Приложение № 5

ОБЩИНА ИСПЕРИХ

7400 Исперих, обл. Разград, гр. Исперих, ул. "Васил Левски" № 70,
тел.: 08431/ 21-78; факс: 0843 / 21-84,
e- mail: isperih@isperih.bg,
www.isperih.bg

GDPR *ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ*

Утвърдил:
Бейсим Руфад
Кмет на Община Исперих

ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОБЩИНА ИСПЕРИХ

I. ОБЩИ ПОЛОЖЕНИЯ.

Чл. 1. /1/ Техническите и организационни мерки определят целите и задачите на сигурността на личните данни, основните принципи за изграждането й, организационните, технологичните и процедурните аспекти за осигуряване на сигурността на личните данни.

/2/ Настоящите технически и организационни мерки са съобразени с европейските и националните регулаторни норми и ведомствените документи, отнасящи се до сигурността на личните данни.

/3/ Техническите и организационни мерки се отнасят за всички структурни звена на Община Исперих, в които се осъществява обработка на лични данни, включително чувствителни лични данни, независимо от вида на техния носител.

/4/ Техническите и организационни мерки се отнасят и до други ведомства и организации, ако те се явяват обработващи на данни, за които Община Исперих е администратор.

/5/ Настоящите технически и организационни мерки, задават рамката на системата от мерки, насочени към:

1. гарантиране на конфиденциалност на информацията, включително личните данни, чрез прилагането на одобрени ограничения върху достъпа и разкриването на информация;
2. осигуряване на цялостност на информацията, чрез защита срещу неправомерни изменения или разрушаване на информация;
3. осигуряване на достъпност на информацията, чрез осигуряване на надежден и навременен достъп до информацията;
4. постигане на отчетност на информацията, чрез въвеждане на контрол върху достъпа и правата върху информационните ресурси и личните данни.

/6/ Видовете заплахи, които могат да застрашат конфиденциалността, интегритета и достъпността на личните данни, които се съдържат на електронен носител, се формулират в съответствие с Приложение № 4 към чл. 31, ал. 3 от Наредба за общите изисквания за мрежова и информационна сигурност.

II. РОЛИ И ОТГОВОРНОСТИ ПО СИГУРНОСТТА НА ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ.

Чл. 2. /1/ Отговорностите по сигурността на информацията са определени в длъжностните характеристики на служителите в община Исперих, разпореждания на ръководителите на дирекции и отдели към системния администратор за определяне на правата на достъп на съответните специалисти, политики по защита на личните данни, заповеди на кмета, секретаря, заместник кметовете или други длъжностни лица на Община Исперих.

/2/ Всички отговорни длъжностни лица са компетентни в своите области и непрекъснато подобряват уменията си с вътрешни и външни обучения.

/3/ Ръководството на община Исперих идентифицира отговорностите за защитата на личните данни и за провеждането на специфични процеси за сигурността им. Определят се отговорностите по управление на риска за сигурността на обработваните от Община Исперих лични данни и в частност, за приемане на остатъчните рискове.

/4/ Ръководителите на дирекции и отдели могат да делегират задачи по сигурността на обработваните лични данни на служителите в дирекцията/отдела, системния администратор по отношения на дейностите в конкретната дирекция/отдел,

както и на други лица. Независимо от делегираните задачи и отговорности, те остават отговорни и трябва да контролират правилното изпълнение на всички делегирани задачи.

/5/ Разделянето на задълженията се приема като метод за намаляване на риска от случайна или преднамерена злоупотреба с лични данни в Община Исперих.

/6/ Отговорност за сигурността за личните данни в Община Исперих носят:

1. Длъжностно лице по защитата на ЛД;
2. Лице/а обработващо/и лични данни –служители, на които е възложено или част от задълженията им са свързани с обработване на лични данни;
3. Системен администратор.

/7/ Всички служители в община Исперих се задължават да спазват политиките по защита на личните данни, техническите и организационни мерки, както и всички технически и технологични правила за обработка на данни, утвърдени в Община Исперих.

Чл. 3. /1/ Цел на техническите и организационни мерки е да се защити достъпната, обработваната, предаваната или съхраняваната информация и в местата за работа от разстояние.

/2/ Кметовете на кметства и кметски наместници в община Исперих, както и служителите на общината спазват изискванията, дефиниращи условията и ограниченията за използване на работа от разстояние. Когато се налага работа от разстояние, се отчитат следните фактори:

1. физическата сигурност на мястото за работа от разстояние /на сградата и местната заобикаляща среда/;
2. сигурността на комуникациите, възможността за отдалечен достъп до вътрешните системи на организацията, чувствителността на информацията, до която ще се осъществява достъп и която ще бъде предавана по комуникационната линия и чувствителността на вътрешната система.

/3/ Използването на домашни мрежи са забранени за служителите.

