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

УТВЪРЖДАВАМ:

АЛЕКСАНДЪР АЛЕКСАНДРОВ
КМЕТ НА ОБЩИНА РУЖИНЦИ
Заповед №…19…/..10..01……..2020 г.

ВЪТРЕШНИ ПРАВИЛА
ЗА
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОБЩИНСКА АДМИНИСТРАЦИЯ РУЖИНЦИ

2020 г.

Глава I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С вътрешните правила за мрежова и информационна сигурност в общинска администрация Ружинци се урежда реда и начина по който се регулира функционирането и защитата на информационните системи, и управление на рисковете за сигурността на информацията.

(2) Настоящите вътрешни правила са изготвени в съответствие с Наредбата за минималните изисквания за мрежова и информационна сигурност (ДВ, бр.59 от 26.07.2019 г.) и поредицата стандарти БДС EN ISO/IEC 27000:2017 – Информационни технологии. Мерки за сигурност. Системи за управление на сигурността на информацията.

Чл. 2. Основните цели на мрежовата и информационна сигурност са:

- **достъпност на информацията** – свойство на информацията да бъде достъпна и използваема от оторизирано лице;
- **интегритет /цялост и наличност/ на информацията** – качество на информацията за точност и пълното;
- **конфиденциалност на информацията** – свойство на информацията да не е предоставена или разкрита на неоторизирани лица.

Чл. 3. (1) Основните цели на мрежовата и информационна сигурност се постигат, чрез реализиране на мерки за управление на рисковете, предотвратяване и намаляване до минимум на въздействието на инциденти, които се групират както следва:

- организационни мерки;
- технологични мерки;
- технически мерки.

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

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

- общ контекс – вътрешна и външна заобикаляща среда;
- лидерство – засилено участие на ръководството в интегриране на системите за управление;
- процесния подход – системно идентифициране и управление на процесите и тяхното въздействие, така че да се постигнат предвидените резултати;
- мислене основано на риска.

Чл. 4. В настоящите вътрешни правила се използват следните понятия:

- **информационна система** – комбинация от информационни технологии и действия на хората, които ги прилагат за управление на процеси, вземане на решения и др. с помощта на компютърни системи;
- **информационна сигурност** – запазване на достъпността, интегритета и конфиденциалността на информацията, чрез защита на мрежите и информационните системи срещу човешки грешки, природни бедствия, технически неизправности или злонамерени атаки;
- **документирана информация** – информация, която се изисква да бъде контролирана и поддържана в организацията и носителя на които се съдържа;
- **заплаха** – потенциална причина за нежелан инцидент, преднамерено или не, които може да окаже нежелано въздействие на самата система, както и на информацията съхранявана в нея /неправомерен достъп, използване, разкриване, увреждане, промяна, преглед, запис или разрушаване/;

- **уязвимост** – слабост на актив и/или система от мерки, която може да се използва от една или повече заплахи;
- **риск** – ефект на несигурността върху целите. Рискът за сигурността на информацията е свързан с потенциала заплахите да използват уязвимостити на информационния актив и по този начин да причинят вреда на организацията;
- **управление на риска** – координирани дейности и мерки за насочване и контрол на организацията по отношение на риска.

Чл. 5. Настоящите вътрешни правила не се отнасят за сигурността на класифицираната информация и информационните активи на които тя се създава, обработва, съхранява и унищожава по смисъла на Закона за защита на класифицираната информация.

Глава II
УПРАВЛЕНИЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Раздел I
РАЗПРЕДЕЛИНИЕ ВА РОЛИ И ОТГОВОРНОСТИ

Чл. 6. (1) Ръководството на община Ружинци /кмет, заместник-кмет и секретар на община/ осъществяват ангажираност чрез:

1. гарантиране, че политиките за сигурност на информацията и целите за сигурност на информацията са установени и съвместими със стратегическите цели на общинска администрация;
2. гарантиране, че изискванията на системата за управление на сигурността на информацията са интегрирани в процесите на общинска администрация;
3. гарантиране, че необходимите ресурси за реализиране на мерките за сигурност на информацията са налични;
4. гарантиране, че системата за управление на сигурността на информацията постига предвидените резултати;
5. насочване и подкрепа на служителите да допринасят за ефективността на системата за управление на сигурността на информацията;
6. съдействие за непрекъснато подобряване.

