ОБЩИНА БОБОВ ДОЛ

УТВЪРЖДАВАМ:

ЕЛЗА ВЕЛИЧКОВА
КМЕТ ОБЩИНА БОБОВ ДОЛ

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

В ОБЩИНА БОБОВ ДОЛ

РАЗДЕЛ I – Общи положения

РАЗДЕЛ II – Контрол на достъпа и правила за работа с потребители

РАЗДЕЛ III – Работно място

РАЗДЕЛ IV – Ползване на компютърна мрежа и интернет

РАЗДЕЛ V – Защита от компютърни вируси и друг зловреден софтуер

РАЗДЕЛ VI – Непрекъснатост на работата

РАЗДЕЛ VII – Създаване на резервни копия

РАЗДЕЛ VIII – Заключителни разпоредби

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящите Вътрешни правила се утвърждават на основание чл. 1, ал. 1, т. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност и имат за цел осигуряването на контрол и управление на работата на информационните системи в Общинска администрация Бобов дол. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от общинската администрация или с общо предназначение.

Чл. 2 Потребителите на информационни системи в Общинска администрация Бобов дол са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3 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 (ДВ, БР. 59 от 19.07.2019 Г.)

РАЗДЕЛ II
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл. 4 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 специализирани звена и служители на администрацията.

Чл. 5 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. 6 Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско

име, осигурено от Системния администратор/ оторизираното за това лице, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7 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. 8 Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн.

Чл. 9 Всички пароли за достъп на системно ниво се променят периодично.
Чл. 10 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. 11 На служителите на Общинска администрация Бобов дол, 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. 12 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. 13 При изнасяне на носители извън физическите граници на Общинска администрация Бобов дол, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 14 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. 15 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. 16 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.17 Събирането, подготовката и въвеждането на данни на страницата се извършва от служители на Общинска администрация Бобов дол, определени със заповед на кмета на Община Бобов дол. На посочените длъжности лица се създават потребителски имена и пароли за извършване на актуализациите.

Чл.18 Събирането и подготовката на данните се извършва от служители в техния ресор, след което данните се изпращат в електронен вид (на файлове) на служителите отговорни за качването им на интернет страницата на Община Бобов дол.

РАЗДЕЛ III
РАБОТНО МЯСТО

Чл.19 Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл.20 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.21 Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения обособени за целта в сградата на Общинска администрация Бобов дол, съобразени с мерките за противопожарна защита.

Чл.22 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.23 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.24 Забранява се на външни лица работата с персоналните компютри на Общинска администрация Бобов дол, 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 изрично определен служител от Общинска администрация Бобов дол.

Чл.25 След края на работния ден всеки служител задължително изключва компютъра, на който работи, или го привежда в режим „log off";

Чл.26 При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор/ оторизираното за това лице, който му оказва съответна техническа помощ;

Чл.27 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.28 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 от Системния администратор/ оторизираното за това лице.

Чл.29 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 Бобов дол.
Чл.30 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.31 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.32 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.33 Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ IV - ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.34 Системния администратор/ оторизираното за това лице извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща в Общинска администрация Бобов дол.

Чл.35 Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл.36 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.37 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.38 Компютрите, свързани в мрежата Общинска администрация Бобов дол използват интернет само от доставчик, с когото Община Бобов дол има сключен договор за доставка на интернет.

Чл.39 Забранява се свързването на компютри едновременно в мрежата на Общинска администрация Бобов дол и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Общинска администрация Бобов дол и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредбата за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.).

Чл.40 Забранява се инсталирането и използването на комуникатори (като facebook, icq, skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на Общинска администрация Бобов дол 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 Бобов дол.

Чл.41 Забранява се съхраняването на сървърите на Общинска администрация Бобов дол на лични файлове с текст, изображения, видео и аудио.

Чл.42 Забранява се отварянето без контрол от страна на Системния администратор/ оторизираното за това лице:

(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.43 С цел антивирусна защита се прилагат следните мерки

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.
(2) Системния администратор/ оторизираното за това лице 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 на файловите системи на компютрите за вируси.

2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на системата, освен в случаите когато работата с определени продукти или услуги на други институции не изискват различни настройки;

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 локалната мрежа, всеки служител от съответното работно място задължително информира Системния администратор/ оторизираното за това лице.

РАЗДЕЛ VI
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.44 Следните мерки се прилагат с цел антивирусна защита:

1. Всички сървъри и устройства за съхранение на данни да са свързани към устройство за не прекъсваемост на ел. снабдяването.

2. При липса на ел. захранване за повече от 5 мин., задължително се уведомява Системния администратор/ оторизираното за това лице, който при необходимост 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. 45. Системния администратор/ оторизираното за това лице осигурява автоматизираното създаване на резервни копия на всички база данни и електронни документи всеки ден.

Чл. 46 Информацията, включително тази, съдържаща лични данни, се архивира 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) Базите данни на следните програми се архивират всяка вечер:

3.1. база данни от Информационната система за местни данъци и такси „Матеус“

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

4.1. база данни на деловодна система „Архимед“

4.2. база данни на програма „Локална база данни“
4.3. база данни на програма „Актопис“

(5) Споделените документи се архивират поне 2 пъти седмично.

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

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

(8) Резервните копия периодично се изпитват за консистентност и интегритет чрез пробно възстановяване на данни.

РАЗДЕЛ VIII
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

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

§ 2. Контролът по спазване на правилата се осъществява от Секретаря на Община Бобов дол и началниците на отдели.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като Общинска администрация Бобов дол 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 (в сила от 26.07.2019 г.) и влизат в сила от датата на извеждане на Заповедта на кмета на Община Бобов дол.