ВЪТРЕШНИ ПРАВИЛА
ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
В ОБЩИНА НЕСЕБЪР

Раздел I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила имат за цел осигуряване 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.

Раздел II
КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Чл. 2. (1) Настоящият раздел е разработен на основание чл. 6 и Приложение 2 от Наредбата за минималните изисквания за мрежова и информационна сигурност и определя начина как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага Община Несебър.
(2) За класификация на информацията не се допуска използването на нивата на класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация, както и техният гриф.

Чл. 3. (1) Въз основа на важността и чувствителността на информацията, както и с цел да се гарантира достатъчна, адекватна и пропорционална на заплахите защита на тази информация, същата се разделя на 4 категории.
(2) Ръководителите на структурни звена отговарят за информацията, с която работи звеното и нейното управление: обозначение, съхранение, разпространение и унищожаване.
(3) При обмен на информация се използва класификация TLP (traffic light protocol).

ПРОТОКОЛ	ДЕФИНИЦИЯ
TLP-RED	Само за определени получатели: информация се предава устно или лично, обикновено по време на среща.
TLP-AMBER	Ограничено разпространение: получателят споделя тази информация с други служители на общината, но само ако е спазен принципът "необходимост да се знае". Източникът на информацията следва да уточни веднага след маркировката на кого може да се споделя информацията или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.
TLP-GREEN	**Широка общност**: информацията в тази категория се разпространявана широко в рамките на администрацията. Въпреки това в първоначалния й вид информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън администрацията.
TLP-WHITE	**Неограничено**: при спазване на стандартните правила за авторско право и личните данни тази информация може да се разпространява свободно, без ограничения.

(4) Категории класификация на информацията

КАТЕГОРИЯ	ОПИСАНИЕ НА ИНФОРМАЦИЯТА	СЪОТВЕТСТВИЕ С TLP
Ниво 0	• Обхваща открита и общодостъпна информация, която може да се публикувана на сайта на общината, предполага анонимно ползване на информацията и липса на средства за защита на конфиденциалността ѝ; • Оповестяването на информация не е ограничено.	**TLP-WHITE**
Ниво 1	• Споделянето на информацията е ограничено само за Община Несебър; • Информацията може да се разпространява, когато тя е полезна за осведомеността на всички участващи организации, както и за партньори от широката общност или сектор; • Получателите могат да споделят информация с партньорски организации в рамките на своя сектор или общност, но не и чрез обществено достъпни канали; информацията в тази категория може да се разпространява широко в дадена общност, но не и извън нея; • Изисквания към **информационните и комуникационните системи (ИКС)**: - достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели; - ползвателите да се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп; за установяване на идентичността трябва да се използва защитен механизъм от типа идентификатор/парола; няма изисквания за доказателство за идентичността при регистрация; - идентифициращата информация трябва да бъде защитена от нерегламентиран достъп; - доверителната изчислителна система, т. е. функционалността на информационната система, която управлява достъпа до ресурсите, трябва да поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи хода на работата; - информационната система трябва да разполага с технически и/или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система; - защитните механизми трябва да са преминали тест, който да потвърди, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.	**TLP-GREEN**
Ниво 2	• Разпространението на информация е разрешено само в рамките определени структурни звена, които са създали, обработват, съхраняват или обменят информацията; • Създателят може да използва тази класификация, когато информацията изисква защита, за да бъде ефективно обменена, и носи риск за неприкосновеността на личния живот, репутацията или операциите, ако се споделя извън общината; • Получателите могат да споделят информацията с членове на собствената си организация и с	**TLP-AMBER**

	потребители/клиенти, които трябва да са запознати с нея, за да се защитят или да предотвратят допълнителни щети; създателят на информацията има правото да определи допълнителни планирани граници на споделянето, които трябва да се спазват; • Изисквания към **ИКС** – в допълнение към изискванията към предишното ниво: - като механизъм за проверка на идентичността да се използва удостоверение за електронен подпис, независимо дали е издадено за вътрешноведомствени нужди в рамките на вътрешна инфраструктура на публичния ключ, или е издадено от външен доставчик на удостоверителни услуги; - доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти; - доверителната изчислителна система трябва да осигури взаимна изолация на процесите чрез разделяне на адресните им пространства.	
Ниво 3	• Информацията не се оповестява, разпространението й е ограничено само до лицата, които са създали, съхраняват и обработват информацията; • Информацията не се обменя с други страни, разпространението й може да доведе до въздействие върху неприкосновеността на личния живот, репутацията или операциите на дадена страна, ако с нея бъде злоупотребено; • Информацията не се споделя с която и да е страна извън конкретния обмен, обработка или съхранение; достъпът до информацията е ограничен само до лицата, участващи в обработката й. Информацията се предава лично; • Изисквания към **ИКС** – в допълнение към изискванията към предишното ниво: - като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис; - доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване; - комуникацията между потребителя и системата да се осъществява по криптирани канали, използващи протокол Transport Layer Security (TLS) поне 1.2, като минималната дължина на криптиращия ключ трябва да е поне 256 бита; - доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.	**TLP-RED**

(5) Информацията без класификация е достъпна за общо ползване при спазване на стандартните правила за авторски права и защита на личните данни, към нея не се прилагат механизми за защита.

(6) Нивото на класификацията (Ниво 1, Ниво 2 и Ниво 3) трябва да бъде нанесено върху документираната информация на всяка страница в горния десен ъгъл, освен ако няма други нормативни ограничения.