Определени от Кмета на община Исперих лица могат да ползват домашна мрежа, като носят лична отговорност за сигурността на мрежите и се задължават да използват определените им пароли и имена, както и правила за идентификация и автентификация.

/4/ Работата от разстояние се отнася за всички форми на работа извън Община Исперих, включително нетрадиционни работни среди, като така наричани среди на

„дистанционна работа /телекомпютри/”, „гъвкаво работно място”, „отдалечена работа” и „виртуална работа“.

III. МЕРКИ ПО ОТНОШЕНИЕ НА СИГУРНОСТТА НА ЧОВЕШКИТЕ РЕСУРСИ.

Чл. 4. /1/ При първоначално назначаване на нов служител, в зависимост от длъжността, която предстои да заеме и личните данни, до които ще му бъде предоставен достъп / напр. финансова, чувствителни лични данни и други специални категории лични данни/, могат да се извършат проверки свързани с репутационния риск на лицето.

/2/ Информацията по ал. 1 се събира и обработва в съответствие с приложимото национално законодателство, като кандидатите предварително се информират за това.

/4/ Отговорностите на Кмета на Община Исперих, секретаря на общината и длъжностното лице по защита на данните по отношение на служителите на община Исперих са:

1. подкрепа за прилагане политиките, процедурите, мерките и механизмите за контрол на сигурността на личните данни;
2. провеждане на инструктаж и обучения за техните роли и отговорности за сигурността на личните данни, преди да им бъде даден достъп до информационни системи;
3. даване на указания за очакванията по отношение на сигурността на личните данни и за тяхната роля в организацията;
4. мотивиране на служителите да изпълняват политиките по сигурност на личните данни и информация;
5. постигане на ниво на осъзнаване на важността на сигурността на личните данни, съответно на техните роли и отговорности;
6. осигуряване на комуникационен канал за анонимно докладване на нарушения на политиките или процедурите по сигурност на информацията и личните данни.

Чл. 5. /1/ Служители, извършили нарушение в сигурността на личните данни носят дисциплинарна отговорност по Кодекса на труда за неизпълнение на политиките и техническите и организационни мерки по сигурността на личните данни.

/2/ Дисциплинарният процес се прилага след предварителна проверка, доказваща, че е настъпило нарушение на сигурността на личните данни. Служителите се информират при постъпването им на работа за предвидените дисциплинарни наказания.

/3/ В дисциплинарния процес се вземат под внимание фактори като: естеството и тежестта на нарушението и неговото въздействие върху дейността, независимо дали това е първо или поредно нарушение.

Чл. 6. /1/ Отговорностите и задълженията по отношение сигурността на личните данни при прекратяване на правните отношения или промяна на заеманата длъжност са ясно дефинирани и оповестени на служителя.

/2/ Отговорностите, задълженията и декларацията за поверителност са валидни след прекратяването на правните отношения, като тези допълнителни условия се съдържат в условията на наемането на работа.

/3/ Прекият ръководител на напускащия служител/служителя, който преминава на друга позиция има задължението да уведоми Системния администратор и длъжностното лице по защита на личните данни, които трябва да предприемат незабавни мерки по прекратяване/ промяна на правата на достъп до:

1. сградния фонд;
2. системите за обработка на личните данни и всички информационни системи на Община Исперих;
3. предоставените активи на общината /изземване на комуникационни устройства, стационарни и преносими носители на информация и др./;
4. прекратяване/ промяна на потребителски права и пароли /от системния администратор като се изваждат от йерархията и/или се заключат/забранят профилите за достъп до системата/;
5. и др.

/4/ Измененията на отговорностите се управляват както при прекратяването на текущата отговорност или длъжност, така и при започването на нова отговорност или длъжност.

IV. УПРАВЛЕНИЕ НА АКТИВИ ЗА ОБРАБОТКА НА ЛИЧНИТЕ ДАННИ.

Чл. 7. /1/ Всички информационни активи, свързани с лични данни и средствата за обработка на информация са ясно идентифицирани от Община Исперих и на тези

активи е съставен и се поддържа точен опис в съответствие с Приложение № 6 към чл.35 от Наредбата за общите изисквания за мрежовата и информационна сигурност.

/2/ Община Исперих идентифицира активите, съответстващи на жизнения цикъл на информацията и документира тяхната важност. Жизненият цикъл на личните данни и информацията включва получаване/създаване, обработване, съхранение, обмен/предаване, изтриване и унищожаване.

/3/ За всички активи, поддържани в описа, е определен собственик на актива. Собствениците на активи са тези лица и субекти, които имат одобрена отговорност за жизнения цикъл на активите.

Чл. 8. /1/ Служителите в община Исперих се уведомяват за изискванията за сигурност на информацията на активите на организацията, свързани с информацията, средствата и ресурсите за обработка на лични данни.

