NETERRA
telecommunications

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

Политики и процедури на Отговорностите за Сигурност на Информацията

Ниво на достъпа	Лице, което има достъп	Място за съхранение	Изпращане на електронно копие	Достъп до хартиено копие
Вътрешен достъп: **Свободен** **Internal:All**	*Този документ и информацията в него е предназначен за ползване от служители на „Нетера“ ЕООД*	*В електронен вид документът може да се съхранява на всички сървъри, работни станции, преносими компютри и преносими носители в дружеството.*	*Документът може да бъде изпращан на служебните електронни пощи (neterra.net, neterra.tv) на служителите.*	*Свободен достъп до настоящия документ на хартиен носител имат всички служители на „Нетера“ ЕООД.*
Външен достъп: **Свободен** **External-All**	*Няма ограничения в правото на достъп до настоящия документ и информацията в него.*	*Няма ограничения по отношение мястото на съхранение на документа.*	*Няма ограничения за изпращането на електронно копие от документа, както и за съхранението му в електронен вид.*	*Няма ограничения за съхранението на настоящия документ на хартиен носител.*

Table of Contents

NETERRA
telecommunications

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

1. Преглед

Осигуряването на безопасност и сигурност на активите и системите на компанията започва с дефиниране на отговорностите по Сигурност на Информацията и Възлагането на тези отговорности на съответни служители в **НЕТЕРА ЕООД**. Сигурността на информацията трябва да е приета от всички служители на компанията, за да се гарантира нейното изпълнение и непрекъсваемостта на бизнес процесите, също както е от изключителна важност ролите и отговорностите да бъдат разпределени.

В съответствие с изискванията по Сигурност, установени и одобрени от ръководството, **НЕТЕРА ЕООД** е въвела официална Политика по Сигурност на информацията и поддържащи процедури. Тази политика се прилага, заедно с всички свързани и приложими процедури. В допълнение, Политиката трябва да се преразглежда минимум веднъж годишно, при Прегледа от ръководството, за да се гарантира нейната адекватност спрямо целите и нуждите на **НЕТЕРА ЕООД,** както и че покрива всички всички фирмени политики и процедури.

2. Цел

Цел по осигуряване на сигурността на информацията, информационните технологии и услуги на **НЕТЕРА ЕООД** е и определяне на нейните рискове, свързани с контекста на организацията и активи и защитата им от вътрешни, външни, предумишлени и случайни заплахи.

Политиката и приложимите процедури са създадени, за да осигурят на **НЕТЕРА ЕООД** документиран и формализиран процес за осигуряване на Сигурността на информацията и ясно идентифицирани и разпределени отговорности на съответните служители. В допълнение, спазването на тази Политика и съответните процедури гарантира сигурността, интегритета и наличността на компонентите на Системата на **НЕТЕРА ЕООД**.

3. Обхват

Политиката и процедурите обхващат всички компоненти на системата, които са собственост, поддържат се и се управляват от **НЕТЕРА ЕООД** и всички други компоненти на системата, вътрешни и външни, които взаимодействат с тези системи, както и процесите по **Консултиране, проектиране, изграждане, внедряване, предоставяне и поддръжка на системи и решения в областта на телекомуникациите, радио и сателитни свързаности, аудио и видео услуги, колокация, IT услуги, облачни услуги, мрежова инфраструктура, управляеми услуги и мрежова сигурност.**

- Вътрешните компоненти на системата са тези, които са собственост, управляват се и се поддържат от **НЕТЕРА ЕООД** и включват всички мрежови устройства (защитни стени, рутери, комутатори и др.), сървъри (физически и виртуални, заедно със системите за управление и поддържащите ги приложения) и всички други системни компоненти, влизащи в обхвата на ISO 27001, както и всички системни компоненти за контрол на достъпа и физическата сигурност, влизащи в обхвата на PCI DSS.

- Външните компоненти на системата са тези, които са собственост, поддържат се и се управляват от субект, различен от **НЕТЕРА ЕООД**, но за които такива външни ресурси могат да повлияят на поверителността,

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

целостта и наличността и цялостната сигурност на гореспоменатото описаните „Вътрешни компоненти на системата".

• Бележка: **НЕТЕРА ЕООД** няма способността да осигури, утвърди, защити и внедри системните компоненти на друга организация, но ще следва най-добрите практики за комплексна проверка на PCI DSS, както е предвидено в изискване 12 от стандартите за сигурност на данните на платежните карти, като получи цялата съответна информация, гарантираща, че такива системи са безопасни и сигурни.