(2) Служителя по мрежова и информационна сигурност осъществява, следните дейности:

1. идентифициране и опис на защитаваните мрежови и информационни активи;
2. идентифициране на заплахите за мрежовите и информационни активи и тяхната оценка;
3. обосновава и предлага мерки и действия за защита на информационните активи;
4. следи за реализацията на одобрените мерки и действия;
5. извършва оценка на постигнатите предвидени резултати;
6. следи за актуализиране на използвания софтуер и фърмуер;
7. следи за появата на нови киберзаплахи /вируси, зловреден код, спам атаки и др./ и предлага мерки за противодействието им;
8. уведомява за инциденти съответния секторен екип.

(3) Служителите в общинска администрация Ружинци е необходимо:

1. непрекъснато да усъвършенстват и актуализират знанията си по политиките и процедурите за сигурност на информацията;
2. с отговорни действия да гарантират ефективното и ефикасно използване на системите за управление на сигурността на информацията;
3. да разбират и осъзнават необходимостта от управление на рисковете за сигурността на информацията.

Чл. 7. Ръководството на община Ружинци разработва и приема политика за мрежова и информационна сигурност, която преразглежда редовно, и при необходимост я актуализира.

Раздел II

УПРАВЛЕНИЕ НА РИСКА

Чл. 8. (1) Управлението на рисковете за мрежовата и информационната сигурност е постоянно повтарящо се действие с което се постигат целите за сигурност на информацията и се вземат аргументирани решения.

(2) Управлението на рисковете включва прилагането на следните процеси:

1. обмен на информация и консултиране – процес на предоставяне, споделяне или получаване на информация и диалог със заинтересованите страни относно управлението на риска;
2. идентификация на рисковете – процес за намиране, разпознаване и описване на рисковете;
3. анализ на рисковете – процес на разбиране на естеството на риска и определяне на нивото на риска /последиците, които могат да причинят и вероятността за тяхното възникване/;
4. оценка на рисковете – процес на сравняване на резултатите от анализа на риска с критериите за риск, за да се определи дали рискът или неговата величина е приемлива или поносима;
5. преценка на рисковете – създава се приоритетен ред за въздействие;
6. въздействие на рисковете – процес на промяна на риска до приемливо ниво;
7. наблюдение, преглед на работата и ефективността на управление на рисковете и практикуване на непрекъснато усъвършенстване;
8. документиране на дейностите.

(3) Анализът и оценката на рисковете се извършват регулярно най-малко веднъж годишно. При изменения на вътрешните и външните условия за работа, комуникационната и информационната инфраструктура също се извършва анализ и оценка на риска.

(4) На основание на анализа и оценка на рисковете се изготвя план за намаляване на неприемливите рискове, които включва:

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.

Чл. 9. Действията по управление на риска се извършват в съответствие с Международен стандарт БДС EN ISO/IEC 27005:2017 и Стратегията за управление на риска в общинска администрация Ружинци.

Раздел III

УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИ АКТИВИ

Чл. 10. Жизнения цикъл на управление на информационните и комуникационни системи включва следните етапи:

1. придобиване;
2. въвеждане в експлоатация;
3. поддръжка;
4. преместване/изнасяне;
5. извеждане от експлоатация;
6. унищожаване на информационни системи и техните компоненти.

Чл. 11. Информационните активи/ресурси, които ще бъдат защитавани са:

- информация, база данни и файлове с данни;
- софтуерни активи- приложен софтуер, системен софтуер, програми;
- физически активи- компютърна и периферна техника, носители на данни;
- услуги извършвани от общинска администрация.

Чл. 12. За информационните активи в общинска администрация Ружинци се изготвя подробен опис. Информацията е необходима за анализ и оценка на риска, управление на уязвимости, управление на измененията и разрешаване на инциденти.

