ОБЩИНА ДОСПАТ
4831, гр. Доспат, обл. Смолян
ул. „Кап. Петко Войвода" № 3
Тел.: 03045/23 10, факс: 03045/ 23 12

MUNICIPALITY OF DOSPAT
4831, Dospat, Smolian Region
3 „Kap. Petko Voivoda" Str.
Phone: 03045/23 10, Fax: 03045/ 23 12

Web: www.dospat.bg, e-mail: obshtina.dospat@dospat.egov.bg

Вътрешни правила за дейностите, свързани с администрирането, експлоатацията и поддръжката на хардуер и софтуер в община Доспат

Версия: 1

Дата:

Одобрени от:

Инж. Елин Радев – кмет на Община Доспат

ОБЩИНА ДОСПАТ КМЕТ гр.Доспат

Класификация: За служебно ползване

Раздел I

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящите правила касаят процеса на управление на жизнения цикъл на информационните и комуникационните системи и техните компоненти в рамките на община Доспат.

Чл.2. Условията, начинът и редът за придобиване, въвеждане в експлоатация, поддръжка, преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти в община Доспат са в компетенциите на секретаря на общината.

Чл.3. Описът на информационните активи по смисъла на чл. 5, ал. 1, т. 1 от Наредбата за минималните изисквания за мрежова и информационна сигурност (Наредбата), съдържа информация, необходима за разрешаването на инциденти, анализ и оценка на риска, управление на уязвимости и управление на измененията, като:

1. еднозначна идентификация, като инвентарен, сериен номер или др.;
2. основни характеристики;
3. услуги, процеси и дейности, в които участва;
4. местоположение;
5. година на производство, където е приложимо;
6. дата на въвеждане в експлоатация, където е приложимо;
7. версия, където е приложимо;
8. местонахождение на свързаната с него документация (техническа, експлоатационна, потребителска и др.);
9. отговорно лице.

Чл.4. (1) Настоящите правила са приети в съответствие с изискването на чл. 5, ал. 1, т. 6 от Наредбата с цел намаляване на риска от инциденти, настъпили в резултат на изменения във важните за дейността информационни активи, и по-точно в информационните и комуникационните системи и обслужващата ги инфраструктура, в процесите и дейностите, в конфигурациите, в софтуера или във фърмуера.

(2) Преди извършването на изменения, изрично оправомощени служители на общината правят анализ и оценка на риска за всеки конкретен случай и в съответствие с чл. 7 от Наредбата.

(3) Измененията се:

1. планират, като се определят срокове и отговорности за всяка дейност, която ще бъде извършена преди, по време на и след изменението;
2. съгласуват предварително с всички страни, имащи отговорности към процесите и дейностите в обхвата на наредбата;

3. одобряват от административния орган, или от изрично упълномощено от него лице;
4. оповестяват по подходящ начин на всички страни, които са заинтересовани;
5. информирането на заинтересованите страни трябва да е поне 3 дни преди да се направи изменението;
6. проверяват в тестова среда.

(4) Общината разработва план за връщане на системите в предишното им състояние, за да се намали продължителността на потенциален инцидент, настъпил в резултат на изменението.

Чл.4. (1) При разработване на проекти и технически задания общината включва адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване.

(2) Изготвените технически задания/спецификации по ал. 1 се вписват в регистъра по чл. 51 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги и се утвърждават съгласно чл. 53 от същата Наредба от председателят на ДА "Електронно управление" или определено от него длъжностно лице, в срок две седмици след вписването им.

(3) Общината въвежда в експлоатация нови информационни и комуникационни системи планирано и след успешно проведени и документирани тестове, доказващи защитата на информацията от загуба на достъпност, интегритет и конфиденциалност.

Чл.5. (1) Общината поддържа информационна и комуникационна инфраструктура, която гарантира, че информационните и комуникационните системи, изпълняващи различни функции, са разделени и изолирани помежду си физически и/или логически, както и че са разделени и изолирани от информационните и комуникационните системи на трети страни, с цел да се ограничи разпространението на инциденти с мрежовата и информационната сигурност.