(7) При електронна кореспонденция чрез пощенски кутии (e-mail) трябва да указва нивото на информацията чрез TLP обозначенията в линията Subject и в началото самата определена

информация. Обозначението TLP трябва да е с главни букви: TLP: RED, TLP: AMBER, TLP: GREEN или TLP: WHITE. (Напр.: Subject: TLP-RED: Парола за достъп, или TLP-AMBER: Доклад от одит).
(8) При обмен на документи, нивото на класификация трябва да бъде определено чрез TLP обозначенията в горния колонтитул на всяка страница , като се изписва с главни букви.
(9) Класификацията на информацията се определя от служителя, който я създава, съгласно длъжностната му характеристика или оправомощаване от кмета, съответно от неговия пряк ръководител.
(10) Унищожаването на информацията се извършва от отговорния служител на информацията по предходната алинея, като се спазват изискванията на Вътрешните правила за дейността на учрежденския архив в общината и Номенклатурата на делата със сроковете за съхраняване. Унищожаването се извършва контролирано и надеждно, без възможност за последващо възстановяване.
(11) Мерките за съхранение и достъп на данните са реципрочни на нивото на класификация и са съобразени с нормативните изисквания, ако има такива.

Раздел III
УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ И КОМПОНЕНТИ

Чл. 4. Настоящият раздел е разработен на основание чл. 8, ал. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност и указва условията, начина и реда за придобиване, въвеждане в експлоатация, поддръжка, преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти.

ПРИДОБИВАНЕ И ВЪВЕЖДАНЕ В ЕКСПЛОАТАЦИЯ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ (ИКС)

Чл. 5. (1) При придобиване на ИКС трябва да се прилагат изискванията на раздел VI „Сигурност при разработване и придобиване на КИС“ от настоящите правила.
(2) При придобиването на системи трябва да се спазят изискванията за сигурност на веригата на доставки, където трябва да се извърши проверка на автентичността на компонентите в системата.
(3) Въвеждането в експлоатация на системите се извършва след като са преминали изпитанията, които са предварително дефинирани с конкретни изисквания за приемлив резултат. Приемливите изисквания са следствие на направената оценка на риска за идентифицираните заплахи към системата.
(4) Резултатите от изпитанията се проверяват и приемат като се състави протокол, подписан за общината от служител на отдел „Информационна сигурност“ и определения за администратор общински служител, след което системата се въвежда в експлоатация със заповед.
(5) Ако резултатите са неудовлетворителни (надвишават очакваните рисковете), системата не се въвежда в експлоатация.
(6) Записите от изпитанията се съхраняват минимум 3 г.

ПОДДРЪЖКА НА ИКС

Чл. 6. (1) За всяка придобита и въведена в експлоатация система трябва да бъде осигурена гаранционна и извънгаранционна поддръжка от доставчика.
(2) Поддръжката се извършва от квалифицирани специалисти на доставчика.
(3) При сключване на договор с доставчика, последния трябва да докаже, че служителите му притежават съответната квалификация и компетентност.
(4) Към договорите за поддръжка с доставчика следва има споразумение за ниво на услугите (Service Level Agreement), в което да бъдат дефинирани параметрите на услугите, времето за реакция и отстраняване на установени нередности.

(5) В договорите с достачиците следва да бъде включена и последващата актуализация на системите и условията за тяхното предоставяне.
(6) Поддържката на информационните системи може да се извършва и от служители на отдел „Информационна сигурност“.
(7) Всички записи, свързани с осъществяване на поддръжката на системите се съхраняват за периода на договора с доставчика. Отговорност за съхранение на записите е на отдел „Информационна сигурност“.

ПРЕМЕСТВАНЕ И ИЗНАСЯНЕ НА ИКС И КОМПОНЕНТИ

Чл. 7. (1) При необходимост от преместване на системи, отдел „Информационна сигурност“ разработва проект за преместването, като взема под внимание разписаното в раздел V „Управление на измененията в информационните активи“ от настоящите правила.
(2) Записите, генерирани в резултат на преместването се съхраняват от отдел „Информационна сигурност“ минимум 3 г.
(3) Изнасянето на информационни системи извън сградата на администрацията се извършва със заповед на кмета на общината.

ИЗВЕЖДАНЕ ОТ ЕКСПЛОАТАЦИЯ И УНИЩОЖАВАНЕ

Чл. 8. (1) Извеждане от експлоатация на ИКС се извършва след като се установи липса на възможност за нейната поддръжка и актуализация.
(2) Ако е необходимо трябва да се осигури нова съответстваща система, като се приложат разпоредбите на раздел VI „Сигурност при разработване и придобиване на ИКС“ от настоящите правила.
(3) Извеждането от експлоатация се извършва чрез бракуване от комисия, назначена от кмета на общината с участието на служители от отдел „Финансово-счетоводно обслужване“ и отдел „Информационна сигурност“.
(4) Данните от системата се архивират преди извеждането от експлоатация и се съхраняват съгласно класификационната схема определена съгласно чл. 2 от настоящите правила. След архивирането данните от системата се изтриват по начин, който не позволява тяхното възстановяване.
(5) При необходимост и с решение на комисията по ал. 3 дисковете с данни от системите не се бракуват, а се съхраняват от отдел „Информационна сигурност“.
(6) Допуска се старата и новата система да функционират паралелно с цел съпоставяне на данните и резултати.
(7) Унищожаването на дисковете след архивиране на информацията и нейното премахване от тях се извършва механично, с ръчни инструменти (дрелка, флекс, чук) от отдел „Информационна сигурност“ и се предават за рециклиране.

