



РЕПУБЛИКА БЪЛГАРИЯ
ОБЩИНА РУЖИНЦИ ОБЛАСТ ВИДИН
3930, с.Ружинци, обл.Видин, ул. „Георги Димитров” № 31
тел. 09324 /2283, факс 09324 /2604, e-mail: rujinci@abv.bg

Политика за мрежова и информационна сигурност на община Ружинци

Версия:	1.00
Дата:	27.03.2020 г.
Утвърдена от:	Кмет на община Ружинци
Класификация:	Ниво „0“

Раздел I ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата политика има за цел осигуряването на мрежова и информационна сигурност в община Ружинци

Чл. 2. Мрежовата и информационна сигурност се осигурява чрез мерки, пропорционални на рисковете за постигането на основните цели:

1. организационни мерки;
2. технологични мерки;
3. технически мерки;

Чл. 3. Мерки, които община Ружинци 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 ѝ жизнен цикъл, включващ създаването, обработването, съхранението, пренасянето и унищожението ѝ в и чрез информационните и комуникационните системи на общината.

Чл. 4. (1) С наборът от планирани и реализирани мерки за сигурност на информацията, които са взаимосвързани и взаимодействащи се изгражда система за управление на информационната сигурност.

(2) Системата за управление на сигурността на информацията се интегрира в дейностите, процесите и управленската структура на община Ружинци съгласно БДС EN ISO/EN 27001:2017, како си взаимодейства и с други внедрени системи за управление на база на общи елементи, както следва:

1. общ контекст – вътрешна и външна среда;
2. лидерство – засилено участие на ръководството в интегрирането на системите за управление;
3. процесен подход – системно идентифициране и управление на процесите и тяхното въздействие, така че да се постигнат предвидените резултати;
4. мислене основано на риска.

Чл. 5. (1) В община Ружинци за мрежовата и информационната сигурност е отговорен служител по мрежова и информационна сигурност, като:

1. с оглед на спазването на всички изисквания, служителят е на пряко подчинение на кмета на общината и пряко го информира за състоянието и проблемите в мрежовата и информационната сигурност;
2. препоръчителни функции на служителят, отговарящ за мрежовата и информационната сигурност, са описани в приложение № 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата).

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 общината 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 общината 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 общината 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 Ружинци 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 общината 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, общината поддържа следната документация:

1. опис на информационните активи – поддържа се актуален регистър на информационните ресурси на общината;
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. вътрешни правила за мрежова и информационна сигурност;
7. инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер;
8. 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 оборот на документи 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 актуализира;
3. утвърдена от кмета на общината 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) Общината поддържа информация, доказваща по неоспорим начин изпълнението на изискванията Наредбата. Същата се поддържа в актуално състояние и е достъпна само за:

1. тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения по силата на трудови, служебни или договорни отношения;
2. представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;
3. други организации, оправомощени с нормативен акт или договорни отношения.

Чл. 14. При установяване на взаимоотношения с доставчици на стоки и услуги, които са "трети страни", общината 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 общината;
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) Кметът на община Ружинци със своя заповед определя служител или служители, отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

(3) Като неразделна част от договора се изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.

Чл. 15. Потребителите на информационни системи в община Ружинци са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 16. (1) Община Ружинци 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 съгласно Стратегия за управление на риска в община Ружинци и се използва препоръчителната методика /Приложение № 3/ на Наредбата за мрежова и информационна сигурност.

(4) На основание на анализа и оценката на риска общината 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.

Раздел II

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

Чл. 17. (1) 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.

(2) 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. 18. Цел на процеса за управление на риска е общината 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 общината.

Чл. 19. 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 общината, 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. 20. Анализът и оценката на риска са част от процеса за управлението му в общината и се обосновават на познаване на всички компоненти, имащи отношение към целите.

