions in the field of Telecommunications, Radio and Satellite connectivity, Audio and Video services, Collocation, IT services, Cloud Services, Network infrastructure, Managed services and Network security**

- Internal system components are those owned, operated, maintained, and controlled by **Neterra Ltd.** and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.

- External system components are those owned, operated, maintained, and controlled by any entity other than **Neterra Ltd.**, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system components".

- Note: While **Neterra Ltd.** does not have the ability to actually provision, harden, secure, and deploy another organization's system components, **Neterra Ltd.** will follow PCI DSS due-diligence best practices as mandated in Requirement 12 of the Payment Card Industry Data Security Standards by obtaining all relevant information ensuring that such systems are safe and secure.

4. Roles and Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to **Neterra Ltd.** information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing Cybersecurity challenges.

4.1. Management Commitment:

The Managers of the structural departments and the Management and Security Group are responsible for the implementation, maintenance and continuous improvement of the Information Security Policy, the Management System and provide full support.

Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Head of Operations department is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.

4.2. Internal Employees and Users:

Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any **Neterra Ltd.** system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of **Neterra Ltd.** system components, and are to also report such instance immediately to senior authorities.

4.3. Vendors, Contractors, other Third-Party Entities:

Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

5. Policy

Neterra Ltd. is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

- The context of the organization and all external and internal issues are defined;
- Any changes in the context of the organization and all external and internal issues are taken into account;
- All requirements of the organization and stakeholders related to information security management are addressed;
- The integrity of the information is maintained;
- The availability of information on all processes is maintained;
- The information is protected from unauthorized access;
- Confidentiality of information is ensured;
- The criteria for risk assessment are determined, as well as the probability of threats

and the severity of their impact on the company's assets, against which the level of acceptable risk is determined;

- The normative and internal company requirements for information security are fulfilled;
- Procedures and instructions for implementation of the Information Security Policy have been developed;
- Training in information security management and management of IT services is provided to all employees;
- All existing and potential breaches will be reported to the Management and relevant responsible management and security officers and will be thoroughly investigated;
- Information Security policies are to clearly define information security responsibilities for both employees and contractors and all other personnel.
- Executive management is to formally establish responsibility for the protection of cardholder data, which includes the following:

- Having overall accountability for maintaining PCI DSS compliance.

- Defining a charter for a PCI DSS compliance program and communication to executive management.

- Formal assignment of information security is to be given to a Chief Security Officer or other security-knowledgeable member of management, who is directly responsible for the following:

- Establishing, documenting, and creating and distributing security policies and procedures is to be formally assigned to authorized personnel.

- Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is to be formally assigned to authorized personnel.

- Establishing, documenting, and distributing security incident response and escalation procedures is to be formally assigned to authorized personnel.

- Administering user account and authentication management is to be formally assigned to authorized personnel.

- Monitoring and controlling all access to data is to be formally assigned to authorized personnel.

5.1. Information Security Responsibilities for Employees and Contractors

All employers and contractors utilizing and having access to a broad range of **Neterra Ltd.** information systems are required to adhere to the policies, procedures, provisions and general guidelines outlined in this security policy document and all other applicable supporting policy and procedure documents. Information security responsibilities include but are not limited to the following system components and any other IT resources deemed critical by **Neterra Ltd.**:

- Network devices and supporting network protocols and activities
- Operating systems and supporting systems

- Applications and supporting systems and activities
- Databases
- Data transmission protocols
- End-user devices and technologies

Information security responsibilities include not engaging in any activity that may potentially compromise the organization's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of system components or any other IT resources deemed critical by the organization. Violation of these information security responsibilities is grounds for being reprimanded, suspended or terminated.

5.2. Formal Assignment of Information Security

The formal assignment of information security is to be given to and directed by a Chief Security Officer or other security-knowledgeable member of management. This individual will be responsible for all facets of information security, which include but are not limited to the following:

- Oversight of all information security initiatives
- Approval of all Information Security policies, procedures, provisions and general guidelines
- The administration and assignment of information security activities to authorized personnel within the organization
- Ensuring that all information security initiatives are aligned with all company-wide regulatory compliance, governance and security mandates

Information Security Director	Title	Notes and Comments
Head of Operations department	Chief Security Officer	In charge of all aspects of information security responsibilities, initiatives and mandates
Manager of Legal and Regulatory Policy	Information Security Officer	In charge of legal aspects of information security responsibilities, initiatives and mandates

5.2.1. Information Security Responsibilities Matrix

Responsibility	Responsibility Formally Assigned to the Following Personnel (Title)	Notes and Comments
Creating and distributing security policies and procedures	Head of Operations department	

