ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА ОБЩИНА НЕСЕБЪР

Раздел I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата политика има за цел осигуряването на мрежова и информационна сигурност в Община Несебър.

Чл. 2. Мрежовата и информационна сигурност се осигурява чрез организационни, технологични и технически мерки, които са подходящи и пропорционални на рисковете за постигането на основните цели на мрежовата и информационната сигурност.

Чл. 3. Мерките, които Община Несебър прилага във връзка с осигуряването на мрежова и информационна сигурност, са насочени към запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл, включващ създаването, обработването, съхранението, пренасянето и унищожението й в и чрез информационните и комуникационните системи на Община Несебър.

Чл. 4. В Община Несебър за мрежовата и информационната сигурност са отговорни определени в Плана за изпълнение на организационните и технически мерки за повишаване на нивото на мрежовата и информационна сигурност в Община Несебър служители, като:

1. с оглед на спазването на всички изисквания, служителите информират едновременно и Кмета и Секретаря на общината за състоянието и проблемите в мрежовата и информационната сигурност;
2. функциите на служителите, отговарящи за мрежовата и информационната сигурност, са описани в приложение № 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата).

Чл. 5. **Управление на ролите и отговорностите**

(1) Кметът на Община Несебър осигурява необходимите организационни, финансови и технически ресурси за поддържане на адекватно ниво на мрежова и информационна сигурност.

(2) Началник отдел "Информационна сигурност" координира дейностите по управление на риска, наблюдение на сигурността, управление на инциденти и контрол по изпълнение на настоящата политика.

(3) Ръководителите на структурни звена са отговорни за прилагането на мерките по мрежова и информационна сигурност в рамките на съответните административни процеси.

(4) Всички служители са длъжни да спазват изискванията на настоящата политика и незабавно да докладват за установени слабости, инциденти или нарушения на сигурността.

Чл. 6. Настоящата политика се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.

Чл. 7. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 8. На служителите на Община Несебър е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 9. При извършване на работа от разстояние служителите на Община Несебър спазват всички изисквания за осигуряване защитата на данните, в т.ч. лични данни на трети лица и/или по класификацията на информацията.

Чл. 10. Криптографските механизми, които се използват от Община Несебър са съобразени с уязвимостта на информацията към заплахи за нейните конфиденциалност и интегритет и с нормативните и регулаторните изисквания към нейното създаване, съхраняване и пренасяне.

Чл. 11. (1) Всеки служител на Община Несебър има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

(2) Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заеманата длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 12. При разработването на нови информационни и комуникационни системи от Община Несебър се спазват всички изисквания на Наредбата така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда.

Чл. 13. (1) С цел да се намалят загубите от инциденти чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, Община Несебър поддържа следната документация:

1. опис на информационните активи;
2. физическа схема на свързаност;
3. логическа схема на информационните потоци;
4. документация на структурната кабелна система;
5. техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;
6. инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер;
7. вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.

(2) Документацията по ал. 1 е:

1. еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др.;
2. поддържана в актуално състояние, като се преразглежда и при необходимост се обновява поне веднъж годишно;
3. одобрена от кмета на Община Несебър или от упълномощено от него лице;
4. класифицирана по смисъла на чл. 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност;
5. достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.

(3) Община Несебър поддържа информация, доказваща по неоспорим начин изпълнението на изискванията на Наредбата. Същата се поддържа в актуално състояние и е достъпна само за:

а) тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения по силата на трудови, служебни или договорни отношения;

б) представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;

в) други организации, оправомощени с нормативен акт или договорни отношения.

Чл. 14. (1) При установяване на взаимоотношения с доставчици на стоки и услуги, които са "трети страни", Община Несебър договаря изисквания за мрежова и информационна сигурност, включително:

1. за сигурност на информацията, свързани с достъпа на представители на трети страни до информация и активите на Община Несебър;
2. за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;
3. за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност;
4. последици при неспазване на изискванията за сигурност на информацията;
5. отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност;
6. за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент.

(2) Община Несебър определя служител или служители, отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

Чл. 15. **Управление на сигурността на доставчиците**

(1) При възлагане на дейности, свързани с информационни и комуникационни системи, се извършва предварителна оценка на риска, свързан с доставчика.

(2) Община Несебър поддържа актуален регистър на критичните доставчици на информационни и комуникационни услуги.

(3) При установяване на съществен риск от страна на доставчик се предприемат коригиращи действия или се прекратяват договорните отношения при условията на съответния договор.

Чл. 16. С цел повишаване на квалификацията на служителите и на осведомеността им по отношение на мрежовата и информационната сигурност, настоящата политика е сведена до знанието им.

Чл. 17. **Осведоменост и обучение**

(1) Всички служители преминават първоначално обучение по мрежова и информационна сигурност при постъпване на работа.

(2) Най-малко веднъж годишно се провеждат обучения и дейности за повишаване на осведомеността по темите:

   1. киберсигурност;
   2. социално инженерство;
   3. фишинг атаки;
   4. защита на личните данни;
   5. работа от разстояние;
   6. докладване на инциденти.

(3) Проведените обучения се документират.

Чл. 18. Потребителите на информационни системи в Община Несебър са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 19. (1) Община Несебър извършва анализ и оценка на риска за мрежовата и информационната сигурност регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите, влизащи в обхвата на Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) Анализът и оценката на риска са документиран процес по смисъла на чл. 5, ал. 1, т. 6 от Наредбата. В него са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.