Чл. 13. Работното място на служителите в общинска администрация Ружинци се състои от работно помещение, работна маса и стол, компютърна и периферна техника, системен и приложен софтуер, база данни и информация, комуникационни средства.

Чл. 14. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл. 15. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл. 16. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off;

Чл. 17. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява служителя по мрежова и информационна сигурност, който му оказва съответна техническа помощ;

Чл. 18. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само след съгласуване със служителя по мрежова и информационна сигурност.

Чл. 19. При използване на сменяеми носители на информация за прехвърляне на файлове и данни между компютри, свързани в локалната мрежа на общинска администрация, същите да бъдат сканирани за вируси и зловреден код.

Чл. 20. По време на транспортиране носителите, съдържащи информация, трябва да бъдат защитени от неоторизиран достъп, използване не по предназначение или подправяне.

Чл. 21. Всички носители на данни се съхраняват в безопасна и сигурна среда, с ограничен и контролиран достъп.

Чл. 22. За нарушение целостта на данните се считат следните действия:

1. унищожаване на бази данни или части от тях;
2. повреждане на бази данни или части от тях;
3. вписване на невярна информация в бази данни или части от тях.

Чл. 23. На служителите на община Ружинци, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

1. да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);
2. да ги използват извън рамките на служебните си задължения;
3. да ги предоставят на външни лица без да е заявена услуга.

Чл. 24. След като повече не са необходими, носителите се унищожават сигурно и безопасно за намаляване на риска от изтичане на чувствителна информация към неупълномощени лица. Физическото унищожаване на информационните носители става със счупване. Предварително се проверят, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Раздел IV

СИГУРНОСТ ПРИ РАЗРАБОТВАНЕ И ПРИДОБИВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ

Чл. 25. (1) При разработването на проекти и технически задания на мрежови и информационни системи се включват адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска за сигурността на

информацията съгласно изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) При въвеждане на нови информационни и комуникационни системи се извършват документирани тестове, доказващи защитата на информацията от загуба на достъпност, интегритет и конфиденциалност.

Раздел V

УПРАВЛЕНИЕ НА ВЗАИМОДЕЙСТВИЯТА С ТРЕТИ СТРАНИ

Чл. 26. (1) При установяване на взаимоотношения с доставчици на стоки и услуги, наречени „трети страни" се сключва договор с изисквания за мрежова и информационна сигурност, включително

1. за сигурността на информацията и активи на общинска администрация Ружинци, свързана с достъпа на представители трети страни;
2. за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност;
3. третата страна да и способна да докаже произхода на предлагания ресурс/услуга и неговата стойност;
4. последици при неспазване изискванията за сигурност на информацията;
5. отговорност при неспазване на договорените срокове, количества и/или качество на услугата, което маже да създаде риск за постигане на целите на мрежовата и информационна сигурност;
6. взаимодействие при възникване на инцидент, които най малко включва: контактни точки, начин на докладване, време за реакция, време за възстановяване, условия за затваряне на инцидент.

(2) Страните определят, служители отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

Чл. 27. Общинска администрация Ружинци изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.

Глава III

ЗАЩИТА

Раздел I

УПРАВЛЕНИЕ НА ДОСТЪПИТЕ

Чл. 28. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

1. разделяне на потребителски от администраторски функции;
2. установяване на нива и достъп до информация;
3. регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
4. осъществяването на контрол от служители на общината.

Чл. 29. (1) Правата за достъп до конкретни информационни ресурси е според заеманата длъжност, разписани функции в длъжностната характеристика или заповед за оправомощаване. Не се задава и не се осигурява достъп на неоторизирани лица.

(2) Всеки служител има точно определени права за достъп и потребителски профил за вход в информационната система, за която е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

Чл. 30. (1) Служителят по мрежова и информационна сигурност или системният администратор на информационната система извършват необходимите настройки за достъп до информационните системи и интернет, създават потребителски имена и пароли на

служителите.

(2) Ползването на компютърната мрежа или информационната система става чрез получените потребителско име и парола.

(3) Служителите в общинска администрация са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща, чрез използване на предоставените им потребителски имена и пароли.