(2) В случай че дадена система е съставена от подсистеми, разделянето им се осъществява на последно физическо или логическо ниво, като уеб сървърът, сървърът с приложния софтуер и сървърът с базата данни на една информационна система се разполагат на различни машини и в различни мрежи.

Чл.6. (1) Общината гарантира, че трафикът между отделните системи и техните подсистеми е контролиран чрез подходящо филтриране (по IP адрес, по протокол, по номер на порт от Transmission Control Protocol (TCP)/Internet Protocol (IP)) с цел превенция на евентуални атаки и ограничаване на разпространението на инциденти. Филтрирането на трафика трябва да бъде по предварително разписани и одобрени **правила**, основаващи се на функционалността и сигурността, които трябва да бъдат редовно проверявани за нерегламентирани изменения и да бъдат актуализирани с оглед на нововъзникващи заплахи.

(2) Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) се забраняват чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.

Чл.7. (1) Общината приема ясно дефинирани политики относно неоторизираното използване на:

1. лични технически средства в мрежата, която контролират;
2. преносими записващи устройства.

Чл.8. (1) Общината прилага следните мерки за защита на профилите с административни права за информационните и комуникационните системи и техните компоненти:

1. преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;
2. администраторските профили са персонални;
3. администраторските профили се използват само за административни цели;
4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);
5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;
6. данните за автентикацията на администраторските акаунти:
7. са различни за всяка система;
8. са с възможно най-голяма сложност, позволена от системата или нейния компонент;
9. се съхраняват подходящо физически и логически защитени, като достъп до тях има само оторизиран представител на [конкретна за всяка община структура: дирекция, отдел или служител];
10. поддържа списък на администраторските профили за информационните и комуникационните системи и техните компоненти;
11. при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини правата на административния му акаунт се спират за съответния период;
12. поне веднъж годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.

(2) Паролите за автентикация на администраторските профили се сменят задължително:

1. периодично – най-малко веднъж в годината;
2. при прекратяването на договорните или служебни отношения със служители или трети страни, на които тези данни са били известни;
3. при пробив в мрежовата и информационната сигурност.

(3) Всички операции, процеси и дейности в информационните и комуникационните системи и техните компоненти, извършени с администраторски права, се документират по

смисъла на чл. 5, ал. 3 и 4 от Наредбата за всеки администраторски профил и в съответствие с изискванията на чл. 29, ал. 2, 4, 5 и 6 от Наредбата.

(4) В документацията по ал. 3 не се въвеждат и не се съхраняват пароли на административен профил под формата на явен текст или хеш.

Чл.9. (1) Общината използва отделна, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти. Тази среда е изолирана от другите информационни и комуникационни системи на общината и от интернет и не се използва за други цели.

(2) В случай че администрирането на информационните и комуникационните системи и техните компоненти не се осъществява през средата по ал. 1, потоците на тази информация са защитени чрез механизми за удостоверяване и криптиране.

Чл.10. (1) Общината дава достъп до информационните и комуникационните си системи на потребител или автоматизиран процес само когато този достъп е строго необходим на потребителя, за да изпълни задълженията си, или на автоматизирания процес да извърши необходимите технически операции. За да гарантира, че достъп до информационните и комуникационните му системи имат само оторизирани потребители, устройства (включително други информационни системи) и автоматизирани процеси, общината определя:

1. правата на достъп до конкретни информационни активи на служителите според длъжността им;
2. реда за заявяване, промяна и прекратяване на достъп;

(2) Общината прилага задължителни мерки за автентикация, оторизация и одит на компютърните мрежи и системи, които включват и изисквания за определена сложност на данните за автентикация, ако се използват пароли те:

1. следва да съдържат малки и големи букви, цифри и специални символи;
2. са дълги не по-малко от 8 символа за потребителските и 12 символа за администраторските профили;
3. паролите на потребителските акаунти се сменят регулярно на период не по-голям от шест месеца;

(3) Общината гарантира, че потребителските профили са индивидуални;

(4) В ежедневната работа се използват профили с най-ниското ниво на достъп, което дава възможност за изпълнение на служебните задължения;