/2/ При прекратяване на техните правни отношения, служителите в община Исперих се задължават да върнат всички обработвани от тях лични данни на прекия си ръководител, системния администратор или на Длъжностното лице по защита на личните данни.

/3/ През периода на предизвестие за прекратяване на правно отношение, се контролира неоторизираното копиране на лични данни.

Работа с информационни носители.

Чл. 9. /1/ Процесите за сигурно унищожаване на носители са управляеми, за да се намали до минимум рискът от изтичане на лични данни към неоторизирани лица.

/2/ Прилаганите способи за сигурно унищожаване на носители са пропорционални на чувствителността на тази информация.

/3/ Носителите, съдържащи лични данни, включително чувствителни лични данни, се съхраняват и унищожават по сигурен начин: напр. чрез изгаряне, нарязване, физическо разрушаване или изтриване на данни/.

/4/ Периодично се извършва идентификация на обектите, които изискват сигурно унищожаване съгласно Вътрешни правила за съхранение и унищожаване на лични данни.

/5/ За повредените устройства, съдържащи чувствителни данни, ако се наложи, се извършва извънредно оценяване на риска, за да се вземе решение дали те да бъдат физически унищожени или предадени за ремонт.

/6/ В определени случаи се организира събиране и сигурно унищожаване на всички носители, поради затруднения или невъзможност да се отделят чувствителните активи и специални категории лични данни.

/7/ Подборът на външната страна за събиране и унищожаване на носители се извършва като се отчитат редица фактори като опит, прилагане на адекватни механизми за контрол и др.

V. ПОЛИТИКА ЗА КОНТРОЛ НА ДОСТЪПА.

Чл. 10. /1/ Кметът на Община Исперих, секретарят на общината, системният администратор, длъжностното лице по защита на данните или друго определено лице определят подходящи правила за достъп и ограничения за специфични/конкретни потребителски права, при отчитане на свързаните със сигурността на информацията рискове и в съответствие с Приложение № 5 към чл. 32, ал. 2 и Приложение № 13 към чл. 51 от Наредбата за общите изисквания за мрежовата и информационна сигурност.

/2/ Всички механизми за контрол на достъпа са както логически, така и физически.

/3/ Изискванията, на които трябва да отговарят механизмите за контрол на достъпа са ясно указани на служителите.

/4/ При прилагането на политиката за контрол на достъпа се вземат предвид:

1. изискванията за сигурност на приложенията на общината;
2. политиките за разпространение и оторизиране на информация, принципът „необходимо е да знае” и нивата на сигурност на информацията ;
3. разделянето на ролите за контрол на достъпа /оторизиране на достъпа, администриране на достъпа/;
4. изискванията за оторизиране на заявките за достъп;
5. изискванията за периодичен преглед на правата на достъп;
6. отнемането на права на достъп;
7. архивирането на записите на всички значими събития, засягащи използването и управлението на идентичността на потребителите и тайната информацията за автентификация;
8. ролите с привилегирован достъп.

/5/ Достъпът до мрежи се отнася за използването на мрежи и мрежови услуги и обхваща:

1. използването на мрежите и мрежовите услуги, които са позволени за достъп в общината;
2. регламенти за оторизиране и за определяне на кого е позволено да има достъп, и до кои мрежи и мрежови услуги;
3. управлението на защитата на достъпа до мрежови връзки и мрежови услуги;
4. средствата, използвани за достъп до мрежи и мрежови услуги;
5. ограничаване на броя несполучливи опити /до 3 броя/ на потребител за вход в системата, за определен интервал от време, след което акаунтът му се заключва;
6. определяне на предупреждаващите съобщения, информиращи потребителя преди предоставяне на достъп, относно:

а) общите ограничения, налагани от системата;

б) възможният мониторинг, протоколиране и одит на използването на системата;

в) забраните и възможните санкции при несанкционирано използване на системата;

г) възможните действия на потребителя, които могат да бъдат изпълнени от информационната система без необходимост от автентикация и оторизация.

7. изискванията за автентифициране на потребителя за достъп до различни мрежови услуги;

Управление на достъпа на потребителите.

Чл. 11. /1/ Управлението на достъпа на потребителите се извършва чрез идентификация.

/2/ Процесът за управление на идентификацията на потребителите включва:

1. използване на уникални идентификатори на потребителите, за да се разреши на потребителите да се свързват и да носят отговорност за своите действия;
2. използването на споделени идентификатори е разрешавано само там, където те са необходими за дейността или по оперативни/експлоатационни причини и е одобрено от Системния администратор и Длъжностното лице по защита на данните;
3. незабавно забраняване или отстраняване на потребителски идентификатор на служители, които са напуснали Община Исперих;

4. периодично идентифициране, отстраняване или забраняване на излишни потребителски идентификатори;

Чл. 12. /1/ Предоставянето или отменянето на достъп до информация обикновено е действие за присвояване, разрешаване, или отказване на потребителски идентификатор, както и предоставяне или отказване на права на достъп на такъв потребителски идентификатор.

