ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ В ОБЩИНА НЕСЕБЪР

РАЗДЕЛ I ОБЩИ ПОЛОЖЕНИЯ

Чл. 1 Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в Община Несебър. 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 (1) Потребителите на информационни системи в Община Несебър са задължени с отговорни действия да гарантират ефективното използване на системите.

(2) Отдел „Информационна сигурност“ предлага и реализира концепция за защита и опазване на електронните бази данни.

Чл. 3 Създаването, разместването, преконфигурирането на работни места в общината, на чието разположение са или се предвижда да бъдат предоставени компютърни конфигурации се съгласува с отдел „Информационна сигурност“.

Чл. 4 (1) 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 Българската национална рамка за оперативна съвместимост на информационните системи в изпълнителната власт, Наредбата за общите изисквания за мрежова и информационна сигурност и Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги.

(2) Планирането на информационни системи включително и при необходимост от взаимодействие с информационни системи извън рамките на Община Несебър се извършва от ръководителя на структурното звено и се утвърждава от зам. кмет „Бюджет и финанси“.

(3) Заявки за доставки на компютърна и периферна техника, и програмни продукти за календарната година се правят съгласно Вътрешните правила за управление на цикъла на обществените поръчки и поддържане на профила на купувача в Община Несебър: от ръководителите на структурни звена до началник отдел „УОП“ в срок до 30.11 на предходната година.

(4) При проектиране, изграждане и надграждане на информационни и комуникационни системи ръководителите на структурни звена разработват писмено

задание, което съдържа подробно описание на предвидения за компютъризиране технологичен процес, специфични изисквания към програмния продукт, входящи и изходящи данни и начини за разпространение на информацията.

(5) Техническото осигуряване с компютърна и периферна техника се избира с оглед на изискванията на програмните продукти, които ще се използват на съответното работно място, както и със състоянието и тенденциите за развитие на компютърните технологии. Поръчване на необходимо оборудване се прави съгласно Раздел „Режим на снабдяване“ от Правилника за вътрешния трудов ред на Община Несебър като заявката се съгласува с началник отдел „Информационна сигурност“.

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 общината.

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 отдел „Информационна сигурност“, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 7 (1) Ръководството на общината задава определени права на достъп до конкретни информационни ресурси, според заемната длъжност, съгласно разписани функции в длъжностната характеристика или заповед за оправомощаване. Не се задава и не се осигурява достъп на неоторизирани лица.

(2) При прекратяване на служебно или трудово правоотношение отдел „Човешки ресурси и ТРЗ“ уведомява отдел „Информационна сигурност“ за прекратяване правата на достъп до мрежови ресурси, електронната поща и при необходимост за преинсталиране на персоналния компютър на освободения от длъжност служител.

Чл. 8 Служителите, 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 Във Вътрешните правила за мерките за защита на личните данни в Община Несебър се регламентират мерки за защитата на автоматизираните информационни системи и мрежи..

Чл. 11 На служителите на Община Несебър, 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 Община Несебър 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 служебна 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 служебна 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 Публикуването на данни и информация на официалната интернет страница на Община Несебър се извършва от определен със заповед на кмета на общината служител.

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 служителя по чл. 17 от тези правила.

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 15.08.2005г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи.

Чл.21 Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45, ал. 2 от Наредба за общите изисквания за мрежова и информационна сигурност.

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 (1) Забранява се на външни лица работата с персоналните компютри на Община Несебър, освен за специалистите от софтуерните фирми, които са обработващи лични данни за Община Несебър при спазване на строга поверителност, заложена в договорните отношения.

(2) Инсталирането и актуализацията на програмни продукти се извършва в присъствието на служителя, който ползва съответното работно място.

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 отдел „Информационна сигурност“.

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 нерегламентиран 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 служител на отдел „Информационна сигурност“.

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 Община Несебър.

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 нерегламентиран достъп.

Чл.33 Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава само до специализиран по поддръжката им персонал в присъствието на специалистите от отдел „Информационна сигурност"

РАЗДЕЛ IV ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.34 Служители от отдел „Информационна сигурност" извършват необходимите настройки за достъп до интернет, създават потребителски имена и пароли за работа с компютърната мрежа и електронната поща на Община Несебър.

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 на Община Несебър използват интернет само от доставчик, с когото Община Несебър има сключен договор за доставка.

Чл.39 Забранява се свързването на компютри едновременно в мрежата на Община Несебър и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на Община Несебър или е в противоречие с изискванията на Закона за електронното управление и Наредбата за общите изисквания за мрежова и информационна сигурност.

Чл.40 Забранява се инсталирането и използването на комуникатори (като icq, skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на Община Несебър 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 Община Несебър.

Чл.41 Забранява се съхраняването на сървърите на Община Несебър на лични файлове с текст, изображения, видео и аудио.

Чл.42 Забранява се отварянето без контрол от страна на служител от отдел „Информационна сигурност“ 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

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. отдел „Информационна сигурност“ 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 система;

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 отдел „Информационна сигурност“.

РАЗДЕЛ VI НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.44 (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. отдел „Информационна сигурност“ започва процедура по поетапно спиране на сървърите.

(3) При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на персоналния 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. 45 Създаването на резервни копия на информационните масиви и електронните документи се извършва съгласно утвърдени със заповед на кмета на общината Процедури за архивиране и възстановяване на данни в Община Несебър.

Чл.46 Инциденти, свързани с информационната сигурност се отстраняват съгласно :

1. Процедура за реакция при defacement на уебсайт – приложение №1;
2. Процедура за реакция при фишинг атака – приложение №2;
3. Процедура за реакция при заразяване със злонамерен софтуер – приложение №3.

Чл. 47 (1) За всеки инцидент в информационната система на Община Несебър, който има въздействие върху непрекъснатостта на работа, началник отдел „Информационна сигурност“ уведомява екипа за реагиране при инциденти с компютърната сигурност към Държавната агенция „Електронно управление“ /контактни точки: 029492212, 0878908546, cert@govCERT.bg/. Първоначално уведомяване се прави до два часа след констатирането на инцидента. В срок до 5 работни дни се предоставя пълната информация за инцидента.

РАЗДЕЛ VII ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите в Община Несебър са длъжни да познават и спазват разпоредбите на тези правила. Настоящите правила се включват в т.I на Декларацията за информираност, която попълват всички новопостъпили служители в Община Несебър.

§ 2. Контролът по спазване на правилата се осъществява от секретаря на общината, директорите на дирекции и началниците на отдели.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед тяхната ефективност, като Община Несебър може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тези правила са разработени на основание чл.26 от Наредбата за общите изисквания за мрежова и информационна сигурност и са утвърдени със заповед на кмета на Община Несебър № 1300/16,07,2019г.

Изготвил:
Дочка Маринова – секретар на Община Несебър

Съгласувал:
Л. Борисов – началник отдел «Информационна сигурност»