(5) Общината гарантира, че лицата, имащи право да заявяват даване, променяне и спиране на достъп, определени съгласно ал. 1, правят редовни прегледи на достъпите, но не по-рядко от веднъж в годината;

(6) При тези прегледи се установява дали всички, на които е даден достъп до мрежата, до отделните системи и/или приложения, имат право на него в съответствие със служебните им задължения, дали външни лица имат достъп и какъв е той (бивши служители, представители на трети страни);

(7) За целите на прегледите администраторите на съответните информационни и комуникационни системи предоставят на оправомощените по ал. 1 лица списък на всички, които имат достъп до системата и нивото на достъпа, а оправомощените лица документирано потвърждават или дават указания за промяна;

(8) Общината ограничава даването на привилегирован достъп (по-високо ниво на достъп или достъп до система, до която лицето не трябва да има достъп); привилегированият достъп се дава само за определен период и действията с него се контролират;

(9) Общината гарантира, че достъпът до споделени файлове и принтери е разрешен само от мрежата, контролирана от бщината.

Раздел II

ЗАЩИТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл.11. При необходимост от достъп до информационни активи извън мрежата, контролирана от общината, се спазват изискванията на чл. 19 от Наредбата, включително:

1. се използва най-малко двуфакторна автентикация;
2. се използват само канали с висока степен на защита като Virtual Private Network (VPN);
3. не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

Чл.12. (1) За намаляване на риска от инциденти, предизвикани от технически повреди на системите, общината:

1. осигурява климатико-механичните условия, указани от производителя;
2. осъществява наблюдение на параметрите на условията по т. 1;
3. провежда планирана регулярна техническа профилактика на устройствата.

(2) За намаляване на риска от неоторизиран достъп, общината разполага устройствата в зони, които са физически и логически защитени в съответствие с класификацията на информацията, с която работят.

Чл.13. (1) Общината инсталира и поддържа само версии на използвания в системите софтуер и фърмуер, които се поддържат от доставчиците или производителите и са актуални от гледна точка на сигурността.

(2) Кметът на общината, одобрява софтуера, който се използва в информационните и комуникационните системи.

(3) Общината поддържа библиотека с дистрибутиви на използвания софтуер и фърмуер с цел намаляване на времето за възстановяване на дадена система след срив.

(4) Общината предприема мерки за:

1. недопускане на инсталирането и използването на неодобрен софтуер и фърмуер;
2. контрол върху използвания софтуер и фърмуер, включително неговата актуалност.

(5) Общината приема вътрешни правила и инструкции за регламентиране на действията по:

1. поддържане на библиотеката с дистрибутиви на използвания софтуер и фърмуер в актуално състояние;
2. управлението на достъпа до нея;
3. проследяване за новооткрити уязвимости в сигурността на използвания в системите софтуер и фърмуер и за техни актуализации (нови версии, ъпдейти и пачове), които отстраняват тези уязвимости, или мерки за смекчаването им, публикувани от производителите или доставчиците;
4. придобиване и проверка на произхода и целостта на актуализацията преди инсталирането й;
5. прилагането на актуализациите и препоръчаните мерки, които трябва да се извършват съобразно разпоредбите на Наредбата.

(6) Общината гарантира, че устройствата и системите са конфигурирани в съответствие с препоръките за сигурност на съответния им доставчик или производител, като се приложат и изискванията на приложение № 4 от Наредбата.

(7) Общината съхранява off-line копие от актуалните конфигурационни файлове и/или описание на настройките, като достъпът до тях трябва е контролиран. Копията се проверяват регулярно относно качество и годност.

(8) Общината регулярно прави проверка на конфигурационните файлове и настройките на системи и устройства за нерегламентирани изменения.

Чл.14. (1) Общината прилага в информационната и комуникационната си инфраструктура подходящи мерки за защита от проникване и мерки за откриване и справяне със зловреден софтуер.

(2) Мерките за защита от зловреден софтуер:

1. са приложени към всички компоненти на информационните и комуникационните системи, където това е възможно;
2. се поддържат в актуално състояние, за да имат способността да защитават от новооткрити заплахи.