Раздел IV
СИГУРНОСТ НА ЧОВЕШКИТЕ РЕСУРСИ

Чл. 9. (1) Настоящият раздел е разработен на основание чл. 9 от Наредбата за минималните изисквания за мрежова и информационна сигурност, за да се определят отговорностите и задълженията по отношение на сигурността на информацията при подбор, прекратяване или промяна на служебните / трудовите отношения, професионално обучение за повишаване на квалификацията на служителите в Община Несебър
Чл. 10. (1) Назначаването на служители се извършва съобразно действащото законодателство и Правила за подбор, назначаване, атестиране, преназначаване и квалификация на персонала на Община Несебър като отдел „Човешки ресурси и ТРЗ“ съхранява служебните/трудовите досиета, където са приложени подписани от служителя Декларация за информираност, съгласно чл.5, ал. 3 от

Вътрешните правила за мерките за защита на личните данни в Община Несебър и длъжностна характеристика с разписани отговорности, в т.ч. и за конфиденциалност .
(2) Задълженията и отговорностите на общинските служители по отношение на професионалната етика и неразкриване на информация са разписани в Правилника за вътрешния трудов ред, Кодекса за поведение на служителите в общината и др. вътрешни нормативни документи, които са публикувани на интернет страницата на общината http://www.nessebar.bg/ustroistwo.html и всеки новопостъпил служител е длъжен да познава и спазва.
Чл. 11. (1) При промяна на служебните/трудовите правоотношения се прилагат изискванията по отношение на достъпите, описани в Политиката на Община Несебър за мрежова и информационна сигурност в раздел V. „Управление на достъпа и автентикацията“.
(2) Със служителя се сключва нов договор и подписва нова длъжностна характеристика.
(3) При необходимост служителят връща всички информационни активи.
Чл. 12. (1) При постъпване на нов служител от отдел „Информационна сигурност“ провеждат вътрешно въвеждащо обучение по отношение мрежовата и информационна сигурност, за което се попълва формуляр по образец, съгласно изискванията на Интегрираната система за управление на качество ISO 9001:2015, който се съхранява в трудовото/служебното досие.
(2) Вътрешно обучение на всички служители, свързано с мрежовата и информационна сигурност се провежда периодично (поне на три години) с цел повишаване на знанията и запознаване с промените в политиките и вътрешните правила. Обучението се организира от началник отдел „Информационна сигурност“, съгласувано със секретаря на общината и се провежда от компетентно лице, което може да бъде и външен за администрацията. Обученията се документират с формуляр по образец, съгласно изискванията на Интегрираната система за управление на качество ISO 9001:2015, който се съхранява в отдел „Човешки ресурси и ТРЗ“.
(3) Ръководството на общината осигурява външни обучения за професионално и служебно развитие на служителите в съответствие с използваната техника и технологии, както и за мрежова и информационна сигурност. Копия на сертификатите и удостоверенията се съхраняват в трудовите/служебните досиета.
(4) Ежегодно се оценява ефективността от проведените обучения като резултатите се вписват в Протокол от преглед от ръководството на интегрираната система за управление на качеството ISO 9001:2015.
Чл.13. (1) При прекратяване на трудово / служебно правоотношение служителят връща всички информационни активи.
(2) За да завери Обходния лист (съгласно чл. 14, ал.1 от Правилника за вътрешния трудов ред) отдел „Информационна сигурност“:
1. спира правата за достъп до информационни ресурси;
2. прибира картата за достъп до административната сграда на Общинска администрация и спира достъпа;
3. прибира за съхранение квалифицирания е-подпис (ако служителят е притежавал такъв) до момента на неговото деактивиране;
4. премахва данните на служителя от Указателя на администрацията;
5. отчислява заведените активи на служителя в Регистър на информационните ресурси.
Чл.14. Дисциплинарният процес и видовете дисциплинарни наказания за служителите, които са извършили нарушение по отношение на политиките и вътрешните правила за мрежова и информационна сигурност се определят съгласно действащата законова уредба.

Раздел V
УПРАВЛЕНИЕ НА ИЗМЕНЕНИЯТА В ИНФОРМАЦИОННИТЕ АКТИВИ

Чл.15. (1) Настоящият раздел е разработен на основание чл. 11 от Наредбата за минималните изисквания за мрежова и информационна сигурност с цел да осигури контрол върху измененията в

