ОБЩИНА МОНТАНА

3400 МОНТАНА, ул."Извора"1, тел:(096) 300 400, факс: (096) 588 391,E-mail: mayor@montana.bg

Утвърждавам:

Златко ЖИВКОВ

КМЕТ на община МОНТАНА

ПОЛИТИКА
ЗА
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

1. Въведение.

Документът определя стратегическите цели на Община Монтана, по отношение на мрежовата и информационната сигурност, подхода за постигането им в съответствие с общите стратегически и оперативни цели, нормативните актове и договорните условия, текущите и потенциалните вътрешни и външни заплахи, които биха имали негативно влияние върху постигането на тези цели и сигурността на информацията. Община Монтана, утвърждава настоящата Политика по информационна сигурност, във връзка със стремежа на ръководството и нейните служители към постоянно подобряване на процедурите и мерките по защита на информацията.

**Подписът не се визуализира в публикуваната версия на документа с оглед защита на личните данни.*

Информационната сигурност представлява защита на информацията, без значение от нейния формат, включително: хартиени документи, цифрова и интелектуална собственост, аудио и видео съдържание.

Мрежовата сигурност има за цел да осигури защитен, оторизиран достъп до ресурси, респективно данни в мрежата само до съответното ниво на упълномощеност. Тя покрива разнообразие от компютърни мрежи, както публични, така и частни и е насочена към гарантиране на сигурността на дадена мрежа и защита/ наблюдение на операциите, извършвани в нея.

2. Цел.

Целта на настоящата политика е:

- да осигури необходимата стабилност, надеждност и защита на критичните информационни системи, ресурси и инфраструктура от различни заплахи като хакерски атаки, зловреден софтуер, опити за нерегламентиран достъп и други форми на киберпрестъпност.
- да минимизира риска от възможни загуби или вреди, причинени от пробиви в информационната сигурност.
- да защити данните и информацията, по начин, който да гарантира тяхната поверителност, цялост и наличност.
- да информира служителите за техните отговорности и задължения по отношение на информационната сигурност.
- да осигури необходимото обучение и осведоменост за разпознаване и противодействие срещу опити за кибератаки.
- да осигури необходимите ресурси за поддържане на ефективна информационна система,
- да гарантира спазването на добрите практики за информационна сигурност, защита на данните и приложимите нормативни изисквания.

3. Обхват

Политиката е приложима за всички служители, изпълнители, доставчици и трети страни, които имат достъп до мрежата и информационните системи и ресурси на Общинска администрация Монтана. Настоящата политика е разяснена и предоставена на вниманието на всички служители и заинтересовани страни, които имат достъп до информационните ресурси и активи на общинската администрация.

4. Роли и отговорности.

Ролите и отговорностите за информационната и мрежова сигурност се разпределят в рамките на цялата общинска администрация, с оглед гарантиране на адекватна подкрепа от страна на ръководството.

Конкретните задължения и отговорности са част от внедрените политики, процедури и специфичните длъжностни характеристики на служителите.

- **Кмет на община Монтана:** председател на Ръководството на общинската администрация и представляващ мрежовата и информационната сигурност на най – високо ръководно управленско равнище.
- **Ръководството на община Монтана:** отговаря за осигуряването на необходимите човешки и информационни ресурси за прилагането на тази политика, идентифициране и оценка на риска за сигурността, извършването на регулярни прегледи на документи и процеси имащи отношение към информационната сигурност и защитата на данните.
- **Екип Мрежова и системна администрация:** отговаря за изграждане, конфигурация, поддръжка, мониторинг и защита на мрежовата инфраструктура, управлението на сървърни конфигурации, операционни системи, бази данни и приложения, системи за сигурност и защита, системи за мониторинг и диагностика, системи за архивиране и възстановяване, системи за управление на потребителски достъп.
- **Екип Сигурност:** отговаря за разработката, внедряването и контрол върху изпълнението на политики и процедури за физическа и техническа сигурност, оценка на рисковете за сигурността, разследване на събития свързани с нарушаване на наложените правила.
- **Екип Регулации:** отговаря за осигуряването на съответствие със приложимото законодателство и нормативна уредба.
- **Потребители / служители на отдели и дирекции:** отговарят за спазването на наложените правила за мрежова и информационна сигурност и докладването на потенциални нарушения или инциденти със сигурността.

- **Трети страни:** отговорят за спазването на политиките за сигурност, съгласно изискванията на разписаните договори и допълнителни споразумения.

5. Стратегия за мрежова и информационна сигурност.

Стратегията за мрежова и информационна сигурност, е в съответствие с бизнес целите на общинската администрация и включва набор от политики, процедури и процеси, които имат за цел да защитят информационните ресурси и активи от потенциални заплахи, уязвимости и инциденти, които биха могли да доведат до невъзможност за изпълнение на дейности, загуба или компрометиране на данни.

6. Цели на информационната сигурност.

- **Поверителност:** защита на информационните ресурси и активи от неоторизиран достъп.
- **Цялостност:** защита на информационните ресурси и активи от неоторизирана промяна или увреждане.
- **Наличност:** осигуряването на достъпност до информационните ресурси и активи във всеки един момент, в който са необходими.