(3) Мерките за защита от зловреден софтуер позволяват:

1. извършване на пълна проверка за наличие на зловреден софтуер поне веднъж в седмицата, където е приложимо;
2. проверка на електронната поща и файлове, свалени от интернет, както и преносими записващи устройства, преди да бъдат отворени.

(4) Общината извършва регулярно оценка на ефективността на мерките за защита от зловреден софтуер и при констатирани слабости предприема действия за подобряване на защитата.

Чл.15. (1) Общината има разработени политика и вътрешни правила съгласно чл. 5, ал. 1, т. 6 от Наредбата за прилагане на криптографски механизми, които се използват за гарантиране на конфиденциалността и интегритета на чувствителната информация в съответствие с нейната класификация.

(2) Криптографските механизми са съобразени с уязвимостта на информацията към заплахи за нейните конфиденциалност и интегритет и с нормативните и регулаторните изисквания към нейното създаване, съхраняване и пренасяне.

Чл.16. Общината предприема следните мерки за защита на уеб сървърите:

1. инсталира сертификат на уеб сървърите си, издаден от доверена система за сертифициране (trusted certification authority system), който:

а) е издаден за съответния уеб сайт (website) или група сайтове и е уникален;

б) използва алгоритъм за криптиране поне SHA2;

в) е актуален, като сертификатите с изтекъл срок се анулират;

2. за защита на интегритета на информацията, обменяна с потребителите, уеб сайтът (website) на общината е достъпен само по протокол Hypertext Transfer Protocol Secure (HTTPS), като се използват само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г., или следващи по-нови версии;
3. за криптиране на информацията, обменяна между уеб сървъра и потребителите му, се прилагат изискванията на чл. 16 от Наредбата и се вземат предвид публикуваните в RFC на IETF забрани за използване на методи за шифриране в криптографските транспортни протоколи;
4. прилага подходящ Web Application Firewall (WAP), който наблюдава и филтрира трафика от и към съответното приложение с цел защита на уеб приложенията от кибератаки от типа Cross-Site Request Forgery (CSRF), Cross-site Scripting (XSS), file inclusion, SQL injection и др.;

5. не се позволява вмъкване на данни от страна на потребителя, освен на определените за това места;
6. всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент, биват валидирани;
7. приложният софтуер не позволява въвеждане на специални символи, особено такива, които се използват в SQL заявките;
8. всички данни, изпращани от клиента и показвани в уеб страница, са кодирани с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript;
9. за защита от атаки от типа отказ от услуги (DoS):

а) се налага ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по Url;

б) се конфигурират типът и размерът на headers, които уеб сървърът ще приеме;

в) се ограничават времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка, за да се минимизира въздействието и на slow HTTP атаки;

10. за защита от brute force атаки се въвежда ограничение на броя неуспешни опити за влизане в системата;
11. не се извежда списък на уеб директориите;
12. бисквитките (cookies) да имат:

а) флаг за защита (security flag) – този флаг инструктира браузъра, че "бисквитката" може да бъде достъпна само чрез защитени SSL канали;

б) флаг HTTP only – инструктира браузъра, че "бисквитката" може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента;

13. headers на отговорите на заявки, които трябва да гарантират защита както на клиента, така и на уеб сайта (website), съдържат опции, посочени в приложение № 5 от Наредбата;
14. в главната директория на уеб сайта (website) е сложен файл robot.txt, който дава указания на уеб роботите (ботове/паяци) колко често да обхождат сайта, както и кои части от него да обхождат и да индексират; ако този файл не съществува, уеб роботите обхождат целия сайт – всяка една негова страница, подстраница, статия, линк и т.н., което крие риск за конфиденциалността на информацията;
15. при използване на Система за управление на съдържанието (CMS) се променя наименованието по подразбиране на папката за достъп до администраторския панел.

Чл.17. Общината предприема следните мерки за защита на DNS:

1. при използване на повече от един DNS сървър, всеки от тях да е разположен в различна мрежа/подмрежа;
2. да прилага DNSSEC (Domain Name System Security Extensions);
3. да минимизира DNS заявките съгласно RFC 7816 на IETF от 2016 г.;
4. да забрани zone-transfers – злонамерени лица могат бързо да определят всички хостове в определена зона чрез трансфери на DNS зони, да събират информация за домейна, да избират цели за атаки, да откриват неизползвани IP адреси и да заобикалят мрежовия контрол на достъпа, за да крадат информация;
5. в конфигурационния файл да сложи:

а) dmarc (Domain-based Message Authentication, Reporting and Conformance) запис;

б) SPF (Sender Policy Framework) запис.