(3) Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от кмета на Община Несебър и е достъпна за лицата, на които е възложено да участват в процеса. Може да се прилага препоръчителна методика съгласно приложение № 3 от Наредбата.

(4) На основание на анализа и оценката на риска Община Несебър изготвя план за намаляване на неприемливите рискове, който включва минимум:

1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. необходими ресурси за изпълнение на тези мерки;
3. срок за прилагане на мерките;
4. отговорни лица.

(5) При извършване на анализ и оценка на риска се отчитат:

1. рисковете, произтичащи от веригата на доставки;
2. зависимостите от външни доставчици;
3. въздействието върху предоставяните административни услуги;
4. рисковете за защитата на личните данни;
5. възможните последици от киберинциденти върху непрекъсваемостта на дейността.

Раздел II
АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл. 20. Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в Община Несебър. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл. 21. Основните понятия, част от процеса по управление на риска са както следва:

1. конфиденциалност – свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
2. интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
3. наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

Чл. 22. Цел на процеса за управление на риска е Община Несебър да минимизира загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях в Община Несебър.

Чл. 23. Методиката за управление на риска има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от Община Несебър, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

1. регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2. определяне на критериите;
3. определяне на приоритетите на риска.

Чл. 24. Анализът и оценката на риска са част от процеса за управлението му в Община Несебър и се обосновават на познаване на всички компоненти, имащи отношение към целите.

Чл. 25. За целите на управлението на сигурността на мрежите и информационните системи е необходимо да се:

1. познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация; поддържащите ги системи (електрозахранващи, климатизиращи и др.); оперативни процеси/дейности; служители и външни организации), наричани за краткост "информационни активи";
2. идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
3. оцени вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимостите) на информационните активи и мерките, които са предприети за справяне с тях;
4. оцени въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
5. оцени рискът за сигурността;
6. набележат мерки за смекчаване на рисковете с висок приоритет.

Чл. 26. При анализ и оценка на риска Община Несебър използва регистър на рисковете (риск регистър).

Чл. 27. В риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на Наредбата:

1. информационни системи;
2. хардуерни устройства, с които са реализирани информационните системи;
3. софтуери, с които са реализирани информационните системи;
4. бази данни, включително лични данни по смисъла на GDPR;
5. записи за събитията (логове, журнали) на информационните системи;
6. документация на потребителска); информационните
7. комуникационни системи; системи (експлоатационна
8. хардуерни устройства, с които са реализирани комуникационните системи;
9. фърмуерът на тези устройства;
10. софтуери на комуникационните системи;
11. записи за събитията (логове, журнали);
12. документация (експлоатационна и потребителска);
13. поддържащи системи (електрозахранващи, климатични);
14. системи за контрол на физическия достъп и на околната среда; и
15. процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
16. документация на тези процеси и дейности;
17. служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
18. външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;

Чл. 28. (1) За всеки от информационните активи в риск-регистъра на Община Несебър се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

(2) Община Несебър отчита всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.
Чл .29. В риск-регистъра на Община Несебър за всяка заплаха се вписва какви мерки са предприети срещу нея.
Чл. 30. В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които дадена заплаха може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.
Чл. 31 (1) Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:
1. за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;
2. за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.
(2) В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.
Чл. 32. За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:
1. вероятността от реализирането на заплахата е под 10 %;
2. вероятността от реализиране на заплахата е от 10 % до 30 %;
3. вероятността от реализиране на заплахата е от 30 % до 50 %;
4. вероятността от реализиране на заплахата е от 50 % до 70 %;
5. вероятността от реализиране на заплахата е над 70 %.
Чл. 33. За получаване на оценката на риска в Община Несебър се използва следната формула: (Оценка на въздействие х Оценка на вероятност) = Оценка на риска
Чл. 34. С цел прилагане на пропорционални на заплахите механизми за защита в Община Несебър се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложени в Наредбата.
Чл. 35. (1) Приема се, че за рискове с приоритет 3 по смисъла на Наредбата не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.
(2) За рисковете с приоритет 2 по смисъла на Наредбата се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.
(3) За всички рискове с приоритет 1 се определят отговорни лица, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.
Чл. 36. (1) Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплаха.
(2) Кметът на Община Несебър организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.
Чл. 37. **Управление на инциденти по киберсигурност**

(1) Всички инциденти по мрежова и информационна сигурност се регистрират, анализират и обработват по установен вътрешен ред.
(2) За всеки съществен инцидент се извършва анализ на причините и се определят коригиращи мерки.
(3) При необходимост се уведомяват компетентните органи съгласно приложимото законодателство.

Чл. 38. **Непрекъсваемост на дейността**

(1) Община Несебър поддържа мерки за осигуряване на непрекъсваемост на дейността при възникване на инциденти, аварии или бедствия.
(2) Критичните информационни системи подлежат на архивиране и възстановяване съгласно утвърдени процедури.
(3) Плановете за възстановяване се преглеждат и тестват периодично.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящата Политика за мрежова и информационна сигурност се разглежда и оценява периодично с оглед ефективността ѝ, като Община Несебър може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§2. Настоящата Политика е разработена в съответствие със Закона за киберсигурност, Директива (ЕС) 2022/2555 (NIS2), Наредбата за минималните изисквания за мрежова и информационна сигурност, Регламент (ЕС) 2016/679 относно защитата на личните данни (GDPR), както и приложимите вътрешни правила и политики по информационна сигурност на Община Несебър и е утвърдена със заповед № 3313/11.11.2026 г. на Кмета на Община Несебър.