20A, A.Saharov Blvd., 1784 Sofia, Bulgaria,
Phone: +359 2 975 16 16, Fax: +359 2 975 34 36
www.neterra.net

Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel	Manager ITSOC&NMT-IT	
Creating and distributing security incident response and escalation procedures	Manager Network Operations Center (NOC) division	
Administering user account and authentication management	System Administrators	Shared responsibility
Monitoring and controlling all access to data	Senior System Administrator	

5.2.2. PCI DSS Executive Management Charter Matrix

The responsible team will assist **Neterra Ltd.** in getting compliant with the PCI DSS and reduce the scope of items that will need to be compliant with the PCI DSS by implementing the changes set forth by the management. The functions and conditions under which the PCI DSS compliance program is organized and communicated to executive management are:

- Meet at least every six months and on significant case to address issues and findings;
- Develop strategies for remediation of non-compliant items;
- Monitor, support and follow up with clients to ensure any and all corrective actions are applied;
- Report any feedback, concerns and proposals from the clients to the project team;
- Assist clients in proper implementation of their PCI DSS Compliance

Responsibility	Responsibility Formally Assigned to the Following Personnel (Title)	Notes and Comments
Having overall accountability for maintaining PCI DSS compliance.	Senior engineer Collocation	
Defining a charter for a PCI DSS compliance program and communication to executive management.	Manager Procurement of goods division and Product manager Collocation	

6. Procedures

Neterra Ltd. is to ensure that all applicable users adhere to the following procedures and supporting activities listed below. Additionally, the relevant procedures will be fully enforced by **Neterra Ltd.** for ensuring such initiatives are executed in a formal manner and on a consistent basis for all specified systems resources.

- Undertake all necessary activities for ensuring the aforementioned policies are implemented. This ultimately requires coordination amongst various **Neterra Ltd.** personnel, along with utilizing various security tools, vendor documentation, and other supporting materials for ensuring the stated policy mandates are met.
- Complete the **Information Security Responsibilities Matrix** and answer all corresponding columns. This matrix is to be reviewed on a regular basis, which is at a minimum, every six (6) months, or more frequently, if necessary. Specifically, the matrix must be updated when personnel are added, relocated, decommissioned.
- Complete the **PCI DSS Executive Management Charter Matrix** and answer all corresponding columns. This matrix is to be reviewed on a regular basis, which is at a minimum, every six (6) months, or more frequently, if necessary. Specifically, the matrix must be updated when personnel are added, relocated, decommissioned.
- If changes must be made to system components – such as additional hardening procedures, configuration changes, or any other necessary I.T. changes for ensuring continued compliance with the aforementioned policies – then a ticket/change order is to be opened and submitted in the **rt.neterra.net** ticketing system which effectively details the reason for the change, what actual changes will be made, why, and any other relevant information.

7. Compliance Cross Reference Matrix

The following Matrix is to be completed for purposes of cross-referencing this specific PCI DSS document with any other mandated regulatory compliance requirements for **Neterra Ltd.**. As such, a brief summary describing the contents of this document must be provided, allowing management to effectively cross-reference and align with the below referenced compliance standards, framework and/or regulations, etc.

Document Summary	List of Compliance Standards Frameworks, Regulations	Cross Reference Details	General Notes and Comments
Policy and procedures for ensuring that the confidentiality, integrity, and availability (CIA) of **Neterra Ltd.**'s system components are compliant	**ISO 27001/27002**	***A 5.1.1***	
	ISO 27001/27002	**A 5.1.2**	
	ISO 27001/27002	**A 6.1.1**	
	ISO 27001/27002	**A 6.1.2**	

20A, A.Saharov Blvd., 1784 Sofia, Bulgaria,
Phone: +359 2 975 16 16, Fax: +359 2 975 34 36
www.neterra.net

8. Responsibility for Policy and Procedures Maintenance

Chief Security Officer is responsible for ensuring that the aforementioned policy initiatives, and if applicable – the relevant procedures – are kept current as needed for purposes of compliance with mandated organizational security requirements set forth and approved by management.

9. Disclosure

Neterra Ltd. reserves the right to change and modify the aforementioned document at any time and to provide notice to all users in a reasonable and acceptable timeframe and format.

DECLARATION

As a CEO of **Neterra Ltd.**,

I declare my personal participation and responsibility for the implementation of the announced Information Security Policy, regarding the protection against all possible risks and the related information assets from internal, external, premeditated and accidental threats.

Neven Petkov Dilkov
Digitally signed by Neven Petkov Dilkov
Location: Sofia, Bulgaria
Date: 2020.11.25 14:33:57 +0200

20.11.2020 **CEO**: .....

Sofia /N. Dilkov/