ИКС и обслужващата ги инфраструктура, в процесите и дейностите, в конфигурациите, в софтуера и във фърмуера на Община Несебър.
(2) Тези разпоредби позволява да се анализират и минимизират рисковете свързани с мрежовата и информационна сигурност при извършване на промени.
(3) Служителите от отдел „Информационна сигурност“ са отговорни за идентификация на измененията, оценката на риска, планиране и изпълнение.
(4) Измененията се разделят на стандартни и спешни. При стандартните изменения се следва описания в настоящия раздел процес по планиране и изпълнение. При спешните изменения се предприемат незабавни действия с цел възстановяване на дейността, след реализиран инцидент с класификация „висок“.
Чл. 16. (1) Измененията се инициират в резултат настъпили инциденти, стратегически цели на администрацията, нормативни изисквания.
(2) За всяко изменение служителите от отдел „Информационна сигурност“ извършват анализ и оценка на риска за потенциални заплахи, свързани с информационната сигурност, съгласно Стратегията за управление на риска.
(3) За всяко изменение се изготвя план на действие, срокове за изпълнение и отговорници.
(4) Определят се критерии за успешно извършени изменения.
(5) Разработва се план за връщане на системите в предишно състояние, за да намали продължителността на потенциален инцидент при неуспешно изменение.
(6) След изпълнение на ал. 2 – ал. 5, се съставя протокол. Протоколът съдържа:
1. нормативно и/или вътрешно изискване за изменението;
2. ниво на риска (нисък/среден/висок) и приоритет (стандартен/спешен);
3. засегнати системи/приложения;
4. описание на изменението;
5. план за извършване на изменението и критерии за успешно извършване на изменението;
6. план за възстановяване на предишното състояние на системите при неуспешно изменение;
7. съгласувал, одобрил, приел – име, фамилия и длъжност, подпис.
(7) Отдел „Информационна сигурност“ информира минимум 3 дни преди началото заинтересованите от предстоящото изменение страни.
(8) Служителите от отдел „Информационна сигурност“ проверяват плана за действие на изменението в тестова среда, след което преминават към оперативни действия за изпълнение на изменението.
(9) Ако изменението е неуспешно се задейства плана за връщане на предишното състояние на информационната система.
(10) Отдел „Информационна сигурност“ информира заинтересованите страни за статуса на изменението.
(11) Всички стандартни изменения се изпълняват във време, в което няма да бъде нарушен работния процес.
(12) Всички спешни изменения се изпълняват незабавно без съгласуване и одобряване.

Раздел VI
СИГУРНОСТ ПРИ РАЗРАБОТВАНЕ И ПРИДОБИВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ (ИКС)

Чл.17. Настоящият раздел е разработен на основание чл. 12 от Наредбата за минималните изисквания за мрежова и информационна сигурност, за да се определят изискванията за мрежова и информационна сигурност към ИКС в общината.
Чл. 18. (1) При определяне необходимостта от нови ИКС, свързани с дейността и предоставянето на нови административни услуги, отдел „Информационна сигурност“ трябва да разработи техническа спецификация с изисквания към системите.

(2) В изискванията за сигурност на информацията към системите трябва да се определи:
1. изискваното ниво на доверие към заявената самоличност на потребителите, за да се изведат изисквания за идентификация (автентифициране) на потребителите;
2. процесите на предоставяне на достъп и оторизиране за потребители на дейността, както и за привилегировани или технически потребители;
3. информиране на потребителите и операторите за техните задължения и отговорности;
4. изискваните нужди за защита на включените активи, в частност отнасящи се за наличност, поверителност, цялостност;
5. изисквания, извлечени от процесите на дейността, като регистриране на транзакциите и мониторинг, изисквания за неотхвърляне;
6. изисквания, налагани от други механизми за контрол на сигурността, например интерфейси към регистрирането и мониторинга или системи за откриване на изтичането на данни.
Чл. 19. (1) При придобиване на системи трябва да се следват етапи на тестване и придобиване.
(2) Тестването трябва да се извършва в изолирана тестова среда, като се използват тестови акаунти за целта.
(3) Трябва да се преразгледа оценката на риска (да се изготви риск-регистър съгласно Стратегията за управление на риска) във връзка с придобиването на новата ИКС, където да се анализират адекватността на заплахите свързани със сигурността на информацията, техните нива на риск и въведените контроли за управление на риска.
(4) На етап доставка на системите, в договорите с доставчиците трябва да бъдат включени конкретните изисквания за сигурност.
(5) Ако функционалността на сигурността в предлаганата система не удовлетворява определеното изискване, трябва да се преразгледат отново въведените рискове и свързаните с него механизми за контрол, преди да се закупи.
(6) Трябва да се преценят и внедрят наличните указания за конфигуриране на сигурността на системата / продукта, заедно с окончателния пакет софтуер / услуги на тази система.
(7) Трябва да бъдат определени критерии за приемане на продукти, от гледна точка на тяхната функционалност, които дават увереност, че са спазени идентифицираните изисквания за сигурност.
(8) Продуктите трябва да бъдат преценявани спрямо тези критерии преди закупуване. Допълнителната функционалност трябва да бъде преглеждана, за да е сигурно, че тя не внася недопустими допълнителни рискове.

Раздел VII
ДОПУСТИМО ИЗПОЛЗВАНЕ НА АКТИВИ

Чл. 20. (1) Настоящият раздел е разработен на основание чл. 5, ал. 1, т. 7 и чл. 15 от Наредбата за минималните изисквания за мрежова и информационна сигурност, за да се определят правилата за допустимо използване на информационните активи в общината и да се гарантира защитата на информацията.
(2) Разпоредбите на този раздел са задължителни за изпълнение от служителите, доставчиците и всички трети страни, които достъпват и използват активи на администрацията.
(3) Вътрешното въвеждащо обучение по чл. 11, ал. 1 от настоящите правила се извършва преди първоначално ползване на активите.

БАЗОВИ ПРАВИЛА
Чл. 21. (1) При използване на хардуер извън работните помещения на общината, същият не се оставя без надзор.
(2) Служителят трябва да следи постоянно за целостта и изправността на оборудването и да предприема мерки за опазването му от кражба и унищожаване.

