ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА ОБЩИНСКА АДМИНИСТРАЦИЯ БЯЛА СЛАТИНА

Версия:	1
Дата:	26.02.2020
Утвърдена със заповед:	№ 97/ 26.02.2020 г.
Изменение:	___от ____/___/___ **г.**

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл.1 Документът определя стратегическите цели на Общинска администрация Бяла Слатина за мрежовата и информационната сигурност и подхода за постигането им в съответствие с общите му стратегически и оперативни цели, нормативните актове и договорите, текущите и потенциалните вътрешни и външни заплахи за постигането на тези цели и за сигурността на информацията.

Чл.2 Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за минималните изисквания за мрежова и информационна сигурност

Чл.3 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.4 Мерки, които общинска администрация Бяла Слатина 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 общината.

Чл. 5 В общинска администрация Бяла Слатина за мрежовата и информационната сигурност е отговорен главният експерт/системният администратор в дирекция „Административно и информационно обслужване“.

РАЗДЕЛ II
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.6 Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

· разделяне на потребителски от администраторски функции;

· установяване на нива и достъп до информация;

· регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

· осъществяването на контрол от специализирани звена и служители на общината.

Чл.7 Всеки служител 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.

Чл.8 Контролът на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от Системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл.9 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.10 Всички служители използват достатъчно сложни и уникални пароли, които не се записват или съхраняват онлайн. Индивидуалните пароли не се използват съвместно с други потребители.

Чл.11 Всички пароли за достъп на системно ниво се променят на всеки три месеца.

Чл.12 Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл.13 На служителите на общинска администрация Бяла Слатина, 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.14 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.15 При изнасяне на носители извън физическите граници на общината, те се поставят в подходяща опаковка и в запечатан плик.

Чл.16 На служителите 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.17 Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до зловреден софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл.18 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 проверяват, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

Чл.19 Събирането, подготовката и въвеждането на данни на интернет страницата се извършва от оправомощени служители на общинска администрация Бяла Слатина. Длъжностните лица притежават потребителски имена и пароли за актуализиране на сайта.

Чл.20 Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се предават в електронен вид (на файлове) на служителите отговорни за публикуват им на интернет страницата на общината.

Чл.21 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.22 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.23 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.24 (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 в регистъра на информационните ресурси на ДАЕУ от определен със заповед на кмета експерт 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. 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 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 от 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.25 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, свързана 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) Общината определя служител или служители, отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

(3) Общината изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.

РАЗДЕЛ III
РАБОТНО МЯСТО

Чл.26 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл.27 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 26.08.2005г.).

Чл.28 Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения.

Чл.39 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.30 Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола.

Чл.31 Забранява се на външни лица работата с персоналните компютри на общинска администрация Бяла Слатина, освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на Системния администратор.

Чл.32 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off.

Чл.33 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява прекия си ръководител и Системния администратор, който му оказва съответна техническа помощ.

Чл.34 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.

Чл.35 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 Системния администратор.

Чл.36 Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на общинска администрация Бяла Слатина.

Чл.37 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.38 Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на неоторизиран достъп.

Чл.39 Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до Системния администратор.

Чл.40 С оглед да се намали рискът от нерегламентиран достъп, загуба или повреждане на информацията в работно и извън работно време, се прилага политика на „чисти бюра“ и „чисти екрани“. Информацията, оставена на открито върху бюрата, също така може да бъде повредена или разрушена по време на бедствия, като например пожар, наводнение или експлозия. Процесът предвижда следните мерки за контрол:

- Където е уместно, хартиените и електронните носители се съхраняват в подходящи затворени шкафове и/ или метални каси, когато не се използват и по-специално в извън работно време.
- Чувствителната или важната информация е заключена отделно в огнеупорна каса, когато не е необходима, в частност, когато офисът е празен.
- Персоналните компютри и компютърни терминали и принтери не се оставят включени в системата, когато са оставени без наблюдение и са защитени посредством ключалки, пароли и други средства за контрол, когато не се използват.
- Местата с входяща и изходяща поща, факсовете, които са оставени без наблюдение, са защитени.
- Копирните машини се заключват и са защитени от нерегламентирано използване в извън работно време.
- Чувствителната или класифицирана информация, когато се отпечатва, се сваля от принтерите незабавно.

РАЗДЕЛ IV
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.41 Системният администратор извършва необходимите настройки за достъп до локалната мрежа (DC) и интернет като създава потребителски имена и пароли за работа с компютърната мрежа и електронните пощи на общинска администрация Бяла Слатина.
Чл.42 Ползването на компютърната мрежа и електронна поща от служителите става чрез получените потребителско име и парола.
Чл.43 Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.
Чл.44 Служителите на съответните работни места 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 при използване на предоставените им потребителски имена и пароли.
Чл.45 Компютрите, свързани в мрежата на общинската администрация използват интернет само от доставчик, с който Общинска администрация Бяла Слатина има сключен договор за доставка на интернет.
Чл.46 Забранява се свързването на компютри едновременно в мрежата на общинската администрация и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Общинска администрация Бяла Слатина и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ).
Чл.47 Забранява се инсталирането и използването на комуникатори (като icq, skype, социални мрежи и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на общината и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на общинска администрация Бяла Слатина.
Чл.48 Забранява се съхраняването на сървърите на общинска администрация Бяла Слатина на лични файлове с текст, изображения, видео и аудио.
Чл.49 Забранява се отварянето без контрол от страна на системния администратор:

(1) 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 и архивни файлове;

(2) получени по електронна поща съобщения, които съдържат неразбираеми знаци.