Чл. 31. (1) Длъжностни лица от общинска администрация Ружинци, които осъществяват достъп до регистри и/или бази данни на друг първичен администратор:

1. не споделят своите потребителски имена и пароли за достъп с трети лица;
2. използват данните само във връзка с осъществяване на правомощията, възложени от кмета на общината или в други случай, предвидени в закон;
3. съобразно класификацията на използваната информация до която има достъп я обработват, използват, съхраняват и унищожават.

(2) При системни нарушения на изискванията по ал. 1 длъжностните лица, осъществяващи достъп до регистри и/или бази данни на друг първичен администратор:

1. носят дисциплинарна отговорност;
2. временно се преустановяват правата им на достъп.

Чл. 32. Компютрите, свързани в мрежата на община Ружинци използват интернет само от доставчик, с когото община Ружинци има сключен договор за доставка на интернет.

Чл. 33. Забранява се свързването на компютри едновременно в мрежата на община Ружинци и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на община Ружинци и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ).

Чл. 34. (1) При назначаване на нов служител гл.специалист „Човешки ресурси" уведомява служителя по мрежова и информационна сигурност за осигуряване на достъп до мрежови и информационните ресурси според заеманата длъжност и разписани функции.

(2) При прекратяване на трудовото или служебното правоотношение гл.специалист „Човешки ресурси" уведомява служителя по мрежова и информационна сигурност за прекратяване на достъпа до мрежови ресурси и служебна електронна поща.

Чл. 35. Всички пароли за достъп на системно ниво се променят периодично.

Чл. 36. При необходимост от достъп до информационните активи извън мрежата, контролирана от община Ружинци:

- да се използва най-малко двуфакторна автентикация;
- да се използват канали с висока степен на защита /VPN/.

Чл. 37. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 38. (1) Подготовката и въвеждането на данни на официалната интернет страницата на община Ружинци се извършва от определен със заповед на кмета на общината служител.

(2) Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителя отговорен за качването им на официалната интернет страницата на общината.

Раздел II

НЕОТОРИЗИРАНО ИЗПОЛЗВАНЕ НА УСТРОЙСТВА

Чл. 39. За недопускане на неоторизирано използване на информационни активи и устройства собственост на община Ружинци се забранява:

1. външни лица да работят с персонални компютри на община Ружинци, освен

специалистите в случай на първоначална инсталация на компютърна техника, програми, комуникационни устройства и сервизна намеса на място, но задължително в присъствието на служителя, който ползва съответното работна място и на служителя по мрежова и информационна сигурност. При невъзможност на служителя по мрежова и информационна сигурност да присъства кмета или секретаря на общината определят за това друг служител от общинска администрация;

2. 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. 40. Лични технически средства на служителите се използват в мрежата и информационните системи на общинска администрация след уведомяване на служителя по мрежова и информационна сигурност.

Чл. 41. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп.

Раздел III

ЗАЩИТА НА СОФТУЕР И ФЪРМУЕР

Чл. 42. (1) Инсталираните версии на използвания софтуер и фърмуер на компютърните и информационни системи в общинска администрация Ружинци са лицензирани и актуалени от гледна точка на сигурността.

(2) Нови версии на софтуер и фърмуер се инсталират след одобрение на кмета на община Ружинци

(3) Служителят по сигурността на информацията поддържа библиотека с дистрибутиви на използвания софтуер и фърмуер с цел намаляване на времето за възстановяване след срив.

Чл. 43. (1) На компютърните и информационните системи в общинска администрация Ружинци не се допуска инсталирането на неодобрен софтуер и фърмуер.

(2) Служителят по мрежова и информационна сигурност осъществява контрол върху използвания софтуер и фърмуер и неговата актуалност.

Раздел IV

ЗАЩИТА ОТ ЗЛОВРЕДЕН СОФТУЕР

Чл. 44. (1) За недопускане на проникване на зловреден софтуер на компютърните и информационни системи служителите в общинска администрация при ползване на електронна поща:

1. да бъдат внимателни с прикачените файлове и линкове в писмата. Ако има прикачен файл да проверят дали подателя е автентичен и дали има логика подателя да им изпраща подобен файл;
2. да не се отварят получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg;
3. да не се отварят получени по електронна поща съобщения, които съдържат неразбираеми знаци.