/2/ Системният администратор на общината по нареждане на Директор дирекция/началник отдел, зам.-кметовете, секретаря на общината или Кмет на общината определя профили за достъпа на служителите до ресурсите в информационните системи на Община Исперих.

/3/ Процесът, осигуряващ присвояване или отнемане на права на достъп, предоставен на потребителски идентификатор се управлява от системния администратор на Община Исперих и се отразява в Дневник на администратора, който осигурява:

1. верифициране, че предоставеното ниво за достъп е в съответствие с изискванията и е свързано с конкретните задължения;
2. гарантиране, че правата на достъп не са активирани, преди да бъдат завършени процедурите за оторизиране;
3. поддържане на данни за предоставените права на достъп на потребителските идентификатори;
4. адаптиране на правата на достъп на потребители, които са променили ролите си и незабавно премахване или блокиране на права на достъп на потребители, които са напуснали администрацията;

Чл. 13. /1/ Заявките за достъп и прегледите се управляват на ниво задълженията на служителите от съответната дирекция/отдел, а не на ниво конкретни права.

/2/ При направен опит за неоторизиран достъп от персонала или доставчиците Системния администратор на общината докладва на секретаря на общината, който определя съответните санкции към лицата и мерки за защита.

Чл. 14. /1/ Предоставянето на привилегировани права за достъп се контролира чрез процес на оторизиране от системния администратор, който трябва да може да докаже във всеки един момент от кого е получил нареждане за даване на привилегировани права.

/2/ Привилегиите за достъп са предоставени на потребителите въз основа на принципа „необходимост да се знае” и „събитие по събитие”, в съответствие с

политиката по контрол на достъпа, т.е. на база минималното изискване за техните функционални задължения.

/3/ Привилегиите за достъп не се предоставят, докато не бъде завършен процесът на оторизиране, като се дефинират изисквания за крайния срок на привилегиите за достъп.

/4/ Привилегиите за достъп се предоставят на потребителски идентификатор, който е различен от тези за редовните дейности. Редовните дейности не се изпълняват от привилегирован идентификатор.

/5/ Компетентността на потребителите с привилегии за достъп се преглеждат периодично, за да се провери дали те са в съответствие с техните задължения.

Управление на тайната информация за автентификация на потребителите.

Чл. 15. /1/ Информацията за автентификация на потребители се управлява при спазване на строго дефинирани изисквания.

/2/ Процесите в тази политика включват следните изисквания:

1. от потребителите се изисква да подпишат декларация да пазят поверителността на личната информация за автентификация и да пазят груповата /т.е. споделената/ информация за автентификация между членовете на групата; тази подписана декларация може да се включи в сроковете и условията за назначаване;
2. от потребителите се изисква да поддържат своята поверителна информация за автентификация, която те са задължени да променят при първото й използване;
3. регламентира се верифицирането /проверката/ на идентичността на потребителя, преди да му бъде предоставена нова, сменена или временна, информация за автентификация;
4. временната поверителна информация за автентификация се дава на потребителите по защитен начин;
5. временната поверителна информация за автентификация е уникална за служителите и не трябва да бъде разгадаема;
6. потребителите потвърждават получаването на поверителната информация за автентификация;

Чл. 16. Паролите са общо използван тип поверителна информация за автентификация и са често срещано средство за верифициране на идентичността на потребителя.

Чл. 17. /1/ Правата за достъп на потребителите се преглеждат на редовни интервали от Системния администратор поне един път в месеца, или след всяко изменение, като повишение, понижение или прекратяване на правното отношение.

/2/ Правата за достъп на потребителите се преглеждат и дават отново, когато има преминаване от една длъжност в друга в администрацията.

/3/ Оторизацията на привилегиите за достъп се преглеждат на по-чести интервали, за да се гарантира, че не са били получени неоторизирани привилегии. Всички изменения на привилегированите акаунти се записват на периодичните прегледи.

/4/ При прекратяване на трудовото или служебното правоотношение или промяната на заеманата длъжност, в зависимост от оценяването на рисковите фактори, правата за достъп на лицето до информация и активи, свързани със средствата за обработка на лични данни се отнемат, редуцират или спират.

/5/ Правата за достъп, които трябва да бъдат отнети или променени, включват тези за физически и логически достъп. Отнемането или промяната, могат да станат чрез преустановяване, отмяна или заместване на ключове.

Система за управление на пароли.

Чл. 18. /1/ Системата за управление на пароли налага използването на индивидуални потребителски идентификатори и пароли. С нея се поддържа отговорността, дава се възможност на потребителите да избират и променят своите пароли и включва процедура за потвърждаване, която да намалява входните грешки.

/2/ Потребителите променят своите пароли при първото влизане.