Чл. 21. За целите на управлението на сигурността на мрежите и информационните системи е необходимо да се:

1. да се познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата -наричани за краткост "информационни активи".
 - а) информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация.
 - б) поддържащите ги системи (електрозахранващи, климатизиращи и др.).
 - в) оперативни процеси и дейности.
 - г) служители и външни организации.
2. да 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. да се извърши оценка вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;

4. да се извърши оценка 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. да се оцени рискът за сигурността;
6. да се набелязват мерки за смекчаване на рисковете с висок приоритет.

Чл. 22. (1) За всеки от идентифицираните рискове се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

(2) Общината 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. 23. (1) В таблица за оценка на риска за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които 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.

(2) 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.

(3) За оценка на вероятността 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 %.

(4) За получаване на оценката на риска в общината се използва следната формула:

(Оценка на въздействие x Оценка на вероятност) = Оценка на риска

Чл. 24. (1) С цел прилагане на пропорционални на заплахите механизми за защита в общината се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложи в Наредбата.

(2) Рискове с приоритет 3 по смисъла на Наредбата - (Незначителни рискове). Рисковете с този приоритет се наблюдават и не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.

(3) Рисковете с приоритет 2 по смисъла на Наредбата - (Обичайни рискове, Непредвидени рискове). За рисковете с този приоритет 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.

(4) Рискове с приоритет 1 по смисъла на Наредбата - (Критични рискове). За рисковете с този приоритет се определят отговорни лица от общинска администрация, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

Чл. 25. (1) При анализ и оценка на риска община Ружинци използва регистър на рисковете (риск-регистър).

(2) В риск-регистъра се нанасят рискове за информационните активи, имащи отношение към обхвата на Наредбата и съответните заплахи/нежелани събития, оценката за риска, приложените и планираните мерки, срок и отговорен служител, както следва:

1. информационен актив;
2. заплахи и нежелани събития;
3. оценка на присъщия риск /последствия, вероятност/;
4. приложени мерки - процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
5. оценка на остатъчния риск /последствия, вероятност/;
6. планирани мерки - процеси/действия свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
7. срок за изпълнение на планираните мерки;
8. служител/служители, имащи отговорности към мерките.

Чл. 26. (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 общината или упълномощено от него лице 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.

Раздел III

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Политиката за мрежова и информационна сигурност на община Ружинци е разработена съгласно чл. 4, ал. 1 от Наредба за минималните изисквания за мрежова и информационна сигурност.

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

§3. Ръководителите и служителите в община Ружинци са длъжни да познават и спазват разпоредбите на настоящата Политика.

§4. Контролът по спазване на настоящата Политика се осъществява от секретаря на общината, които е и председател на Постоянната работна група по оценка на риска в общинска администрация – Ружинци

§5. Настоящата Политика е стратегически документ и е утвърдена със заповед на кмета на община Ружинци с № 229 / 27.03.2020г.



РЕПУБЛИКА БЪЛГАРИЯ
ОБЩИНА РУЖИНЦИ ОБЛАСТ ВИДИН
3930, с.Ружинци, обл.Видин, ул. „Георги Димитров” № 31
тел. 09324 /2283, факс 09324 /2604, e-mail: rujinci@abv.bg

ЗАПОВЕД

№ *229* / *27.03.2020г.*

На основание чл. 44 ал. 2 от Закона за местното самоуправление и местната администрация и чл. 4, ал. 1 от Наредба за минималните изисквания за мрежова и информационна сигурност.

УТВЪРЖДАМАМ:

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА ОБЩИНА РУЖИНЦИ

Политиката за мрежова и информационна сигурност да се публикува на интернет страницата на община Ружинци и да се доведе до знанието на служителя по мрежова и информационна сигурност в общинска администрация Ружинци и служителите имащи отношение към нея за сведение и изпълнение

Контрол по изпълнение на заповедта възлагам на секретаря на община Ружинци.



АЛЕКСАНДЪР АЛЕКСАНДРОВ
Кмет на община Ружинци

Изготвил:
инж.Пламен Гацев

Секретар на община Ружинци