Чл.18. (1) Общината осигурява физическа защита на информационните си активи чрез прилагане на адекватни и пропорционални мерки срещу заплахи от неоторизиран физически достъп до тях. Мерките трябва да гарантират наличността, интегритета и конфиденциалността на информационните активи.

(2) Общината осигурява защита на информационните си активи от пожар, наводнение, химическа и физическа промяна на въздуха чрез подходящи мерки в съответствие с нормативните актове.

(3) За да гарантира ефикасността на приложените мерки по ал. 1 и 2, общината извършва подходящо наблюдение върху тях.

Чл.19. В случай че общината използва индустриални системи за контрол, от функционирането и сигурността на които зависят съществените услуги, които предоставя, тя прилага подходящи мерки за тяхната защита в съответствие с изискванията на Наредбата, ако са приложими.

Чл.20. (1) Общината използва система/системи за автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за нейната дейност системи, чрез анализ на информационни потоци, протоколи и файлове, преминаващи през ключови устройства, позиционирани така, че да могат да анализират всички потоци, обменяни между собствените им информационни и комуникационни системи, както и с информационните и комуникационните системи на трети страни.

(2) Общината организира чрез инструкции действията за наблюдение и реакция на сигналите от тези системи.

Чл.21. По отношение на системните записи общината гарантира, че:

1. в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово

оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;

2. в записите за всяко от тези събития е отбелязано астрономическото време, когато е настъпило събитието;
3. всички компоненти на системите поддържат единно време в съответствие с изискванията на:

а) стандарти БДС ISO 8601-1 "Дата и време. Представяния за обмен на информация. Част 1: Основни правила" и БДС ISO 8601-2 "Дата и време. Представяния за обмен на информация. Част 2: Разширения"; времето за настъпването на събития с правно или техническо значение се отчита с точност до година, дата, час, минута и секунда, а при технологична необходимост се допуска и отчитане до милисекунда;

б) за синхронизация на часовниците на компоненти на информационните и комуникационните системи трябва да се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;

4. достъпът до информацията по ал. 1 е ограничен само до лица, имащи задължения за наблюдението по смисъла на чл. 30 от Наредбата, за разрешаването на инциденти с мрежовата и информационната сигурност, за разкриването и разследването на тежки престъпления и престъпления по чл. 319а – 319е от Наказателния кодекс в съответствие с чл. 14, ал. 4, т. 2 и чл. 15, ал. 3, т. 3 от Закона за киберсигурност. Достъпът до тази информация трябва да е само за четене;
5. информацията по ал. 1 се архивира и се съхранява за период не по-малък от дванадесет месеца при спазване на изискванията на чл. 32 от Наредбата;
6. общината да е в състояние да извършва корелация на информацията по ал. 1 от различните източници и да прави анализ, за да открият събития, които засягат мрежовата и информационната сигурност.

Чл.22. Във връзка с възникване и управление на инциденти с мрежовата и информационна сигурност:

1. служителите подават сигнал за настъпили или потенциални събития, оказващи негативно влияние върху мрежовата и информационната сигурност до [конкретна за всяка община структура: дирекция, отдел или служител];
2. кметът определя със заповед лице, отговорно за регистъра на инцидентите;
3. с утвърдена от Кмета инструкция се определят реда за регистриране на сигнали, проверката на тяхната достоверност, класифицирането им, тяхното приоритизиране и последващото уведомяване за това на подателя;
4. за инцидента се уведомяват преките ръководители на лицата подали сигнала;
5. информацията за начина за разрешаване на инцидента се подава в писмен вид;
6. инцидента се документира до приключването му;

7. съхраняването и предаването на доказателства, когато инцидентът предполага извършването на процесуални действия срещу лице или организация, включително необходимите за това записи се извършва в писмен вид;
8. достъпът до регистъра на инцидентите е ограничен. Лицата, имащи достъп до него се определят със заповед на кмета.