4. Роли и отговорности

Прилагането и спазването на организационните политики и процедури е съвместно усилие, изискващо истински ангажимент от целия персонал, включително мениджмънт, вътрешни служители и потребители на системните компоненти, заедно с доставчици, изпълнители и други трети страни. Освен това, след като са наясно с ролите и отговорностите, свързани с информационните системи на **НЕТЕРА ЕООД**, всички съответни страни помагат за популяризирането на принципите за поверителност, цялостност и наличност на информационната сигурност в днешния свят на нарастващи предизвикателства в областта на киберсигурността.

4.1. Ангажираност на управлението:

Ръководителите на структурните звена и Групата по управление и сигурност са отговорни за внедряването, поддържането и непрекъснатото подобрение на Политиката по сигурност на информацията, Системата за управление и осигуряват пълна подкрепа.

Отговорностите включват осигуряване на цялостно ръководство, насоки, лидерство и подкрепа за цялата среда на информационните системи, като същевременно подпомага други служители в ежедневните им операции. Оперативният ръководител на отдел Технически трябва редовно да докладва на други членове на висшето ръководство относно всички аспекти на позицията на информационните системи на организацията.

4.2. Вътрешни служители и потребители:

Отговорностите включват спазване на политиките, процедурите, практиките на организацията за информационна сигурност и непредприемането на каквато и да е мярка за промяна на такива стандарти върху компонентите на системата на **НЕТЕРА ЕООД**. Освен това служителите и потребителите трябва да докладват за случаи на несъответствие на висши органи, по-специално такива на други потребители. Служителите и потребителите - докато извършват ежедневни операции - могат също така да забележат проблеми, които биха могли да възпрепятстват безопасността и сигурността на компонентите на системата на **НЕТЕРА ЕООД**, и също трябва незабавно да докладват за такъв случай на висшите органи.

4.3. Производители, Контрагенти и други трети лица:

Отговорностите за такива лица и организации приличат на тези, посочени за служителите и потребителите: придържане към политиките, процедурите, практиките на организацията за сигурност на информацията и не предприемане на каквато и да е мярка за промяна на такива стандарти върху тези системни компоненти.

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

5. Политика

НЕТЕРА ЕООД трябва да гарантира, че всички потребители се придържат към следните политики за целите на спазването на задължителните организационни изисквания за сигурност, определени и одобрени от ръководството:

- Контекстът на организацията и всички външни и вътрешни въпроси са определени;
- Всякакви промени в контекста на организацията и всички външни и вътрешни въпроси се взимат в предвид;
- Всички изисквания на организацията и заинтересованите страни, свързани с управлението на сигурността на информацията, са разгледани;
- Целостта на информацията се поддържа;
- Наличността на информацията по всички процеси се поддържа;
- Информацията е предпазена от неоторизиран достъп;
- Поверителността на информацията е осигурена;
- Критериите за оценяване на рисковете са определени, както е и оценена вероятността от възникване на заплахи и тежестта на тяхното въздействие за активите на фирмата, спрямо които е определено нивото на приемлив риск;
- Нормативните и вътрешно фирмени изисквания по сигурност на информацията се изпълняват;
- Разработени са процедури и инструкции за изпълнение на Политиката по сигурност на информацията;
- Осигурено е обучение по управление на сигурността на информацията и управление на ИТ услуги на всички служители;
- Всички съществуващи и потенциални пробиви ще бъдат съобщавани на Представителя на ръководството и съответните отговорни служители по управление и сигурност и ще бъдат щателно разследвани;
- Политиките за информационна сигурност трябва ясно да определят отговорностите за информационна сигурност както за служителите, така и за изпълнителите, както и за целия друг персонал.
- Изпълнителното ръководство трябва официално да установи отговорности за защитата на данните на картодържателите, което включва следното:

- Цялостна отчетност за поддържане на PCI DSS съответствие.

- Определяне на харта с програма за спазване на PCI DSS и комуникация с ръководството.

- Официалното възлагане на информационната сигурност трябва да се даде на главен служител по сигурността или друг познаващ сигурността член на ръководството, който е пряко отговорен за следното:

- Установяването, документирането и създаването и разпространението на политики и процедури за сигурност трябва да бъде официално възложено на упълномощен персонал.

