

**ПОЛИТИКА
ПО СИГУРНОСТ И НЕПРИКОСНОВЕНОСТ НА ИНФОРМАЦИЯТА
И НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА
на НЕТЕРА ЕООД**

Основната цел на управлението на сигурността и неприкосновеността на информацията и непрекъснатост на дейността, информационните технологии и предоставяне на ИТ услуги е да се осигури целостта и поверителността на информацията, както тази на дружеството така и на клиентите и субектите на лични данни, да се осигури непрекъсваемост на бизнес процесите и повишено внимание към всеки детайл по време на дейностите 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, ИТ услуги, облачни услуги, мрежова инфраструктура, управляеми услуги и мрежова сигурност.**

Тази политика се прилага за всички служители, изпълнители и трети страни, които имат достъп до нашите информационни активи или участват в обработката, съхранението, предаването или управлението на информация в рамките на нашата организация.

"Информационна сигурност" в НЕТЕРА ЕООД включва прилагането на комбинация от технически, административни и физически контроли за защита на информационните активи и има за цел да защитава от широк кръг заплахи, включително неоторизиран достъп, нарушаване на сигурността на данните, кибератаки, зловреден софтуер, вътрешни заплахи и други уязвимости, които могат да компрометират сигурността и надеждността на информацията и информационните системи.

Нашите **цели за информационна сигурност** и непрекъснатост на дейността са следните:

- a. Защита на поверителността на информацията, като гарантираме, че достъпът е ограничен до упълномощени лица и предотвратяваме неразрешено разкриване.
- b. Защита на целостта на информацията чрез поддържане на нейната точност, пълнота и надеждност през целия ѝ жизнен цикъл.
- c. Осигуряване на наличността на информационните ресурси и ИТ системите в подкрепа на бизнес стратегията и изискванията на заинтересованите страни.
- d. Спазване на приложимите закони, регулаторни и договорни изисквания, свързани със сигурността на информацията.
- e. Управление на настоящите и прогнозираните рискове и заплахи за информационната сигурност, като прилагаме подходящи контроли и непрекъснато подобряваме нашата позиция по отношение на сигурността.
- f. Насърчаване на култура, съобразена с информационната сигурност, чрез обучение, програми за повишаване на осведомеността и редовна комуникация.
- g. Повишаване на устойчивостта към бедствия чрез непрекъснато усъвършенстване на системите и мерките за непрекъснатост на дейността]
- h. Намаляване на времето за възстановяване след прекъсвания;

i. Подготовка на персонала за реакция при бедствия.

Принципи за управление на сигурността на информацията и непрекъснатостта на дейността в НЕТЕРА ЕООД:

Конфиденциалност: защита на информацията от неоторизиран достъп или разкриване, за да се запази нейната поверителност.

Интегритет: гарантиране на точността, пълнотата и надеждността на информацията чрез предпазване от неразрешено изменение или изтриване.

Наличност: осигуряване на своевременно и надежден достъп до информация и ИТ системи от оторизирани лица.

Управление на риска: идентифициране, оценяване и намаляване на рисковете за информационната сигурност и непрекъснатостта на дейността с цел защита от потенциални заплахи и уязвимости.

Съответствие: придържане към приложимите закони, разпоредби и договорни задължения, свързани със сигурността на информацията.

Информираност и обучение: насърчаване на култура на информираност за информационната сигурност чрез програми за обучение и образование за целия персонал.

Реагиране на инциденти: създаване на ефективни процедури за реагиране на инциденти с цел бързо откриване, реагиране и възстановяване след инциденти, свързани с информационната сигурност и непрекъснатостта на дейността.

Непрекъснатост на бизнеса: разработване и поддържане на планове за непрекъсваемост на бизнеса, за да се гарантира наличността и своевременното възстановяване на критични информационни активи и ИТ системи.

Принцип на най-малкото право: предоставяне на лица на права за достъп, необходими само за техните роли и отговорности, за да се сведе до минимум рискът от неоторизиран достъп.

Мониторинг и непрекъснато подобряване: редовно преразглеждане и подобряване на мерките за информационна сигурност и непрекъснатост на дейността, за да се адаптират към развиващите се заплахи и технологии.

Сигурност по проект: интегриране на съображенията за сигурност през целия жизнен цикъл на системите, приложенията и процесите – от проектирането до внедряването и поддръжката.

Ангажираност: поемане на отговорност от лицата за техните действия и осигуряване на съответствие с политиките и процедурите за информационна сигурност и непрекъснатост на дейността.

Защита на личните данни: зачитане на правото на неприкосновеност на личния живот и защита на личните данни в съответствие със съответните закони и разпоредби за неприкосновеност на личния живот.

Сътрудничество: насърчаване на сътрудничеството и обмяна на информация между заинтересованите страни с цел подобряване на цялостната позиция по отношение на сигурността и справяне с нововъзникващи заплахи.

Справяне с изключенията и отклоненията: установени процедури и насоки за справяне с изключенията и отклоненията от стандартните практики за информационна сигурност, за

да се сведат до минимум рисковете и да се поддържа цялостната ефективност на Системата за сигурност на информацията и непрекъснатостта на дейността.

Възлагане на отговорности: разпределение на задачи, роли или функции по сигурност на информацията и непрекъснатостта на дейността.

Изграждане на капацитет за възстановяване: поддържане на планове за възстановяване и капацитет за бързо и ефективно възстановяване след прекъсвания.

Тестване и симулации на планове за непрекъснатост на дейността с цел подготовка на персонала за реални ситуации.

Тези цели и принципи ще постигаме чрез поддържане и непрекъснато подобрене на функциониращата Система за управление съгласно изискванията на ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 20000-1:2018 и ISO 22301:2019.

Ръководителите на структурните звена и Групата по управление и сигурност са отговорни за внедряването и поддържането на Политиката по сигурност и неприкосновеност на информацията и непрекъснатост на дейността и осигуряват пълна подкрепа при оповестяването ѝ на заинтересованите страни.

Всички ръководители са пряко отговорни за внедряването на Политиката по сигурност и неприкосновеност на информацията и непрекъснатост на дейността и гарантират нейното изпълнение от всички подчинени.

Политиката по сигурност и неприкосновеност на информацията и непрекъснатост на дейността се преглежда минимум веднъж годишно, при провеждане на прегледа от ръководството.

При необходимост и поискване, политиката по сигурност и неприкосновеност на информацията и непрекъснатост на дейността се предоставя и на външни заинтересовани страни по подходящ и възприет във фирмата начин.

ДЕКЛАРАЦИЯ

Аз, като Управител на NETERRA ЕООД,

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

Декларирам своята ангажираност и съдействие за непрекъснатото подобряване на системата за управление на сигурността и неприкосновеността на информацията и непрекъснатост на дейността.

26.02.2024 г.
София

Управител:

/Н. Дилков/