(3) Общината разработва, проверява и поддържа в актуално състояние планове за справяне с инцидентите, които биха имали най-сериозно въздействие върху мрежовата и информационната сигурност. Плановете съдържат информация за:

1. отговорника за организацията при настъпване на инцидент;
2. реда за информиране;
3. мерките, които следва да се предприемат и отговорното за това лице;
4. реда за консултиране;
5. реда за следене на параметрите по време на инцидента;
6. лицето, което ще събира и съхранява необходимата информация, и др.

(4) Общината разработва стратегия за комуникация, която определя реда за споделяне на информацията за инцидента със служители, партньори, доставчици, клиенти, медии, държавни органи.

Чл.23. (1) При инцидент с мрежовата и информационната сигурност служител от [конкретна за всяка община структура: дирекция, отдел или служител], отговарящо за мрежовата и информационната сигурност, уведомява съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите в сроковете, посочени в чл. 21, ал. 4 и 5 и чл. 22 от Закона за киберсигурност.

(2) За уведомяването по ал. 1 и по чл. 17, ал. 7 от Закона за киберсигурност се използва формата, посочена в приложение № 7 от Наредбата.

(3) При изпълняване на изискването на чл. 17, ал. 8 от Закона за киберсигурност секторните екипи за реагиране при инциденти с компютърната сигурност изпращат обобщената статистическа информация за инциденти към националния екип за реагиране при инциденти с компютърната сигурност, като използват формата, посочена в приложение № 8 от Наредбата.

(4) В случай че информацията по ал. 2 и 3 се изпраща по електронна поща, тя трябва да е подходящо защитена от неоторизиран достъп и да е класифицирана съгласно чл. 6, ал. 7 от Наредбата.

Чл.24. (1) Настоящите правила на община Доспат включват мерки за запазване интегритета на информацията в случай на инцидент, засягащ нейната достъпност.

(2) Във връзка с ал. 1 се изпълняват следните процеси, свързаните с тях дейности и отговорностите по резервиране и архивиране на информацията:

Попълва се от всяка община индивидуално

1. резервиране [и/или] архивиране на информацията от [бази данни, конфигурационни файлове, имиджи на системи и др.];
2. за архивиране и резервиране се използва външен носител;
3. резервирането е частично.
4. архивирането и резервирането се извършват за период от един месец.
5. правят се 1брой копия.
6. времето за съхраняване на всяко копие се определя съгласно изискванията на нормативните актове и оценката на риска;
7. всяко копие се съхранява на външен носител;
8. мерките защита от неправомерен достъп са физически и логически;
9. разрешение за използване се дава от лице, определено със заповед на Кмета.

(3) При резервирането [и/или] архивирането на информацията се спазват следните изисквания:

1. правят се регулярни копия съобразно риска от загуба на информация и динамиката на изменението й;
2. копията на информация са етикетирани по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час;
3. копията на чувствителна информация са в криптиран вид или поне защитени с парола;
4. копията на информацията се съхраняват на отделна машина и по възможност в друга защитена мрежа;
5. едно от копията на критична за дейността информация се съхранява off-line и по възможност в друга сграда или на облачна среда;
6. прави се и регулярна проверка на годността на резервните копия, дали те изпълняват целите, за които са създадени, и постига ли се необходимото време за възстановяване.

Чл.25. Общината предприема подходящи и в съответствие с рисковете мерки за гарантиране на нивото на услугите и дейностите, които са в обхвата на Наредбата, като:

1. резервиране на системи;
2. резервиране на устройства;
3. балансиране на натоварването на критични устройства или системи;
4. резервиране на центрове за данни.

Чл.26. (1) Общината разработва планове за непрекъсваемост за действия в случай на аварии, природни бедствия или други непредвидени обстоятелства, които биха причинили прекъсване на предоставяната от него услуга в съответствие с изискванията на чл. 5, ал. 1, т. 6 от Наредбата.

(2) Плановете по ал. 1 съдържат:

1. обстоятелствата, за които се отнасят;
2. праговете, при които се задействат;
3. лицето, което дава разрешение за задействането им;
4. реда за възстановяване на услугите и дейностите до определено ниво.