/3/ Системата извършва редовни изменения на паролите – на всеки 3 месеца и поддържа запис на предишни пароли и предотвратява повторното им използване.

/4/ При въвеждане паролите не се изобразяват на екрана, а файловете с пароли не съхраняват отделно от данните за приложната система.

Чл. 19. /1/ Служителите на Община Исперих използват следните правила за управление на паролите:

1. минималната дължина на паролите за достъп до информационните ресурси на общината и до потребителските станции е между осем и 16 буквено-цифрови символа.
2. паролите задължително се състоят от поне една главна, една малка буква, един специален символ и една цифра.
3. давността на паролите изтича след три месеца. След този срок потребителят автоматично бива задължен да смени паролата си.
4. настройката на паролите е отговорност на Системния администратор;
5. на потребителите се забранява да записват върху хартия или на друг носител паролите си за достъп до информационните ресурси и лични данни на администратора.
6. на потребителите се забранява да споделят под каквато и да е форма паролите си за достъп до информационните ресурси на администратора.

/2/ Някои приложения изискват потребителските пароли да бъдат присвоявани от независим овластен орган. В такива случаи някои от горните указания са неприложими. В повечето случаи паролите се избират и поддържат от потребителите.

VI. КРИПТОГРАФСКИ МЕХАНИЗМИ ЗА КОНТРОЛ.

Чл. 20. /1/ В резултат на оценката на риска, в съответствие с Приложение №3 към чл.31, ал.2 от Наредба за общите изисквания за мрежова и информационна сигурност, се идентифицира изискваното ниво на защита, отчитайки типа и качеството на допустимо използваните алгоритми за криптиране.

/2/ При внедряване на криптографската политика на общината се вземат под внимание нормативните актове, които са приложими към използването на криптографски техники.

VII. ФИЗИЧЕСКА СИГУРНОСТ И СИГУРНОСТ НА ЗАОБИКАЛЯЩАТА СРЕДА.

Чл. 21. /1/ В Община Исперих са дефинирани границите на физическата сигурност и местата, които съдържат средства за обработка на лични данни и

информация. Всички зони са подходящо защитени срещу неоторизиран достъп с контролни механизми като няма ненаблюдавана външна или вътрешна страна.

/2/ Параметрите на физическата сигурност на информационните системи са определени в съответствие с Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за мрежова и информационна сигурност.

/3/ Където е приложимо, могат да се изграждат физически бариери за предотвратяване на неоторизиран физически достъп.

/4/ Помещенията, в които се разполага техническото оборудване и информационни активи се оборудват със следните технически системи за защита, безопасност и охрана:

а) пожарогасителна система, която трябва да отговаря на изискванията на EN 14520;

б) климатизация;

в) резервно електрозахранване;

г) системи за контрол на достъпа.

/5/ Хартиените носители на информация, съдържаща лични данни се съхраняват в помещения с оторизиран достъп, в шкафове или метални каси.

Чл. 22. /1/ Физическият достъп, датата и часът на влизане и излизане на служители и посетители се записва в съответствие с Пропускателен режим в сградата на община и правилата за видеонаблюдение.

/2/ На лица, представители на външни доставчици на услуги се дава ограничен достъп до зоните за обработка на лични данни.

Ненадзиравани потребителски устройства.

Чл. 23. /1/ Всички служители се осведомяват за изискванията и процедурите за сигурност за защита на ненадзиравани устройства, както и за отговорностите за прилагане на такава защита.

/2/ Служителите на общината се задължават да прекратяват активните си сесии, когато приключат работа, освен ако те не са осигурени с подходящ заключващ механизъм /например защитен предпазен екран с парола/.

/3/ Потребителите се отписват от приложения или мрежови услуги, когато повече не са им необходими и защитават компютрите и мобилните устройства от неоторизирано използване чрез заключване или еквивалентен механизъм за контрол, например достъп с парола, когато не се използват.

Чл. 24. /1/ При спазването на политиката за чисто бюро и чист екран се вземат предвид съответните аспекти на организационна култура и рискове на организацията.

/2/ Отчитат се следните указания:

1. личните данни, било то на хартия или на електронен носител, се съхраняват в сейф, шкаф или други сигурни места за съхранение;
2. компютрите и крайните устройства се изключват от мрежата или се защитават с механизъм за заключване на екрана и клавиатурата, управляван с парола, маркер или подобен механизъм за автентификация на потребителя, когато са ненадзиравани, и трябва да бъдат защитени с ключалки, пароли или други механизми за контрол, когато не са в употреба 3 минути.

Чл. 25. /1/ За да се предотврати неоторизираното използване на фотокопия или носители, съдържащи лични данни, те незабавно се премахват от служителите от печатащите устройства и се прибират на указаните места.