(2) За недопускане на проникване на зловреден софтуер на компютърните и информационни системи служителите в общинска администрация при използването на комуникатори (като icq, skype facebook и др. подобни) се извършват действията по ал. 1.

(2) На компютрите и сървърите на общинска администрация Ружинци е забранено съхраняването на лични файлове с текст, изображения, видео или аудио.

Чл. 45. При посещение на определен сайт ако служителите забележат забавяне на бързодействието на компютърната система, да затворят сайта и да уведомят служителя по мрежова и информационна сигурност. Възможно е тези сайтове да крадат ресурси за копаене на криптовалути.

Чл. 46. С цел антивирусна защита се прилагат следните мерки:

1. всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно;
2. служителя по мрежова и информационна сигурност, а при невъзможност от негова страна системният администратор да извършват следните дейности:
   - активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
   - настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично;
   - активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
   - проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;
3. при поява на съобщение от антивирусната програма за вирус в компютърната или информационната система служителя от съответното задължително информира служителя по мрежова и информационна сигурност.

Чл. 47. Служителят по мрежова и информационна сигурност регулярно извършва оценка на ефективността на мерките за защита от зловреден софтуер и при констатирани слабости предприема действия за подобряване на защитата.

Раздел V

ФИЗИЧЕСКА СИГУРНОСТ

Чл. 48. За осигуряване на физическата защита и недопускане на неоторизиран физически достъп до информационните активи на общинска администрация Ружинци са въведени следните мерки:

1. сградата на общинска администрация е с контролиран достъп и са въведени вътрешни правила за пропускателен режим;
2. работните помещения на служителите са с контролиран достъп, заключват се в отсъствието на служителите които работят в тях;
3. за гарантиране на ефикасността на физическата защита на компютърните и информационни активи се извършва видеонаблюдение поставено в коридорите на сградата на общинска администрация.

Чл. 49. (1) Сървъри на локални компютърни мрежи и информационни системи се разполагат в самостоятелни помещения.

(2) Достъпът до помещението, където и разположен сървърът и комуникационните шкафове се ограничава по възможност само до системния администратор на информационната система, служителя по мрежова и информационна сигурност или секретаря на общината.

Раздел VI

УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 50. (1) При забелязване или установяване на слабости и уязвимости в сигурността на компютърните и информационните системи служителят които е забелязал слабостите и уязвимостите докладва на служителя по мрежова и информационна сигурност в общинска

администрация Ружинци.

(2) Служителя по мрежова и информационна сигурност осъществява:

1. анализ и оценка на слабости и уязвимости за мрежовите и информационни активи;
2. избор и обосновка на мерки и действия за защита на мрежовите и информационни активи;
3. реализация на одобрените мерки и действия;
4. оценка на степента на реализация на мерките и действията.

Чл. 51. (1) При възникване на инцидент и/или кибератака свързан с работата на компютъра, локалната или комуникационна мрежа служителят които е забелязал инцидента докладва на служителя по мрежова и информационна сигурност в общинска администрация Ружинци.

(2) Служителя по мрежова и информационна сигурност събира информация за възникналия инцидент и/или кибератаката и до 2 часа уведомява екипа за реагиране при инциденти с компютърната сигурност към Държавна агенция „Електронно управление" и ръководството на община Ружинци.

(3) Служителите в общинска администрация Ружинци изпълняват на указанията на екипа за реагиране при инциденти с компютърната сигурност към Държавна агенция „Електронно управление" и служителя по мрежова и информационна сигурност за:

- отстраняване на възникналия инцидент;
- описване на вътрешните и външните загубите;
- възстановяване дейността на компютърните и информационни системи в общинска администрация.

(4) Кметът на общината или определен от него служител информира обществеността за възникналия инцидент и/или кибератака в мрежовите и информационни системи в общинска администрация.