7. Основни политики и процедури за мрежова и информационна сигурност.

7.1 Политика за управление на риска

Обхваща управлението на риска, посредством прилагането на последователен и структуриран подход, целящ ефективното идентифициране и оценка на риска, налагането на необходимите мерки за минимизиране на потенциалното му въздействие върху дейността на общинската администрация и постигането на нейните стратегически цели.

7.2 Процедура при управление на инциденти

Обхваща управлението на инциденти, включващо правилната и навременна идентификация, класификация, оценка, документация, комуникация, докладване и реакция, целящи ефективното противодействие и разрешаване на събития, които могат да окажат негативно влияние върху бизнес процесите и устойчивостта на общинската администрация.

7.3 Процедура за мониторинг и управление на регистрационни файлове

Обхваща дейностите и процесите по мониторинг и управление на регистрационни файлове, целящи осигуряването на проследимост, поддръжка, изправност и нормална функционалност на имплементираните системи, бизнес приложения и услуги.

7.4 План за непрекъсваемост на бизнеса и възстановяване след бедствия.

Обхваща дейностите целящи осигуряването на непрекъсваемостта на критичните бизнес процеси и бързото им възстановяване в случай на възникването на потенциални инциденти и събития засягащи мрежовата и информационната сигурност както и нормалното функциониране на критичните бизнес операции.

7.5 Процедура за архивиране и възстановяване

Обхваща управление на процесите по архивиране и възстановяване, целящи осигуряването на защитата, наличността и целостта на критичните данни и информация в случай на събития свързани със загуба, разрушаване или повреда в информационните системи или настъпването на природни бедствия.

7.6 Политика за сигурност на веригата на доставки

Обхваща насоките, правилата и мерките за защита на веригата за доставки от рискове за сигурността, като неоторизиран достъп, киберзаплахи, кражби и физическо увреждане на информационни активи.

7.7 Политика за сигурност при придобиване и разработка на ИКТ

Обхваща дейностите и мерките целящи минимизирането на риска свързан с придобиването на информационни и комуникационни технологии и защитата на чувствителните информационни ресурси и активи.

7.8 Политика за управление на конфигурацията

Обхваща дейностите по налагането на сигурни конфигурации, поддръжка и контрол на информационните системи и процеси с цел осигуряването тяхната надеждност, сигурност и наличност.

7.9 Процедура за управление на промените

Обхваща дейностите и процесите по планиране и контролирано налагане на промени с цел ограничаване на риска от засягане на нормалното функциониране на общинските информационни системи и ресурси.

7.10 Процедура за управление на уязвимости

Обхваща дейностите по управление на уязвимости, посредством тяхната навременна идентификация, оценка и смекчаване с цел осигуряване на необходимото ниво на защита на общинските информационни системи, приложения и мрежи.

7.11 Политика за мрежова сигурност

Обхваща дейностите и процесите по налагане на адекватни технически и организационни мерки за осигуряване на сигурност и надеждност на използваните мрежови услуги, предотвратяването на опити за неоторизиран достъп до вътрешни мрежови ресурси, дефиниране на ред и правила за осъществяване на отдалечен достъп.

7.12 Политика за защита от злонамерен софтуер

Обхваща прилагането на адекватни мерки за защита на информационните системи, ресурси и крайни потребителски устройства срещу проникването на злонамерен софтуер.

7.13 Процедура за обучения по киберсигурност

Обхваща дейностите по повишаване на нивото на осведоменост и практическите умения на служителите по въпросите свързани с киберсигурността и защитата на информацията, чрез провеждането на редовни обучения, предоставяне на актуална информация за заплахите и възможните подходи за противодействие срещу тях.

7.14 Политика за управление на криптографски механизми

Обхваща определянето на правила и стандарти за използване на криптографски мерки и механизми с оглед осигуряването на необходимото ниво на защита на поверителността, наличността и целостта на информацията в съответствие с приетата класификация на активите.

7.15 Политика за физически контрол на достъпа

Обхваща налагането на физически, технически и организационни мерки за сигурност с цел предотвратяването на нерегламентиран достъп, увреждане и кражба на общинско имущество и чувствителна информация.

7.16 Политика за логически контрол на достъпа

Обхваща налагането на организационни мерки, процедури и механизми за сигурност с цел предотвратяването на нерегламентиран достъп и злоупотреба с чувствителна информация и ресурси.

7.17 Политика за управление на данните и информацията

Обхваща налагането на организационни и технически мерки с цел правилна класификация и защита на информационните ресурси и активи на общинската администрация, съгласно тяхната значимост и стойност.

7.18 Политика за управление на активите

Обхваща определянето на правила, роли и отговорности, свързани с идентифициране, класификация и управление на жизнения цикъл на информационните активи.

8. Преглед на политиката.

Политиката за мрежова и информационна сигурност, следва да бъде преразглеждана за актуалност през определени периоди от време (минимум веднъж годишно), след настъпването на значителни промени или след настъпването на значителни инциденти за да се гарантира нейната ефективност и уместност.

9. История на промените.

Версия	Автор	Дата	Извършена промяна

Настоящата политика е утвърдена със Заповед № 1348/24.06.2025 г. на Кмета на община Монтана.