/2/ Забранява се на служителите на общинната да оставят на бюрата си документи, съдържащи лични данни без надзор както и цветни листчета с пароли за достъп. При напускане на бюрото всички документи и носители на лични данни се преместват с заключващи се шкафове.

/3/ Сейфове или други средства за сигурно съхраняване също могат да защитят информацията, съхранявана в тях от бедствия, като пожар, земетресение, наводнение или експлозия.

/4/ В определени случаи могат да се използват принтери с PIN код функция, така че тези, които са подали информация за печатане, да са единствените, които могат да вземат своите копия само когато стоят до принтера.

VIII. ПРОЦЕДУРИ ЗА РАБОТА И ОТГОВОРНОСТИ.

Инсталиране и конфигуриране на системи.

Чл. 26. /1/ На служителите се забранява инсталирането на нелицензиран софтуер и използването на други продукти, което представлява нарушение на правата върху интелектуална собственост.

/4/ Системният администратор на Община Исперих определя и прилага правилата за:

1. резервиране;

2. обработка на грешки или други извънредни условия, които могат да възникнат по време на изпълнение на работа, включително ограничения за използването на системни обслужващи програми;
3. поддръжка и повишаване на контактите, включително контакти за външна поддръжка в случай на неочаквани трудности при работа или технически трудности;
4. процедури за повторно стартиране на системата и възстановяване за използване при повреда на системата.

Механизми за контрол срещу злонамерен софтуер.

Чл. 27. /1/ Нежеланият софтуер, който може да експлоатира уязвимостта на един или няколко информационни актива и да предизвика смущаване на нормалната им работа, увреждане или унищожаване, включва следните основни програми:

а) компютърни вируси;

б) мрежови червеи;

в) троянски коне, и

г) логически бомби.

/2/ Защитата срещу нежелан софтуер в информационните системи на Община Исперих е в съответствие с Приложение 9 към чл.41 от Наредба за общите изисквания за мрежова и информационна сигурност и е ориентирана в две основни направления:

а) чрез забрана за използване на нерегламентиран софтуер;

б) чрез задължително използване на утвърден за администрацията на общината антивирусен софтуер и софтуер за откриване на нерегламентирани промени на информационните активи.

/3/ Програмните продукти, предназначени за откриване на опити за проникване, трябва да разпознават следните подозрителни действия в мрежата:

а) опити да се използват услуги, блокирани от защитни стени;

б) неочаквани заявки, особено от непознати адреси;

в) неочаквани шифровани съобщения;

г) извънредно активен трафик от непознати сървъри и устройства;

д) значителни изменения на предишни действия на мрежата;

е) опити за използване на известни системни грешки или уязвимости;

ж) опити за вход от непознати потребители от неочаквани адреси;

з) несанкционирано или подозрително използване на администраторски функции;

и) значителни изменения в обичайните действия на потребител и пр.

/4/ При установяване на открити опити за проникване незабавно се:

а) уведомява се Ръководството на общината за предприемане на адекватни мерки;

б) изключват или ограничават мрежовите услуги, свързани с информационния актив - обект на проникването.

/5/ Всяко устройство, което се включва в мрежата на общината автоматично да се проверява за вируси и нежелан софтуер, преди да получи достъп до ресурсите на мрежата.

/6/ Системният администратор на общината осъществява откриване и възстановяване от злонамерен софтуер

/7/ Това се постига чрез:

1. внедряване на механизми за контрол, които предотвратяват или откриват използването на неоторизиран софтуер;
2. внедряване на механизми за контрол, които предотвратяват или откриват използването на известни или подозрителни уеб сайтове;
3. създаване на правила за получаване на файлове и софтуер от или чрез външни мрежи или на всякакъв друг носител, показваща какви защитни мерки трябва да бъдат взети;
4. намаляване на уязвимости, които биха могли да бъдат използвани от злонамерен софтуер, например чрез управление на техническата уязвимост;
5. провеждане на редовни прегледи на софтуера и съдържанието на данните на системи, поддържащи критични процеси на дейността; откриването на каквито и да е неодобрени файлове или неоторизирани поправки се разследва/проучва официално;
6. инсталиране и редовно обновяване на софтуер за откриването на злонамерен софтуер и възстановяване на софтуера за сканиране на компютри и носители като превантивен контрол или на рутинна основа;
7. сканиране на всички файлове, получени по мрежите или чрез всякаква форма на запаметяващ носител, за злонамерен софтуер преди използване, а също и сканиране на прикачените файлове от електронна поща и свалени файлове за злонамерен софтуер преди използване; това сканиране трябва да се проведе

на различни места, например на сървъри за електронна поща, настолни компютри и когато се влиза в мрежата на организацията; сканиране на уеб страници за злонамерен софтуер;

8. регламентиране на отговорностите за справяне със защитата от злонамерен софтуер на системите, обучение за тяхното използване, докладване и възстановяване от атаки със злонамерен софтуер;
9. използване на сведения, даващи информация за нов злонамерен софтуер;

Резервиране на информация.