- Мониторингът и анализът на сигналите за сигурността и разпространението на информация до подходящия персонал по сигурността на информацията и управлението на бизнес звената трябва да бъдат официално възложени на оторизиран персонал.

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

- Установяването, документирането и разпространението на процедурите за реакция и ескалация на инциденти по сигурността трябва да бъде официално възложено на упълномощен персонал.

- Администрирането на потребителски акаунти и управлението на удостоверяването трябва да бъде официално възложено на упълномощен персонал.

- Мониторингът и контролът на целия достъп до данни трябва да бъдат официално възложени на оторизиран персонал.

5.1. Отговорности по Сигурност на Информацията на служители и контрагенти

Всички работодатели и изпълнители, които използват и имат достъп до широк спектър от информационните системи на **НЕТЕРА ЕООД**, са длъжни да се придържат към политиките, процедурите, разпоредбите и общите насоки, посочени в този документ за политиката по сигурност и всички други приложими подкрепящи документи за политики и процедури. Отговорностите за информационна сигурност включват, но не се ограничават до следните системни компоненти и всякакви други ИТ ресурси, считани за критични от **НЕТЕРА ЕООД**:

- Мрежови устройства и поддържащи мрежови протоколи и дейности
- Операционни и поддържащи системи
- Приложения и поддържащи системи и дейности
- Бази данни
- Протоколи за предаване на данни
- Устройства и технологии за крайни потребители

Отговорностите за информационна сигурност включват неангажиране с каквато и да е дейност, която може потенциално да компрометира мрежовата инфраструктура на организацията, да причини вреда на други свързани системи или да представлява значителна финансова, оперативна или бизнес заплаха за организацията поради злоупотреба със системни компоненти или други ИТ ресурси, считани за критични от организацията. Нарушаването на тези отговорности за информационна сигурност е основание за порицание, отстраняване или прекратяване на взаимоотношенията с тези лица.

5.2. Формално възлагане на роли при Сигурност на Информацията

Официалното възлагане на информационната сигурност трябва да бъде дадено и ръководено от главен служител по сигурността или друг познаващ сигурността член на ръководството. Това лице ще отговаря за всички аспекти на информационната сигурност, които включват, но не се ограничават до следното:

- Надзор върху всички инициативи за информационна сигурност
- Одобряване на всички политики, процедури, разпоредби и общи насоки за информационна сигурност
- Администриране и възлагане на дейности по информационна сигурност на

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

упълномощен персонал в организацията

• Гарантиране, че всички инициативи за информационна сигурност са съобразени с регулациите, управлението и сигурността в цялата компания

Управление на инфомационната сигурност	Роля	Бележки и коментари
Оперативен ръководител отдел Технически	Главен служител по сигурността	Отговаря за всички аспекти на отговорностите, инициативите и изискванията по сигурността на информацията
Ръководител направление Правна и регулаторна политика	Служител по информационна сигурност	Отговаря за правните аспекти на отговорностите, инициативите и изискванията по сигурността на информацията

5.2.1. Матрица на отговорностите в Сигурност на Информацията

Отговорност	Отговорност, официално възложена на следния служител/и (длъжност)	Бележки и коментари
Създаване и разпространение на политики и процедури за сигурност	Оперативен ръководител отдел Технически	
Мониторинг и анализ на сигналите за сигурност и разпространение на информация до подходящия персонал по управление на информационната сигурност и бизнес звената	Мениджър ITSOC&NMT-IT	
Създаване и разпространение на процедури за реакция и ескалация на инциденти със сигурността	Мениджър направление Център за наблюдение на мрежата	
Администриране на потребителски акаунти и управление на удостоверяването	Системни администратори	Споделена отговорност

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

Мониторинг и контрол на целия достъп до данни	Старши системен администратор	

5.2.2. PCI DSS Матрица на изпълнителния мениджмънт

Отговорният екип ще подпомогне **Нетера ЕООД** при спазването на PCI DSS и ще намали обхвата на елементите, които ще трябва да бъдат съвместими с PCI DSS, като внедри промените, определени от ръководството. Функциите и условията, при които програмата за спазване на PCI DSS се организира и съобщава на изпълнителното ръководство, са:

- Среща на всеки шест месеца и при значими случаи, за да се разгледат въпросите и констатациите;
- Разработване на стратегии за отстраняване на несъответстващи елементи;
- Наблюдение, поддръжка и проследяване на клиенти и партньори, за да се гарантира прилагането на всички коригиращи действия;
- Докладване на всякакви отзиви, опасения и предложения от клиенти и партньори на екипа на проекта;
- Подпомагане на клиентите за правилна имплементация на техните PCI DSS съвместими изисквания.