(3) Служителят е длъжен да гарантира защитата и конфиденциалността на паролите за достъп.
(4) Не разрешава ползването на активите да се извършва с чужд акаунт за достъп.
(5) Паролите за достъп и оборудването не се предоставят на трети лица.
(6) При ползване на активи с дистанционен достъп, веднага след приключване на работата сесията трябва да се затвори.
(7) След приключване на работа, оборудването се изключва с изключение на основното оборудване, като сървъри, защитна стена и друго мрежово оборудване, което е необходимо за дейността на администрацията.
(8) Пренасянето на хардуер се извършва в специално препоръчаните за целта от страна на производителя чанти, раници, куфари и/или кутии, с което да се предотвратят потенциални повреди.

ИЗПОЛЗВАНЕ НА ПРЕНОСИМИ КОМПЮТРИ

Чл.22. (1) Не се разрешава да се използват лични преносими компютри в мрежата на администрацията.
(2) Всички дискове на преносимите компютри да се криптират с BitLocker.
(3) За осъществяване на отдалечен достъп до информационните ресурси и услуги на Община Несебър или на клиенти се прилага раздел VI. „Политиката за работа от разстояние“ от Политиката на общината за МИС.
(4) При ползване на безжична интернет свързаност (включително и на обществени места) трябва да се използва защитена мрежа, която има криптиране по протокол WPA2 или мобилен интернет;
(5) При транспортиране с автомобил, преносимият компютър се съхранява в багажното отделение;
(6) Не се допуска оставяне на преносимия компютър в автомобил;
(7) Преносимият компютър се инсталира със софтуер от разрешения по списъка и да конфигурира съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност, добрите практики за сигурност и настоящите правила.
(8) Използва се оригинално зарядно устройство за работа с преносимия компютър. Не се допуска използването на други зарядни устройства, извън обявените от производителя.
(9) Почистването на LCD екрана или клавиатурата се извършва с подходящи препарати и в изключено състояние.

ИЗПОЛЗВАНЕ НА МОБИЛНИ ТЕЛЕФОНИ

Чл.23. (1) Служебен мобилен телефон се получава от домакините след попълнена заявка за закупуване на канцеларски материали и офис консумативи по образец, съгласно чл.56 от Правилника за вътрешния трудов ред. Домакините чрез имейл изпращат служебния мобилен номер на служителите от отдел „Информационна сигурност“ за вписване в Указателя на администрацията. Домакините водят регистър на използваните мобилни телефони в общината с данни за служителя (имена и структурно звено), ограничение на потреблението, наличие на мобилен интернет, година на закупуване на апарата .
(2) Служебният мобилен телефон трябва да бъде защитен с парола / пин. Всеки потребител на мобилен телефон следва да се грижи за резервиране на информацията в него.
(3) Мобилните телефони не се предоставят за ползване от трети лица.
(4) Инсталирането на мобилен софтуер на телефоните следва да е съобразно политиката за защита на авторските права и съгласувано с отдел „Информационна сигурност“.
(5) Не се допуска да се сваля на мобилните телефони служебна информация от "Ниво 2" и "Ниво 3", съгласно категоризацията определена в раздел II „Класификация на информацията“ от тези правила.
(6) Не се допуска да се използват лични мобилни телефони за служебна дейност. Ако все пак се направи изключение се прилагат същите изисквания, както към служебните телефони.

(7) Служебните разговори трябва да се провеждат в изолирани условия с цел защита на информацията пред неоторизирани лица.
(8) При използване на интернет на мобилния телефон трябва да има инсталирана антивирусна програма.
(9) При ползване на безжична интернет свързаност (включително и на обществени места) трябва да се използва само мрежа, която има криптиране по протокол WPA2 и автентификация.
(10) При загуба или незаконно отнемане на служебен мобилен телефон, служителите са длъжни да уведомят незабавно домакините или секретаря на общината за блокиране на номера. Ако на загубения телефон е инсталирана служебна е-поща, служителят уведомява и отдел „Информационна сигурност“ за смяна на паролата за достъп.

ИЗПОЛЗВАНЕ НА ВЪНШНИ НОСИТЕЛИ НА ИНФОРМАЦИЯ

Чл.24. (1) За изпълнение на служебните си задължения се допуска служителите да използват външни носители USB Flash Drive, CD/DVD и външен диск, само в случаите когато са предоставени от общината.
(2) Служителите получават носителите по ал. 1 от домакините след попълнена заявка за закупуване на канцеларски материали и офис консумативи по образец, съгласно чл.56 от Правилника за вътрешния трудов ред.
(3) Не се разрешава да се изнасят външни носители, съдържащи информация от "Ниво 1" или "Ниво 2" извън сградата на администрацията, освен ако не се съхраняват архиви на други локации одобрени от кмета или секретаря на общината;
(5) Всеки служител носи персонална отговорност за съхранението на външния носител, с който работи.
(6) Не се разрешава на външен носител да се съхранява информация с „Ниво 3“ = TLP-RED;
(7) Не се разрешава да се съхраняват различни категории информация на един и същ външен носител освен при архивиране;
(8) Носителите трябва да бъдат маркирани със съответното ниво на информация, която се съхранява на тях;
(9) Преди използване на външни носители на информация, служителите са длъжни да ги проверят за вируси.