(5) Служителя по мрежова и информационна сигурност до 5 работни дни предоставя пълната информация за възникналия инцидент и/или кибератаката на екипа за реагиране при инциденти с компютърната сигурност към Държавна агенция „Електронно управление".

(5) Служителя по мрежова и информационна сигурност след направен анализ на инцидента и оценка на ефективността на предприетите действия по време на инцидента предлага за реализиране конкретни мерки за подобрение и ограничаване на риска до приемливи нива.

Глава IV

УСТОЙЧИВОСТ

Раздел I

СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 52. (1) Създаването на резервни копия на информационните масиви и електронните документи се извършва съгласно утвърдени правила и процедури за архивиране и възстановяване на данни.

(2) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър/компютър и да се продължи работният процес без чувствителна загуба на данни;

(3) Базите данни на следните програми се архивират всяка седмица:

- база данни на програмите Акстър;
- база данни от програма „Матеус"
- база данни от програма ЛБД „Население"
- база данни от програма "FSD"

(4) Резервните копия се съхраняват на носител, различен от този, на който са

разположени данните или електронните документи.

(5) Съхраняват се най-малко последните три резервни копия.

(6) Резервните копия се изпитват за достъпност, интегритет и конфиденциалност чрез пробно възстановяване на данни най-малко веднъж месечно.

Чл. 53. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае."

Раздел II

ПЛАНОВЕ ЗА НЕПРЕКЪСВАЕМОСТ

Чл. 54. (1) В случай на авария, природно бедствие, криза или други непредвидими обстоятелства, които биха причинили прекъсване на предоставянето на услуги от общинска администрация Ружинци се разработват планове.

(2) Плановете по ал. 1 съдържат:

1. обстоятелствата за които се отнасят;
2. праговете, при които се задействат;
3. лицето, което дава разрешение за задействането им;
4. реда за възстановяване на услугите и дейностите до определено ниво.

(3) Плановете па ал. 1:

1. се проиграват периодично, поне веднъж в годината, с цел да се провери тяхната актуалност и да се тренират служителите, които имат отговорности за тяхното изпълнение;
2. поддържат се в актуално състояние;
3. достъпни са за служителите, които имат отговорности за тяхното изпълнение;
4. съхраняват се най-малко на две места.

Чл. 55. Действията по плановете за непрекъсваемост се извършват в съответствие с Международен стандарт БДС EN/ISO 22301:2015 - Сигурност на обществото. Системи за управление на непрекъсваемостта на дейността и Закона за защита при бедствия.

Глава V
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите вътрешни правила са разработени съгласно чл. 5, ал. 1, т. 6 от Наредба за минималните изисквания за мрежова и информационна сигурност и са утвърдени със Заповед № ...19..... от ..10.01.2020.. г. на кмета на община Ружинци.

§ 2. Вътрешните правила се разглеждат и оценяват периодично, като община Ружинци може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед сигурността на информацията.

§ 3. Ръководителите и служителите в общинска администрация Ружинци са длъжни да познават и спазват разпоредбите на вътрешните правила.

§ 4. Контролът по спазване на вътрешните правилата се осъществява от секретаря на община Ружинци и директорите на дирекции.

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

№ ..19...../ 10.01.2020г.

На основание чл. 44 ал. 2 от Закона за местното самоуправление и местната администрация, във връзка с чл. 5, ал. 1, т. 6 от Наредба за минималните изисквания за мрежова и информационна сигурност.

УТВЪРЖДАМ:

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ОБЩИНСКА АДМИНИСТРАЦИЯ РУЖИНЦИ

Вътрешните правила да се публикува на интернет страницата на Община Ружинци и да се доведат до знанието на служителите от общинска администрация Ружинци и служителя по мрежова и информационна сигурност за сведение и изпълнение

Контрол по изпълнение на заповедта възлагам на секретаря на община Ружинци и директорите на дирекции.

ОБЩИНА – РУЖИНЦИ КМЕТ

АЛЕКСАНДЪР АЛЕКСАНДРОВ
Кмет на община Ружинци

Изготвил:
инж.Пламен Гацев
Секретар на община Ружинци