Чл. 28. /1/ При извършване или организиране на действието „резервиране“, системният администратор прилага строго определени правила в съответствие с Приложение към чл.37 от Наредба за общите изисквания за мрежова и информационна сигурност.

/2/ Правилата по ал.1 включват следните изисквания:

1. точни и пълни записи на резервните копия;
2. честотата на резервиране съответства на изискванията за дейността на Община Исперих, изискванията за сигурност на включената информация и критичността на информацията за непрекъснатост на работа;
3. графиците за резервиране се определят от ръководството - препоръчително е ежедневно резервиране;
4. на резервираната информация да бъде дадено съответно ниво на физическа защита и защита на околната среда;
5. носителите на резервни копия редовно се изпитват, за да е сигурно, че на тях може да се разчита за използване в извънредни случаи, когато е необходимо /това се съчетава с изпитване на процедурите за възстановяване и проверявано спрямо изискваното време за възстановяване/.
6. редовно обновяване на носителите, върху които се записват резервни копия (на период около 2/3 от срока им на годност);
7. изпитването на способността за възстановяване на резервирани данни се изпълнява на специални носители за изпитване. Не се записва върху оригиналния носител, за да не се причинят невъзстановими щети или загуба на данните, ако процесът на възстановяване е неуспешен;
8. в случаи когато е важна поверителността, резервирането може да бъде защитено чрез криптиране;

9. достъпът до резервни и архивни копия се извършва под контрола на Системния администратор на общината.

/3/ Периодично резервирането се проверява, като се следи за откази на предвидените резервирания, за да гарантира пълнота на резервирането.

Регистриране на събития.

Чл. 29. /1/ Регистрите на събития могат да съдържат чувствителни данни и информация за самоличността, поради тази причина се вземат подходящи мерки за защита на личните данни.

/2/ Системният администратор не изтрива или деактивира дневници /записите/логовете/ за своите собствени действия.

/3/ Дневниците на събития включват:

1. идентификатори на потребителя;
2. тип на събитието;
3. резултати от събитието;
4. източник на събитието;
5. работа /дейности/ на системата;
6. дати, време на настъпване и подробности за ключови събития, например влизане и излизане;
7. идентичност на устройство или местоположение;
8. записи на успешни и отхвърлени опити за достъп до системата;
9. записи на успешни и отхвърлени опити за достъп до данни и други опити за достъп до ресурси;
10. изменения на системната конфигурация;
11. използване на привилегии;
12. използване на системни помощни програми и приложения;
13. списък на засегнатите обекти и файлове, до които е имало достъп, и вид на достъпа;
14. мрежови адреси и протоколи;
15. алармени сигнали, издадени от системата за контрол на достъпа;
16. активиране и деактивиране на защитни системи, като антивирусни системи и системи за откриване на нарушители;
17. описание на измененията в системата за защита, произтекли от събитието.

/4/ Системният администратор докладва събитията на секретаря на общината или на друго оторизирано лице.

Синхронизация на часовниците.

Чл. 30. /1/ За осигуряване на точност и пълнота на записите на логовете, които могат да се използват за разследване на неправомерни действия или за нуждите на ангажиране на съдебни доказателства, е осигурено поддържането на единно време в информационните системи съгласно Закона за електронното управление и Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги.

/2/ Дефинирано е стандартно опорно време за използване чрез получаване на опорно време от външен/и/ източник/ци/ и надеждно синхронизирани вътрешни часовници.

/3/ Използва се мрежов протокол за време с цел поддържане на всички сървъри в синхрон с главния часовник.

Управление на техническите уязвимости.

Чл. 31. /1/ Управлението на техническа уязвимост се разглежда като подфункция на управлението на измененията и като такава може да се използва от процесите и процедурите за управление на измененията.

/2/ Наличието на пълен опис на активите е предварително условие за ефикасно управление на техническата уязвимост.

/3/ За всеки информационен актив се определя ниво на защита от неправомерен достъп в съответствие с чл. 34 от Наредба за общите изисквания за мрежова и информационна сигурност.

/4/ При идентификация на потенциални технически уязвимости се спазват определени технически указания, за да се установи ефикасен процес на управление за технически уязвимости:

1. дефинират се и се установят ролите и отговорностите, свързани с управлението на техническата уязвимост, включително мониторинг на уязвимостта, оценка на риска за уязвимост, поправки на софтуера, проследяване на активи и всички изисквани отговорности по координацията;

2. идентифицират се информационните ресурси, които ще се използват за идентифициране на съответните технически уязвимости, за софтуера и друга технология /основана на списъка на активи на общината;
3. след идентифицирането на потенциална техническа уязвимост Община Исперих идентифицира свързаните с нея рискове и действията, които трябва да бъдат предприети;
4. в зависимост от това колко спешно трябва да се обърне внимание на техническата уязвимост, предприетото действие се провежда според механизмите за контрол, свързани с управлението на изменения или чрез следване на процедурите за реакция на инцидент със сигурността на информацията;
5. ако има поправка от легитимен източник, рисковете, свързани с инсталирането на поправката, се оценяват /рисковете, наложени от уязвимостта, се сравняват с риска от инсталиране на поправката/;
6. поддържа се дневник/протокол/ опис за всички предприети процедури;
7. процесът на управление на технически уязвимости е редовно наблюдаван и оценяван, за да се осигури неговата ефикасност и ефективност;
8. системите с висок риск са с приоритет.