ИЗПОЛЗВАНЕ НА ПРИНТЕРИ, МУЛТИ-ФУНКЦИОНАЛНИ УСТРОЙСТВА (МФУ), ФАКС

Чл.25. (1) Не се разрешава размножаването и разпространението на документи без нужда.
(2) Не се разрешава използването на печатащите устройства за лични нужди.
(3) Забравен в скенера на споделен принтер оригинален документ, трябва незабавно да бъде предаден на секретаря на общината.
(4) Принтери и МФУ, които имат технически възможности автентикация трябва да се достъпват с PIN или карта за достъп.
(5) Забранява се от МФУ да се изпраща директно мейл със сканиран документ;
(6) Всички грешно отпечатани документи да се унищожават незабавно от служителите със шредер.
(7) Забранява се изпращането на лични данни по факс.
(8) В края на работния ден да се извършва проверка за забравени постъпили факсове.
(9) В началото на работния да се извърши проверка за постъпили факсове.
(10) Факсовете се предоставят в ЦАИО за регистриране в административно – информационната система като входящи документи.

ИЗПОЛЗВАНЕ НА ИНТЕРНЕТ

Чл. 26. (1) Всички служители имат право на достъп до интернет в работно време;

(2) Всички служители имат право на достъп до интернет базирани системи, съгласно раздел V. „Политика за достъп и автентикация“ от Политиката на общината за МИС;
(3) Забранява се използването на интернет за лични цели.
(4) Забранява се на служителите да тестват за уязвимости ИТ инфраструктурата на администрацията.
(5) На външните лица се осигурява достъп до интернет през безжичната мрежа, която е отделена от останалите като се прилага раздел V. „Политика за достъп и автентикация“ от Политиката на общината за МИС. SSID и паролата на WiFi мрежата за външни лица е поставена на видно място в Центъра за административно и информационно обслужване.

ИЗПОЛЗВАНЕ НА ЕЛЕКТРОННА ПОЩА

Чл. 27. (1) Всеки служител има право на служебна електронна поща в официално регистрирания домейн на Община Несебър: @nesebar.bg като лявата част на адреса се състои от един от следните компонента:

1. име и фамилия на служителя;
2. длъжността, която служителят заема;
3. наименованието (абревиатурата) на структурното звено.

(2) Присвояването на акаунти за достъп до служебна е-поща и администрирането на е-пощи в общината се извършва от отдел „Информационна сигурност“.
(3) Обменът на данни през е-поща се идентифицира съгласно чл. 2, ал. 7 от настоящите правила.
(4) Всеки мейл завършва с визитка, която включва: име и фамилия на служителя, длъжност, логото и името на Община Несебър, контакти – телефон, адрес.
(5) Препоръчително е в края на всеки мейл да има съобщение, определящо действията на получателя при грешно изпратен мейл;
(6) Не се отварят мейли и прикачени файлове от неидентифиициран / непознат адрес, с цел предотвратяване на вирусни атаки. При съмнения за такива мейли служителят следва да уведоми служителите на отдел „Информационна сигурност“.
(7) Достъпът до служебна е-поща може да се осъществява чрез: MAPI – MS Outlook 2016, Web mail, POP3 – при необходимост. Достъпът до служебна е-поща е допустим и на служебните мобилни устройства, ползвани от служителите.
(8) Забранява се служителят да използва за получаване и изпращане на административна информация през друга е-поща освен служебната си.
(9) Служебната е-поща не се използва за лични нужди, като интернет игри, регистрации в интернет, on-line пазаруване и други.
(10) С оглед предотвратяване надвишаването на зададения размер на пощенската кутия служителите следва да изтриват ненужните им съобщения.
(11) При напускане на служител, служебната е-поща се блокира за достъп от потребителя и по преценка на прекия ръководител (отразява се в Обходния лист) пощата се пренасочва към друг служебен адрес.
(12) Изтритата от пощенската кутия информация се пази на сървъра за срок от 14 (четиринадесет) дни.

ЕЛЕКТРОНЕН ПОДПИС

Чл. 28. (1) Електронният подпис (КЕП) е персонален за служителя и не се предоставя за ползване от друг. КЕП се издава на служител за изпълнение на задължения по длъжностна характеристика съгласно заповед на кмета на общината, съгласувана от секретаря на общината и изготвена от прекия ръководител.
(2) Оправомощени със заповед системни администратори представляват кмета на общината пред доставчиците на удостоверителни услуги и извършват вписване в регистър/списък на издадените в общината КЕП.

(3) Всеки служител следи за срока на валидност на КЕП и 30 дни преди изтичане на валидността уведомява прекия си ръководител. Прекият ръководител в срок до 14 дни преди изтичане на валидността чрез мейл информира системните администратори за предприемане действия по подновяване.
(4) Всеки служител, който използва КЕП, носи персонална отговорност за неговото съхранение и опазване от неоторизиран достъп.
(5) При напускане на работното място и след приключване на работния ден, служителят прибира USB четеца в шкаф със заключващ механизъм.
(6) При промяна на длъжността на служител, ако за същата вече не е необходимо използването на КЕП, и при прекратяване на трудовото / служебното правоотношение USB четецът се предава за съхранение в отдел „Информационна сигурност“ до момента на неговото деактивиране и отразяване в регистъра с издадените в общината КЕП.
(7) Инсталация или преинсталация на придружаващия софтуер на КЕП, конфигурация и преконфигурация се извършва от отдел „Информационна сигурност“.