РАЗДЕЛ V
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.50 С цел антивирусна защита се прилагат следните мерки:

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) Системният администратор извършва следните дейности:

2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

2.2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично;

2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата;

2.4. 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 работна станция, всеки служител от съответното работно място задължително информира Системния администратор и прекия ръководител.

РАЗДЕЛ VI
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.51 Следните мерки се прилагат с цел антивирусна защита:

1. Всички сървъри и устройства за съхранение на данни са свързани към устройства за непрекъсваемост на ел. захранването.

2. При липса на ел. захранване за повече от 10 мин., Системният администратор започва процедура по поетапно спиране на сървърите.

3. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра и да се изтрият локалните копия.

РАЗДЕЛ VII
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл.52 Осигурява се автоматизирано създаване на резервни копия на всички бази данни и електронни документи.

Чл.53 Информацията, включително тази, съдържаща лични данни, се резервира по следния начин:

(1) Автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите и дисковите масиви;

(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) Архивирането на базите данни се извършва съгласно Процедури за архивиране и възстановяване на данни в общинска администрация Бяла Слатина, утвърдени със заповед на кмета.

РАЗДЕЛ VIII
УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл.54 Изявяват се необходимите ресурси и се използват по организиран начин за противодействие на отрицателно въздействащи събития, свързани с надеждността и сигурността на информационните активи. Такива въздействия могат да са резултат от атаки, вируси и друг злонамерен код, опити за проникване и отказ от услуги, неразрешен достъп до или некоректно ползване на информационно-технологичните системи и данни и др.

Чл.55 Дейности, свързани с работа по инцидентите:

(1) Пробивите в сигурността на информацията се докладват от всеки служител на прекия ръководител;

(2) Работата по инцидентите се извършва от упълномощени за това служители, притежаващи необходимата подготовка и опит;

(3) Инцидентите и предприетите действия се записват и документират в „Регистър на инцидентите по сигурността“;

(4) Отстраняване на последствията от инцидента възможно най-бързо.

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

Чл.56 Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в общинска администрация Бяла Слатина. 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.57 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
2. интегритет – качество на информацията за точност и пълнота
3. наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице

Чл.58 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.59 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.60 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.61 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. оценява 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. оценява 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. оценява рискът за сигурността;
6. набелязват мерки за смекчаване на рисковете с висок приоритет.

Чл.62 При анализ и оценка на риска общината използва регистър на рисковете (риск-регистър).

Чл.63 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 информационните системи (експлоатационна и потребителска);
7. комуникационни системи;
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;
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.64 (1) За всеки от информационните активи в риск-регистъра на общината 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.65 В риск-регистъра на общината за всяка заплаха се вписва какви мерки са предприети срещу нея.

Чл.66 В риск-регистъра 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.

Чл.67 (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.68 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.69 За получаване на оценката на риска в общината се използва следната формула:

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

Чл.70 С цел прилагане на пропорционални на заплахите механизми за защита в общината се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложени в Наредбата.

Чл.71 (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 от, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

Чл.72. (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 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 X
ФУНКЦИИ НА СЛУЖИТЕЛЯ ОТГОВАРЯЩ ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в политиката на Общинска администрация Бяла Слатина

2. Участва в изготвянето на политиките и документираната информация.

3. Следи за спазването на вътрешните правила по смисъла на чл.5, ал. 1, т. 6 и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност.

4. Консултира ръководството на общинска администрация Бяла Слатина във връзка с информационната сигурност.

5. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност.

6. Периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в административното звено и ги представя на ръководителя.

7. Координира обученията, свързани с мрежовата и информационната сигурност.

8. Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства. Анализира резултатите от тях и организира изменение на плановете, ако е необходимо.

9. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.

10. Следи за акуратното водене на регистъра на инцидентите.

11. Уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл.31, ал. 1 (уведомяване за инциденти) от тази наредба.

12. Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.

13. Следи за актуализиране на използвания софтуер и фърмуер.

14. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им.

15. Организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им.

16. Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган.

17. Предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

РАЗДЕЛ XI
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в Общинска администрация – Бяла Слатина са длъжни да познават и спазват разпоредбите на тази политика.

§ 2. Контролът по спазване на правилата се осъществява от секретаря на общината и директорите на дирекции в общинска администрация – Бяла Слатина.

§ 3. Настоящата политика се разглежда и оценява периодично с оглед ефективността й, като общинска администрация Бяла Слатина може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Политиката е разработена съгласно Наредбата за минимални изисквания за мрежова и информационна сигурност (приета с ПМС № 186 от 19.07.2019 г. и обнародвана в ДВ, бр. 59 от 26.07.2019 г.) и е утвърдена със Заповед № 97 от 26.02.2020 г. на кмета на община Бяла Слатина.