ПОЛИТИКА НА ОБЩИНА НЕСЕБЪР
ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

I. Общи положения

Чл. 1. (1) Документът определя целите на Община Несебър за мрежовата и информационната сигурност и подхода за постигането им в съответствие с нормативните актове и договорите, текущите и потенциалните вътрешни и външни заплахи за постигането на тези цели и за сигурността на информацията.

(2) Документът реферира към вътрешните нормативни документи, свързани с използването на информационни и комуникационни системи в администрацията: Стратегията за управление на риска, Системата за финансово управление и контрол, Правилата за обмен на електронни документи и документи на хартиен носител, Правилата по защита на личните данни, Правилата за мрежова и информационна сигурност и т.н.

II. Стратегическа цел по мрежова и информационна сигурност и подходи за постигането й

Чл. 2. (1) Настоящият раздел е разработен на основание чл. 4 от Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) Контролът и осигуряване на високо ниво на информационна сигурност в Община Несебър се извършва от отдел „Информационна сигурност“.

(3) В съответствие с нормативните изисквания Община Несебър приема и внедрява комплекс от организационни, технологични и технически мерки за мрежова и информационна сигурност, които се прилагат във връзка с дейността на адмиинстрацията - предоставяне на услуги на гражданите и бизнеса.

(4) Всички нови и променени нормативни изисквания свързани с осигуряване на необходимото ниво на мрежова и информационна сигурност се идентифицират от общинските служители своевременно, като се предприемат адекватни действия за тяхното удовлетворяване и последващ контрол за ефективността им.

Чл. 3. **Община Несебър гарантира на заинтересованите страни запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи**.

Чл. 4. (1) Използваната ИТ инфраструктура от администрацията за изпълнение на дейността се контролира и поддържа с нужния капацитет и се осъвременява съобразно новите тенденции.

(2) Администрацията ефективно и ефикасно управлява всички идентифицирани процеси, оказващи влияние върху мрежовата и информационна сигурност. Ръководството на администрацията осигурява необходимото обучение и квалификация на служителите за гарантиране на мрежовата и информационната сигурност.

(3) Внедрената Стратегия за управление на риска в Община Несебър позволява да се предприемат превантивни действия към идентифицираните рискове в областта на технологиите, ИТ инфраструктурата, управлението на информационните активи, човешките ресурси и др. Началник отдел „Информационна сигурност“ идентифицира рисковете, като се вземат под внимание всички външни и вътрешни фактори, които влият

на дейността и информационната сигурност, изготвя рисковия профил на отдела чрез попълване на риск-регистър и докладва управлението на рисковете на Съвета по управление на риска.
(4) За управлението и минимизиране на последиците от непредвидени негативни събития, в администрацията са внедрени правила за управление на инциденти – Раздел IX от Вътрешните правила за мрежова и информационна сигурност в Община Несебър.
(5) Взаимоотношенията с трети страни се уреждат с договорни споразумения с клауза за неразкриване на информация или декларации за конфиденциалност, които се проверяват периодично за адекватност.
(6) Достъпът на служителите и трети страни до информация се предоставя при необходимост и съответното одобрение от оторизиран служител. За целта се прилагат мерки за сигурност определени в раздел V „Управление на достъпите и автентикацията“ от настоящия документ.
(7) Непрекъснатостта на дейността на общинската администрация се организира на основание разработения План със сценарии за възстановяване на услугите в съответните срокове. С цел адекватност на плановете същите се тетстват ежегодно.
(8) Електронните услуги се достъпват от защитения със сертификат официален уеб портал на Община Несебър: http://www.nessebar.bg/ или чрез Единния модел за заявяване, заплащане и предоставяне на електронни административни услуги: https://unifiedmodel.egov.bg/wps/portal/unified-model/for-citizens-and-businesses.
(9) Всички служители и трети страни се задължават да спазват нормативните изисквания, политиките, вътрешните правила и процедурите за мрежова и информационна сигурност.
(10) При нарушаване на вътрешните правила и политиките от служителите се прилагат разпоредбите за дисциплинарната отговорност съгласно Кодекса на труда и Закона за държавния служител, а при констатиране нарушения от трети страни се прилагат калузите от сключените договори и съответните закони.