Раздел VIII
ИЗПОЛЗВАНЕ И ЗАЩИТА НА СОФТУЕР И ФЪРМУЕР

Чл. 29. Настоящият раздел е разработен на основание чл. 22, ал. 5 от Наредбата за минималните изисквания за мрежова и информационна сигурност, с цел да се определят правилата за контрол и актуализация на използвания софтуер и фърмуер в Община Несебър за гарантиране на сигурността им.
Чл. 30. (1) Служителите от отдел „Информационна сигурност“ инсталират и поддържат само версии на използвания в системите на администрацията софтуер и фърмуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността.
(2) Не се допуска използване на софтуер и фърмуер, които са спрени от поддръжка по отношение на сигурността.
(3) Началник отдел „Информационна сигурност“ ежегодно планира и предлага необходимите ресурси за миграция към нови версии, като запис в Протокола от преглед на системата за управление на качеството ISO 9001:2015 от страна на ръководството. Кметът на общината утвърждава Списък с одобрения за използване софтуер, като неразделна част от Протокола от преглед на системата за управление на качеството ISO 9001:2015 от страна на ръководството.
(4) Чрез интернет страницата на Министерски съвет (msoft.goverment.bg) е осигурен достъп до библиотеката с дистрибутиви на използвания софтуер на „Майкрософт“ “, определени за държавната / общинската администрация. Началник отдел „Информационна сигурност“ поддържа акаунта на Община Несебър в Информационната система за лицензите в администрацията (ИСЛА) – достъп с потребителско име и парола.
(5) Инсталиране и актуализиране на софтуер и фърмуер се извършва само от служителите на отдел „Информационна сигурност“ и доставчици на информационни системи, които имат администраторски акаунт.
(6) На всички останали служители с потребителски акаунти е забранено да инсталират и актуализират софтуер и фърмуер.
(7) Актуализация на софтуера и фърмуера се извършва при идентифицирани нови версии, ъпдейти и пачове, които отстраняват уязвимости по сигурността, или мерки за смекчаването им, публикувани от производителите или доставчиците. Контролът се извършва от отдел „Информационна сигурност“ и доставчиците на информационни системи.
(8) Служителите от отдел „Информационна сигурност“ съхраняват off-line копие от актуалните конфигурационни файлове направени съгласно раздел X „Резервиране и архивиране на информация“ от настоящите правила. Достъпът до копията е контролиран (само за отдел „Информационна сигурност“). Копията се проверяват регулярно относно качество и годност съгласно раздел X.

(9) Служителите на отдел „Информационна сигурност“ регулярно правят проверка на конфигурационните файлове и настройките на системи и устройства за нерегламентирани изменения.
Чл. 31. (1) Забраняват се:
1. macros в office пакетите;
2. pop-up в браузерите;
3. TRACE/TRACK методът;
4. anonymous authentication;
5. TLS renegotiation в системи, използващи TLS или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия;
6. използването на AutoComplete;
7. достъпа до BIOS.

(2) Auto play функцията се конфигурира винаги да иска потвърждение на потребителя.
(3) User Account Control се конфигурира до най-високо ниво, така че винаги да издава предупреждения.
(4) При споделянето на файлове и принтери не се използва настройка Everyone, а се указва кои акаунти точно да имат право на достъп до тях.
(5) Използва се Unicast Reverse-Path Forwarding (uRPF) за предпазване от фалшиви IP адреси и rate-limiting за ограничаване на броя на заявките по IP адрес.
(6) Съобщенията за грешки в системите не трябва да дават излишна информация..
(7) Използват се приложения (add-ons) към браузърите за блокиране на рекламно съдържание.
(8) При инсталиране и конфигуриране на софтуер / фърмуер се прилагат препоръките за сигурност на съответния доставчик или производител.

Раздел IX
УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 32. (1) Настоящият раздел е разработен на основание чл. 30 и чл. 31 от Наредбата за минималните изисквания за мрежова и информационна сигурност и определя реда за идентификация на събитие, реда за категоризиране и приоритизиране на инциденти, ролите и отговорностите на служителите и трети страни при управлението на инцидентите.
(2) В раздела се използват следните понятия:
1. Събитие - идентифицирана случка по отношение на състоянието на система, услуга или мрежа, показваща възможен пробив в политиката за сигурност на информацията или отказ на защитите, или предварително неизвестна ситуация, която може да бъде свързана със сигурността.
2. Инцидент - отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията, които с голяма вероятност могат да предизвикат компрометиране на дейността на общината и целостта на базата данни, и които заплашват сигурността на информацията.
3. Значим инцидент - отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията, които могат да предизвикат катастрофални последици за дейността на общината и целостта на базата данни, и сигурността на информацията.
Чл. 33. (1) Отговорен за управлението на инциденти е отдел „Информационна сигурност“.
(2) Служителите подават сигнали за настъпили или потенциални събития, оказващи негативно влияние върху мрежовата и информационната сигурност към отдел „Информационна сигурност“ на телефон 0554/29380 или на мобилните телефони и служебните мейли на служителите в отдела.
(3) Постъпилият сигнал се описва във формуляр по образец „Уведомление за инцидент“ (Приложение 1 на настоящите правила) от служител на отдел „Информационна сигурност“.
(4) В рамките на работния ден в отдел „Информационна сигурност“ се обсъжда регистрирания инцидент, като се класифицира и се определя приоритета (съгласно Приложение 2 от настоящите