IX. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ.

Чл. 32. /1/ С цел намаляване на риска произтичащите от появата на инциденти в Община Исперих е разработена и внедрена политика за управление на инциденти, в съответствие с Приложение № 10 към чл. 43, ал. 2 и Приложение № 12 към чл. 48 от Наредба за общите изисквания за мрежова и информационна сигурност.

/2/ Всички служители се осведомяват за отговорностите да докладват събития със сигурността на личните данни и информацията.

/3/ Случаите, които се вземат под внимание за докладване на събития със сигурността на информацията, включват:

1. неефикасен контрол на сигурността;
2. нарушаване на очакванията за цялостността, поверителността или наличността на информацията;
3. човешки грешки;
4. несъответствие с политики или указания;

5. нарушения на физическата сигурност;
6. неконтролирани изменения на системата;
7. неправилна работа на софтуер или хардуер;
8. нарушения на достъпа.

Докладване за слабости в сигурността на личните данни.

Чл. 33. /1/ Всички служители докладват за възникнали проблеми с информационните системи, съгласно Процедура за действие при нарушение на сигурността на личните данни, за да се предотвратят инциденти със сигурността на личните данни.

/2/ Служителите нямат право да правят опити да доказват подозрителни слабости в сигурността. Изпитването на слабостите може да се тълкува като потенциална злоупотреба със системата и би могло да причини и повреда на информационната система и услуга и да доведе до правна отговорност за лицето, което изпълнява изпитването.

Чл. 34. /1/ Община Исперих предприема марки за реакция на инциденти със сигурността наличните данни в съответствие с Процедура за действие при нарушение на сигурността на личните данни.

/2/ Реакцията при инциденти включва следното:

1. събиране на доказателства, колкото е възможно по-скоро след възникването;
2. извършване на разследващ анализ за сигурността на информацията, ако се изисква;
3. осигуряване на правилно записване/регистриране на всички участващи дейности по реакцията за последващ анализ;
4. съобщаване за съществуването на инцидент със сигурността на личните данни и информацията или всякакви съответни подробности за него на други вътрешни и външни лица или организации в съответствие с националното законодателство;
5. обработка на слабост/и със сигурността на информацията, открита/и, че причиняват или допринасят за инцидента;
6. официално приключване и записване на инцидента, след като той бъде успешно обработен.

/3/ След инцидента, ако е необходимо се провежда анализ, за да се идентифицира източникът на инцидента.

Чл. 35. /1/ Информацията, придобита от преценяването на инцидентите със сигурността на личните данни и информацията се използва за идентифициране на повтарящи се инциденти или инциденти с голямо въздействие.

/2/ Преценяването на инцидентите дава информация дали е необходимо усъвършенстване или допълнителни механизми за контрол, които да ограничат честотата, щетите и цената на бъдещи появи или да бъдат взети под внимание в процеса на преглед на политиката по сигурността.

X. ПЛАНИРАНЕ НА НЕПРЕКЪСНАТОСТТА НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

Чл. 36. /1/ Община Исперих прави анализ на въздействието върху дейността за аспектите на сигурността на личните данни и информацията, за да определи изискванията за сигурност на информацията.

/2/ Според изискванията за непрекъснатост на сигурността на информацията Община Исперих създава, документира, внедрява и поддържа:

1. механизми за контрол на сигурността на информацията в рамките на процесите, процедурите и поддържащите системи и инструменти за непрекъснатост на дейността и възстановяване от бедствие;
2. процеси, процедури и изменения за прилагането на съществуващите механизми за контрол на сигурността на информацията по време на неблагоприятен случай;
3. компенсиращи механизми за контрол за механизмите за контрол на сигурността на информацията, които не могат да бъдат поддържани по време на неблагоприятен случай.

XI. ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ.

§.1. Настоящите технически и организационни мерки за защита на личните данни са неразделна част **/Приложение № 5/** от Вътрешните правила/политики за защита на личните данни в общинска администрация Исперих и влизат в сила от датата на тяхното утвърждаването от Кмета на община Исперих.

§.2. Настоящите технически и организационни мерки за защита на личните данни се преглеждат и актуализират при всяка промяна в нормативната уредба, но най-малко веднъж годишно.