III. Политика за взаимоотношение с трети страни

Чл. 5. Настоящият раздел е разработен на основание чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност има за цел да определи рамка на взаимоотненията на Община Несебър с доставчиците, за да се гарантира защитата на информацията.
Чл. 6. (1) Взаимоотношенията с доставчиците на стоки и услуги, имащи отношение към мрежовата и информационна сигурност на общинта се определят чрез сключване на договори и споразумения, където се описват детайлно какви достъпи и до какви информационни системи се предоставят, лицата които ще упражняват контрол върху достъпа, времето за осъществяване на дейността, мерките за физическа сигурност, които трябва да се прилагат, дефиниции за инцидент и събитие и реда за докладване и др.
(2) Договорите с доставчиците трябва да включват клаузи за конфиденциалност, в качеството им на обработващи лични данни.
(3) Достъпът на външни страни до чувствителна и критична информация или до активите се допуска само в присъствието и под контрола на компетентен служител на администрацията, при наличие на договорни отношения.

(4) Договорите трябва да включват клаузи за неустойки и съдебни мерки при нарушения на мрежовата и информационна сигурност, договорените срокове, количества и/или качество на услугата от страна на доставчиците.
(5) За определяне на взаимоотношенията с доставчиците се прилагат и нормативните изисквания на Закона за обществните поръчки и Закона за задълженията и договорите.
(6) Заявяването и предоставянето на достъп за служителите на доставчика се осъществява като се следват договорните изисквания и разпоредбите на раздел V „Политиката за управление на достъпа и автентикация“ от настоящия документ.
(7) Достъпът до информационните системи на администрацията се осъществява като се използват канали с висока степен на защита като Virtual Private Network (VPN).
(8) Доставчиците трябва да съгласуват с администрацията план за актуализацията на приложните софтуери в администрацията, като се спазят всички мерки за осигуряване на цялостност, наличност и конфиденциалност на информацията.
(9) Доставиците на ИТ услуги и стоки следва да прилагат мерки за мрежова и информационна сигурност на същото или по-високо ниво както Община Несебър, за което трябва да е способен да предостави доказателства за проведени одити или съответните сертификати.
(10) Доставчикът трябва да е способен да докаже произхода на предлагания ресурс/услуга и неговата сигурност.
(11) В договорите се определя общински служител, който трябва да следи изпълнението на договорните споразумения.
(12) В случай на неспазване на уговорените дейности и клаузи с третата страна служителят по предходната алинея изготвя докладна записка, която включва план за действие и договорът се прекратява.

IV. Политика за използване на криптографски механизми

Чл. 7. Настоящият раздел е разработен на основание чл. 4, ал. 3 и чл. 16 от Наредбата за минималните изисквания за мрежова и информационна сигурност и има за цел да определи типовете криптографски механизми и реда за тяхното използване в Община Несебър, за да се гарантира защитата на информацията.
Чл. 8 (1) За осигуряване на криптиран канал за връзка между инфраструктурата на администрацията и заинтересовани страни, с които има договорни споразумения или има нормативни изисквания се използва IPSec VPN или Open VPN.
(2) При свързване към пощенския сървър с електронните пощи на администрацията, всеки служител използва HTTPS.
(3) При трансфер на електронна поща между сървъра на администрацията и други пощенски сървъри, при възможност се използва Secure Socket Layer/Transport Layer Security (SSL/TLS) за изграждане на криптирана свързаност. Този контрол се прилага и при защитата на комуникацията с интернет портала на администрацията, както и за други сървъри, на които е необходима подобна сигурност.
(4) При необходимост от използване на удостоверителни услуги се осигуряват персонални за всеки служител квалифицирани електронни подписи (КЕП), чието използване се регламентира в Закон за електронния документ и електронните удостоверителни услуги.

(5) За защита на комуникацията в безжичните мрежи на администрацията се използва протокол WPA2, което се администрира от отдел „Информационна сигурност“.
(6) При архивиране на файлове се използва файлов архиватор 7zip, който позволява криптиране на информацията.
(7) С цел да не се съхраняват паролите в явен формат от служителите, се допуска да се използва софтуерен инструмент за защита на паролите в криптиран вид (*напр.: Dashlane, One password, Key vault, Key pass).*
(8) За предаване на данни се използват протоколите SSH и SFTP.