правила), анализира се и се определят мерки, които да се предприемат за прекратяване на негативното действие.
(5) За всички инциденти с висок и среден приоритет се уведомява кмета на общината.
(6) Служител на отдел „Информационна сигурност“ запознава заинтересованите страни и подателите за всички инциденти с нисък и среден приоритет и предприетите действия по прекратяване на негативното действие.
(7) Началник отдел „Информационна сигурност“ уведомява всички заинтересовани стани при установен инцидент с висок приоритет и ги информира за предприетите действия по прекратяване на негативното действие.
(8) Ефективността на предприетите мерки се наблюдава и оценява от началник отдел „Информационна сигурност“ , който определя инцидента за приключен, ако няма нови събития.
(9) Всички доказателства, свързани с инцидента (логове, snapshots, записи и др.) се събират от служителите работили по инцидента и се съхраняват в отдел „Информационна сигурност“, за да послужат за извършването на процесуални действия срещу лице или организация, ако инцидента предполага подобни искания.
(10) Достъп до записите и доказателствата, свързани с инцидентите имат кмета, секретаря, ръководителя „Вътрешен одит“ и служителите на отдел „Информационна сигурност“.
(11) Отдел „Информационна сигурност“ разработва, проверява и поддържа в актуално състояние планове за справяне с инцидентите, които биха имали най-сериозно въздействие върху мрежовата и информационната сигурност. Планът за справяне с инциденти съдържа следните данни:
1. отговорник при настъпване на инцидент;
2. ред за информиране;
3. мерки, които следва да се предприемат;
4. ред за следене на параметрите по време на инцидента.

УВЕДОМЯВАНЕ НА СЕКТОРНИЯ ЕКИП

Чл. 34. (1) При инцидент с мрежовата и информационната сигурност началник отдел „Информационна сигурност“ уведомява секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност.
(2) Първоначално уведомяване се прави до 2 часа след констатирането на инцидента. Уведомленията се подават по образец (Приложение № 7 към чл. 31, ал. 2 от Наредбата за минималните изисквания за мрежова и информационна сигурност) и съдържа информация, която дава възможност на секторния екип да определи евентуалното трансгранично въздействие на инцидента. Докладването може да се направи и чрез интернет страницата на Националния екип за реагиране при инциденти в компютърната сигурност: https://www.govcert.bg/BG/SitePages/IncidentsForm.aspx.
(3) В срок до 5 работни дни началник отдел „Информационна сигурност“ предоставя на секторния екип пълната информация за инцидента.
(4) В случай че информацията за инцидентите се изпраща по електронна поща, тя трябва да е подходящо защитена от неоторизиран достъп и да е класифицирана съгласно раздел II „Класификация на информацията“.

Раздел X
РЕЗЕРВИРАНЕ И АРХИВИРАНЕ НА ИНФОРМАЦИЯТА

Чл. 35. (1) Настоящият раздел е разработен на основание чл. 32 от Наредбата за минималните изисквания за мрежова и информационна сигурност, за да се гарантира пълнотата и наличността на информацията в общината, както и използване на изолирани тестови среди за тестване на нови информационни системи или нови версии.
(2) Процесът на резервиране на информацията обхваща всички информационни системи.

Чл. 36 (1) Информацията, подлежаща на резервиране и архивиране е описана в Матрица (електронна таблица), неразделна част от тези правила, където се определят:

1. информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира;
2. технологията, която ще се използва за архивиране и резервиране;
3. типът на резервиране (частично, пълно и др.);
4. периодът на извършване на архивирането и резервирането;
5. броят на копията, които ще се правят;
6. времето за съхраняване на всяко копие съгласно изискванията на нормативните
7. актове и оценката на риска;
8. мястото на съхраняване на всяко копие;
9. начинът на защита от неправомерен достъп (физическа и логическа);
10. случаите на използване;
11. лицето, което дава разрешение за използването.

(2 Всички изисквания в Матрицата за резервиране и архивиране на информацията са съобразени с времето, за което тя трябва да се възстанови, за да се гарантира необходимото ниво на наличност на услугата.

(3) Резервирането и/ или архивирането на информацията се извършва от служител в отдел „Информационна сигурност“.

(4) При резервирането и/или архивирането на информацията се спазват следните изисквания:

1. да се правят регулярни копия съобразно риска от загуба на информация и динамиката на изменението ѝ;
2. копията на информация да са етикетирани по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час (напр.: Backup_DC_TLP-RED_13032020-0130);
3. копията на чувствителна информация да са в криптиран вид или поне защитени с парола съответстваща на Политиката за управление на достъпите и автентикацията;
4. копията на информацията да се съхраняват на отделен сървър или сторидж, които са на същата локация и да са по възможност в друга защитена мрежа;
5. по решение на ръководството едно от копията на критична за дейността информация да се съхранява off-line на външни дискове или сървъри и по възможност в друга сграда на общинската адмиинистрация или в Център на данни. Копието може да се съхранява на нает дисково пространство с осигурена надеждна защита;
6. да се прави регулярна проверка на годността на резервните копия, дали те изпълняват целите, за които са създадени, и постига ли се необходимото време за възстановяване.

(5) Копията с информация трябва да се проверяват за тяхната годност минимум веднъж годишно, като се отчитат времената за тяхното възстановяване и съпоставят с допустимото време за прекъсване.

(6) Неуспешните тестове за въстановяване на резервните копия се изследват за причините и се избират коригиращи действия.

(7) Записите с резултатите от тестовете се съхраняват 1 година.

(8) Тестването на резервните копия се извършва в изолирана тестова среда.

(9) Архивираните база данни се изпитват веднъж месечно за консистентност и интегритет чрез пробно възстановяване.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила се преглежда за адекватност редовно от отдел „Информационна сигурност“ минимум веднъж годишно, като при необходимост се актуализира.

§ 2. Настоящите правила са утвърдени със заповед на кмета на общината №2171/02.08.2023 г.