(3) Плановете по ал. 1:

1. се проиграват периодично, но не по-рядко от веднъж в годината, с цел да се провери тяхната актуалност и да се тренират лицата, които имат отговорности за изпълнението им;
2. се поддържат в актуално състояние;
3. са достъпни само за лицата, които имат отговорности за тяхното изпълнение;
4. се съхраняват най-малко на две места, едно от които е извън сградата, в която се намират системите, за които се отнасят.

Раздел III

ИЗИСКВАНИЯ ЗА КОНФИГУРИРАНЕ

Чл. 27. Във връзка с изискванията за конфигуриране, залегнали в Наредбата:

1. се забраняват macros в office пакетите;
2. забранява се pop-up в браузерите;
3. Auto play функцията се конфигурира винаги да иска потвърждение на потребителя;
4. User Account Control се конфигурира до най-високо ниво, така че винаги да издава предупреждения;
5. при споделянето на файлове и принтери не се използва настройка Everyone, а се указва кои акаунти точно да имат право на достъп до тях;
6. забранява се TRACE/TRACK методът;
7. забранява се anonymous authentication;
8. използва се Unicast Reverse-Path Forwarding (uRPF) за предпазване от използването на фалшиви IP адреси и rate-limiting за ограничаване на броя на заявките по IP адрес;
9. забранява се TLS renegotiation в системи, използващи TLS, или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия;
10. съобщенията за грешки в системите не дават излишна информация;
11. не се използва AutoComplete;
12. използват се приложения (add-ons) към браузърите за блокиране на рекламно съдържание;

Чл.28. Във връзка с изисквания към headers на отговорите на заявки за уеб сайтовете, които са залегнали в Наредбата, общината предприема следните мерки:

1. Headers на отговорите на заявките да не съдържат информация за платформите и версиите на използвания софтуер.
2. Headers на отговорите на заявките съдържат следните опции:

а) HTTP Strict Transport Security (HSTS) – политика съгласно RFC 6797 на IETF от 2012 г., която принуждава уеб браузъра на клиента да се свърже директно чрез HTTPS при преразглеждане на уеб сайта; препоръчителна стойност на периода на валидност на кеша на HSTS (max-age) е поне шест месеца;

б) X-Content-Type-Options – инструктира потребителския браузър да следва стриктно типа MIME, дефиниран в Content header; единствената валидна стойност за този хедър е "X-Content-Type-Options-nosniff";

в) X-XSS-Protection – настройва конфигурацията за XSS филтъра, вграден в повечето браузъри, което предотвратява някои категории XSS атаки; препоръчителна стойност "X-XSS-Protection: 1; mode=block";

г) X-Frame-Options – дава указания на браузъра да не вкарва уеб страницата във frame/iframe на други уеб страници; препоръчителна стойност "x-frame-options: SAMEORIGIN";

д) Content-Security-Policy – предотвратява широк спектър от атаки, включително Cross-site scripting и други cross-site injections;

е) Referrer-Policy Header – позволява на сайта да контролира колко информация с навигация да се включва в браузъра извън документа;

ж) Feature-Policy Header – позволява на сайта да контролира кои функции и приложни програмни интерфейси (API) могат да се използват в браузъра;

з) HTTP Public Key Pinning (HPKP) – защитен механизъм, който позволява на HTTPS уеб сайтовете да се противопоставят на имитация от страна на атакуващите, използвайки неправилно издадени или лъжливи сертификати.

РАЗДЕЛ IV

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

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

§2. Контролът по спазване на правилата се осъществява от секретаря на Общината за гарантиране на мрежовата и информационната сигурност на използваните информационни системи в Общинска администрация – Доспат. Допустими са допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защита на информацията.

§3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като община Доспат 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 Наредба за минималните изисквания за мрежова и информационна сигурност и са утвърдени със заповед на кмета на общината № А-613...../...22.10.....2020 г.

Изготвил:

Инж. Веселин Калфов, секретар на Община Доспат

Съгласувал:

Реджеп Реджепов

Абонаментна поддръжка на информационните ресурси