V. Политика за управление на достъпите и автентикация

Чл. 9. (1) Настоящият раздел е разработен на основание чл. 4, ал. 3 и чл. 17 – 19 от Наредбата за минималните изисквания за мрежова и информационна сигурност.
(2) С политиката се определят:
1. Редът за управление на правата за логически достъп (стандартни и привилегировани) на потребителите до информационни системи на Община Несебър;
2. Редът за преглед правата за логически достъп на потребителите;
3. Отговорностите на длъжностните лица при управлението на правата за достъп;
4. Правилата за избор и защита на паролите;
5. Изключения от общите правила за управление на достъпите.
(3) Политиката се отнася за всички служители и доставчици.
Чл. 10. (1) Правата за достъп за служители и доставчици се определят на принципа да са достатъчни за изпълнение на задълженията, без това да нарушава сигурността на данните в зависимост от тяхната поверителност.
(2) Управлението на потребителите, техните привилегии и автентикации се извършва от Domain Controller на Windows Server.
(3) Правата за достъп се определят в съответствие с длъжността, заемана от даден служител.
(4) Правата за достъп на доставчиците се определят съгласно предмета на дейност в сключените договори.
(5) Правата за достъп на служителите по структурни звена се определят от ръководителят на структурното звено, от заместник кметовете по ресори или от секретаря на общината. Достъпите се актуализира ежегодно и при настъпили промени. Видове достъпи:
1. Електронна поща – обем на кутията ….. MB и максимален размер на прикачен файл …. MB;
2. Active Directory – Username, "Group Membership", Локален администратор;
3. ИМЕОН - User ID, наименование на достъпните модули – достъпът се осигурява след електронно писмо на секретаря на общината;
4. Апис;
5. Национална/локална база данни „Население“ – достъп имат служителите на отдел „ГРАО“;
6. ПОЛИКОН – достъп имат служителите на отдел „Човешки ресурси и ТРЗ“ и касиер в отдел „ФСО“;
7. ПП ГРОБИЩЕН ПАРК - достъп имат служителите на отдел „ГРАО“;

8. СЧЕТОВОДНА ПРОГРАМА АЖУР-L – достъп имат служителите от отдел „ФСО“;
9. Мрежови услуги: 9.1. КЕП; 9.2. WiFi Routers; 9.3. VPN;
10. Сървъри – достъп имат служителите от отдел „Информационна сигурност“. Допуска се създаването на хранилище за данни на определено структурно звено;
11. Физически обекти – достъп до административната сграда на Общинска администрация имат всички служители, за което получават магнитна карта за достъп, издадена от системния администратор (снимка, име и фамилия, длъжност и структурно звено). Съгласно длъжностната характеристика всеки служител ползва работно място в заключващо се помещение. Достъп до сървърните помещения имат системните администратори и началник отдел „Информационна сигурност“.
(6) Създават се два типа акаунти: администраторски и потребителски.
(7) Данните за автентикацията на администраторските акаунти трябва да:
1. са различни за всяка система;
2. са с възможно най-голяма сложност, позволена от системата или нейния компонент;
3. се съхраняват на хартиен носител запечатан в плик.
(8) С цел служителите да не съхраняват паролите в явен формат, се допуска да се използва софтуерни инструменти за защита на паролите в криптиран вид, напр.: Dashlane, One password, Key vault, Key pass.
(9) Всички акаунти са персонални.
(10) Не се разрешава да се ползва чужд акаунт за достъп до информационни системи и ресурси.
Чл. 11. (1) Регистрацията и промяна в регистрацията на потребители със съответните достъпи се инициира от ръководителя на структурното звено (началник отдел / директор дирекция и др.), който изпраща мейл до отдел „Информационна сигурност“ с копие до секретаря на общината, като в него се включва следната информация: имената на служителя; длъжност; структурно звено; дата на назначаване; работен офис/кабинет; необходим достъп (електронна поща, КЕП, работа с конкретна информационна система и др).
(2) Ръководител на структурното звено попълва заявка по образец, съгласувана от началник отдел „Информационна сигурност“ и началник отдел „ФСО“ и утвърдена от секретаря за осигуряване на необходимото ИТ оборудване на служителя. При освобождаване чрез заверка на обходния лист отдел „Информационна сигурност“ и домакините от отдел „ФСО“ отнемат достъпа и отчисляват ИТ оборудването.
(3) Системният администратор осигурява необходимото ИТ оборудване, инсталира и конфигурира.
(4) Системният администратор създава / деактивира акаунта на служителя със съответните достъпи до информационните системи и ресурси.
(5) Домакин от отдел „ФСО“ предава първичните счетоводни документи на ИТ оборудването в отдел „ФСО“ и сканирани копия на системния администратор за завеждане в Регистъра на информационните ресурси.
(6) Системен администратор предоставя на служителя потребителското име и паролите за достъп до информационните системи и ресурси. Паролите се създават като временни и следва да бъдат сменени при първоначално влизане от служителя.