Отговорност	Отговорност, официално възложена на следния служител/и (длъжност)	Бележки и коментари
Цялостна отчетност за поддържане на PCI DSS съответствие.	Старши инженер Колокация	
Определяне на харта на програма за съответствие с PCI DSS и комуникация с изпълнителното ръководство.	Мениджър направление Доставка на стоки и Продуктов мениджър Колокация	

6. Процедури

НЕТЕРА ЕООД трябва да гарантира, че всички потребители се придържат към следните процедури и поддържащи дейности, изброени по-долу. Освен това съответните процедури ще бъдат изцяло приложени от **НЕТЕРА ЕООД**, за да се гарантира, че такива инициативи се изпълняват по официален начин и последователно за всички посочени системни ресурси.

- Предприемане на всички необходими дейности за осигуряване на изпълнението на гореспоменатите политики. Това изисква координация между различния персонал на **НЕТЕРА ЕООД**, заедно с използването на различни инструменти за сигурност, документация на доставчици и други помощни материали за осигуряване на спазването на посочените политики.

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

• Попълване на **Матрицата за отговорности на информационната сигурност** и на всички съответни колони. Тази матрица трябва да се преразглежда редовно, което е минимум, на всеки шест (6) месеца или по-често, ако е необходимо. По-конкретно, матрицата трябва да се актуализира, когато при персоналът се назначава, премества или напуска служител.

• Попълване на **PCI DSS Изпълнителната харта за управление** и на всички съответни колони. Тази матрица трябва да се преразглежда редовно, което е минимум, на всеки шест (6) месеца или по-често, ако е необходимо. По-конкретно, матрицата трябва да се актуализира, когато при персоналът се назначава, премества или напуска служител.

• Ако трябва да се направят промени в системните компоненти - като допълнителни процедури за утвърждаване, промени в конфигурацията или други необходими I.T. промени за осигуряване на непрекъснато спазване на гореспоменатите политики - тогава тикетът / заявката за промяна трябва да бъде отворен и подаден в системата **rt.neterra.net**, която ефективно детайлизира причината за промяната, какви действителни промени ще бъдат направени, защо и всякаква друга подходяща информация.

7. Контролна матрица за съответствие

Матрицата е попълнена за целите на кръстосано свързване на този специфичен документ, PCI DSS с други изисквания за нормативно съответствие на **НЕТЕРА ЕООД**. Като такова трябва да се предостави кратко резюме, описващо съдържанието на този документ, което позволява на ръководството ефективно да прави препратки и да се привежда в съответствие със посочените по-долу стандарти за съответствие, рамка и / или разпоредби и т.н.

Резюме на доикумента	Списък на рамките за стандарти за съответствие, регламенти	Подробности за кръстосани детайли	Общи бележки и коментари
Политика и процедури, които гарантират, че поверителността, целостта и наличността на системните компоненти на **НЕТЕРА ЕООД** са в съответствие	**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**	

8. Отговорност за поддръжка на Политиките и Процедурите

Главния служител по сигурността на информацията е отговорен и гарантира, че гореспоменатите политики и, ако е приложимо - съответните процедури, се поддържат актуални при необходимост за целите на спазването на изискванията за сигурност, определени и одобрени от ръководството.

NETERRA
telecommunications

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net

9. Разпространение

НЕТЕРА ЕООД си запазва правото да променя и модифицира гореспоменатия документ по всяко време и да известява всички заинтересовани страни в разумен и приемлив срок и формат.

ДЕКЛАРАЦИЯ

Аз, като Управител на **НЕТЕРА ЕООД,**

Декларирам личното си участие и отговорност за изпълнение на обявената Политика за управление на сигурността на информацията, относно защитата от всички възможни рискове и свързаните с тях информационни активи от вътрешни, външни, предумишлени и случайни заплахи.

Neven Petkov

Digitally signed by Neven Petkov
Location: Sofia, Bulgaria
Date: 2020.11.25

20.11.2020 **Управител**: .....

София /Н. Дилков/

NETERRA
telecommunications

Камбаните Грийн Офиси, ет.3,
ул. „Витошки Камбани“ 9, в.з. Малинова долина,
1766 София, България, тел.: +359 2 975 16 16
www.neterra.net