ОБЩИНА БАНИТЕ, ОБЛАСТ СМОЛЯН

ОБЩИНСКА АДМИНИСТРАЦИЯ

Вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи на община Баните

Версия:	01
Дата:	05.08.2020 г.
Одобрени от:	Милен Белчев - Кмет на община Баните
Класификация:	

Раздел I

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящите правила се приемат с цел намаляване на риска от инциденти, умишлено или неумишлено предизвикани от служители на общината и във връзка с Политиката на община Баните за минималните изисквания за мрежова и информационна сигурност.

Чл.2. Наемането на работа в администрацията на община Баните се осъществява в съответствие с приложимите закони и подзаконови нормативни актове, професионалната етика и съобразно изискванията, свързани с дейността им – класификацията на информацията съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата), до която имат достъп, и предполагаемите рискове.

Чл.3. Служителите се информират за отговорностите и задълженията по отношение на сигурността на информацията при назначаване, прекратяване или промяна на служебните/договорните им отношения с община Баните.

Чл.4.Община Баните документира отговорностите на лицата с ясно определени срокове и задължения по отношение на сигурността на информацията.

Чл.5. Мрежовата и информационна сигурност се осигурява посредством:

1. подходящо професионално обучение за повишаване на квалификацията на служителите в съответствие с използваната техника и технологии;
2. периодично инструктиране на служителите за повишаване на вниманието им по отношение на мрежовата и информационната сигурност; инструктажът се прави по утвърден график и се документира по начин, гарантиращ проследяемост.

Чл.6. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от системния администратор, който контролира компютрите, имащи достъп до мрежи и мрежови услуги.

Чл.7. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не трябва да се записват или съхраняват онлайн;

Чл.8.Всички пароли за достъп на системно ниво се променят периодично. Лицата, имащи право да заявяват даване, променяне и спиране на достъп, определени във вътрешните правила, правят редовни прегледи на достъпите, но не по-рядко от веднъж в годината

Чл.9. 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.10. На служителите на община Баните, 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.11. 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.12.При изнасяне на носители извън физическите граници на община Баните, те се поставят в подходяща опаковка и в запечатан плик.

Чл.13.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.14.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.

Чл.15. Въвеждането на данни на интернет страницата на общината се извършва от служител, определен от кмета на общината. На посоченото длъжностно лице се създава потребителско име и парола за достъп, необходими за публикуването и поддържането в актуалност на данни, публикувани на сайта на общината.

Чл.16. Събирането и подготовката на данните се извършва от служители в отделните структурни звена на общината, след което данните се изпращат в електронен вид (на файлове) на служителя отговорен за качването им на интернет страницата на общината.

Чл.17. Работното място се оборудва при спазване на изискванията за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи.

Чл.19. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на правилата за мрежова и информационна сигурност.

Чл.19. 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.20. Забранява се на външни лица работата с персоналните компютри на община Баните, 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 Системният администратор.

Чл.21. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола. След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим log off;

Чл.22. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор, който му оказва съответна техническа помощ.

Чл.23. 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.24. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява системния администратор, който му оказва съответна техническа помощ;

Чл.25. 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 системният администратор.

Чл.26. 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 община Баните от лица, които не са служители в общинска администрация.

Чл.27. 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.”

Чл.28.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 несанкциониран достъп.

Чл.29. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

Чл.30. Системният администратор извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на общината.

Чл.31. Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.32. 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.33. 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.34. Компютрите, свързани в мрежата на общината използват интернет само от доставчик, с когото общината има сключен договор за доставка на интернет.

Чл.35. Забранено е свързването на компютри едновременно в мрежата на общината и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на общината и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за минималните изисквания за мрежова и информационна сигурност.

Чл.36. Забранено се инсталирането и използването на комуникатори (като icq, skype 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.

Чл.37. Забранено е съхраняването на сървърите на общината на лични файлове с текст, изображения, видео и аудио.

Чл.38. Забранено е отварянето без контрол от страна на системния администратор на:

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.

Чл.39. (1) С цел антивирусна защита всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) Системният администратор извършва следните дейности:

1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;
2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично.
3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;
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 локалната мрежа, всеки служител от съответното работно място задължително информира системния администратор.

Чл.40. Следните допълнителни мерки се прилагат с цел защита от загуба на данни:

1. всички сървъри и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.
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.

Чл.41. Служители, определени със заповед на кмета на общината осигуряват създаване на резервни копия на всички бази данни и електронни документи всеки ден.

Чл.42. (1) Информацията, включително тази, съдържаща лични данни, се резервира като 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) Базите данни на следните програми се архивират всяка вечер:

1. **база данни на програмите Акстър;**
2. **база данни от програма Матеус;**
3. **база данни от програма ЛБД Население;**
4. **база данни от програма Актопис**
5. **база данни от програма Информационно обслужване.**

(4) Споделените документи се резервират 2 пъти седмично.

(5) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

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

(7) Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

РазделII

ФУНКЦИИ НА СЛУЖИТЕЛЯ, ОТГОВАРЯЩ ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

Чл.43. Главния експерт „ИОТ и ВО“ на община Баните ръководи дейностите, свързани с постигане на изискуемото по Наредбата ниво на мрежова и информационна сигурност, и целите, заложени в Политиката за мрежова и информационна сигурност на общината.

Чл.44. За целта:

1. участва в изготвянето на политиките и документираната информация;

2. следи за спазването на вътрешните правила по смисъла на чл. 5, ал. 1, т. 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност;
3. консултира ръководството на общината във връзка с информационната сигурност;
4. ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност;
5. периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в общината и ги представя на ръководителя;
6. координира обученията, свързани с мрежовата и информационната сигурност;
7. 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;
8. поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;
9. следи за акуратното водене на регистъра на инцидентите;
10. оведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 (уведомяване за инциденти) Наредбата;
11. организира извършването на анализ на инцидентите, свързани 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;
12. следи за актуализиране на използвания софтуер и фърмуер;
13. следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им;
14. организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им;
15. организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган;
16. предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

Раздел III

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Ръководителите и служителите в общинска администрация са длъжни да познават и спазват разпоредбите на тези правила.

§2. Контролът по спазване на правилата се осъществява от секретаря на общината за гарантиране на мрежовата и информационната сигурност на използваните информационни системи в общинската администрация.

§3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като община Баните може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§4. Тези правила са разработени съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност и са утвърдени със заповедта на кмета на община Баните № РД-229 от 06.08.2020 г.