(7) При създаване на потребителското име се прилага следната конвенция: напр. Иван Димитров – ivan.dimitrov (име и фамилия). При наличие на повторение на име и фамилия, се добавя и инициала от презимето, напр.: Иван Стоянов Димитров – ivan.s.dimitrov. Допуска се служителите на едно структурното звено да ползват обща електронна поща.
(8) Системен администратор провежда обучение на служителя за работа с ИТ оборудването и информационни системи и допустимото им използване.

VI . Политика за работа от разстояние

Чл. 12. (1) Настоящата политиката е разработена на основание чл. 4, ал. 3 и чл. 20 от Наредбата за минималните изисквания за мрежова и информационна сигурност.
(2) Политиката се отнася за всички с отдалечен достъп до информационните ресурси на Общинската администрация – служители, кметства, второстепенни разпоредители с бюджет, както и доставчици, които предоставят услуги по поддръжка на информационната и комуникационна инфраструктура и системи.
Чл. 13. (1) Заявяването и предоставянето на достъп за работа от разстояние на служител или доставчик се осъществява като се следват договорните изисквания и раздел V. „Политиката за управление на достъпа и автентикация“.
(2) За достъп до информационната система на администрацията от кметствата и второстепенните разпоредители с бюджет се използват канали с висока степен на защита като Virtual Private Network (VPN).
(3) Отговорността за внедряването, поддръжката и контрола на прилагане на мерките за информационна сигурност е на служителите от отдел „Информационна сигурност“.
(4) При необходимост от достъп до информационни активи извън мрежата, контролирана от Общинската администрация, се:

- използва най-малко двуфакторна автентикация;
- използват Virtual Private Network (VPN);

(5) При работа от разстояние не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.
(6) При работа от разстояние се използва надеждна интернет връзка, като за безжичен достъп се изисква да се използва протокол WPA2.
(7) За дистанционна работа да се използват служебни преносими компютри (лаптопи).
(8) При използване на лични технически средства за работа от разстояние се прилагат технически мерки за защита определени за администрацията, като задължително се създава отделен профил за достъп до компютърната конфигурация.
(9) Забранява се свалянето и съхранението на данни с категория „Ниво 2“ и „Ниво 3“ локално на личен хардуер при работа от разстояние.
(10) Обработването на информацията да се извършва само на сървъри на Общинската администрация.
(11) При необходимост от дистанционна работа, на потребителя може да се определи времеви диапазон за достъп до информационните ресурси.
(12) Не се допуска запаметяване на данните за удостоверяване при свързване през VPN.
(13) Всички логовете на работещите от разстояние се съхраняват минимум 1 г.

(14) Всички работни станции и мобилни компютри, които се свързват от разстояние трябва да бъдат защитени с антивирусни програми.
(15) Дисковете на мобилните компютри, които се използват за дистанционна работа, за целта трябва да бъдат с включен BitLocker.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите политики се преглежда за адекватност редовно от отдел „Информационна сигурност“ минимум веднъж годишно, като при необходимост се актуализират.
§ 2. Настоящите политики са утвърдени със заповед на кмета на общината №2171/02.08.2023 г.