Приложение № 5

ОБЩИНА ГЪРМЕН
2960 Гърмен, ул. "Първа" №35, тел.: 07523/20 40; 07523/20 47, факс: 07523/31 79; 0751/6 10 62,
e- mail: obs_garmen@bitex.bg; oba_garmen@abv.bg,
www.garmen.bg

GDPR ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

УТВЪРДИЛ:

МИНКА КАПИТАНОВА
Кмет на Община Гърмен

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

I. ОБЩИ ПОЛОЖЕНИЯ.

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

/3/ Техническите и организационни мерки се отнасят за всички структури на Община Гърмен, в които се осъществява обработка на лични данни, включително чувствителна информация /ЛД/, а също така и за структурите, осигуряващи обслужването и нормалното функциониране на общината.

/4/ Техническите и организационни мерки се отнасят и до други ведомства и организации, ако те се явяват обработващи - потребители на информацията, създавана, обработвана и предавана в структурите на Община Гърмен.

/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.

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, разпореждания на ръководителите на отдели към системния администратор за определяне на правата да достъп на съответните специалисти, политики по защита на личните данни, заповеди на кмета, секретаря, заместник кмет или други длъжностни лица на Община Гърмен.

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

/3/ Ръководството на община Гърмен 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 Гърмен лични данни и в частност за приемане на остатъчните рискове.

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

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

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

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

II. 1. Политика за работа от разстояние в Община Гърмен.

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

/2/ Кметовете на кметства, кметски наместници в Община Гърмен и служителите на общината спазват изискванията, дефиниращи условията и ограниченията за използване на работа от разстояние. Там, където се налага работа от разстояние, се отчитат следните фактори: физическата сигурност на мястото за работа от разстояние /на сградата и местната заобикаляща среда/:предлаганата физическа среда за работа от разстояние – в сградата на кметството и в сградата на Община Гърмен;

1. 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;
2. предоставянето на виртуален достъп до настолни компютри, който предотвратява обработването и съхраняването информация на лични устройства;
3. заплахата от неоторизиран достъп до информация или ресурси от други лица, които използват помещението, например външни посетители и граждани, които ползват услугите на Община Гърмен или на Кметствата в общината;
4. използването на домашни мрежи и изискванията или ограниченията за конфигурацията на услугите по безжична мрежа са забранени за служителите на Община Гърмен. Кмета на Община Гърмен както и кметовете на кметства, кметските наместници, секретарят на общината и зам. кметовете могат да ползват домашна мрежа, като носят лична отговорност за сигурността на мрежите и се задължават да използват определените им пароли и имена, и правила за идентификация и автентификация;
5. достъпът да лични устройства /за верифициране на сигурността на машината или по време на разследване/, който може да е забранен по закон.

/3/ Работата от разстояние се отнася за всички форми на работа извън общината, включително нетрадиционни работни среди, като тези наричани среди на „дистанционна работа /телекомпютри/”, „гъвкаво работно място”, „отдалечена работа” и „виртуална работа“.

II. 2. Контакт с оторизирани органи.

Чл.4. /1/ Община Гърмен има определени служители, който поддържат контакт със съответните компетентни органи. Контакта се осъществява със съответното направление/дирекция, кой трябва да се свърже с компетентни органи/например правоприлагащите органи, регулаторните органи, надзорните власти/ и те са задължени и своевременно да докладват за идентифицираните инциденти и нарушения със сигурността на личните данни /например дали се подозира, че е нарушено законодателството/, с цел да се предприемат действия срещу източника на атаката.

/2/ Контактите с други компетентни органи са свързани с предоставяните административни услуги, оборудване, услуги при извънредни ситуации, електроснабдяване, здраве и безопасност, например противопожарна охрана, доставчици на телекомуникации /във връзка с маршрутизирането на линии и готовността/ и водоснабдяване, климатизация и други /във връзка с охладителните системи на устройствата/.

III. МЕРКИ ПО ОТНОШЕНИЕ НА СИГУРНОСТТА НА ЧОВЕШКИТЕ РЕСУРСИ.

Чл.5. /1/ Преди да бъдат наети служители, се извършва проучване за проверка на биографичните данни на всички кандидати за наемане на работа в съответствие със съответните закони, нормативни актове и етика /по отношение на предишни инциденти, свързани с обработването на лични данни/, и съобразно изискванията, свързани с дейността, класификацията на информацията, до която имат достъп, и предполагаемите рискове /виж актуалната оценка на риска, плана за въздействие на риска и плана за действие/.

/2/ Когато работата при първоначално назначаване или при повишение налага лицето да има достъп до средства за обработка на лични данни и в частност, до поверителна информация /напр. финансова, чувствителни лични данни и други специални категории лични данни/, могат да се предвиждат и допълнителни, по-подробни проверки свързани с репутационния риск на лицето.

/3/ Допълнителните проверки по ал.2 трябва да бъдат съобразени с националното законодателство и одобрени от ръководител на човешки ресурси и длъжностното лице по защита на личните данни.

/4/ Информацията за всички кандидати, които са обсъждани за позиции в организацията, се събира и обработва в съответствие с всяко приложимо национално законодателство. В зависимост от приложимото законодателство кандидатите предварително се информират за дейностите по подбора им.

/5/ Отговорностите на ръководството на община Гърмен и длъжностното лице по защита на данните, по отношение на служителите на Община Гърмен са:

1. демонстриране ангажираност и подкрепа за 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 поверителна информация или 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 сигурността на личните данни, съответно на техните роли и отговорности;
6. периодичното информиране, обучение и квалификация да имат подходящите умения и квалификация и да се образоват редовно;
7. осигуряване на комуникационен канал за анонимно докладване, на нарушения на политиките или процедурите по сигурност на информацията и личните данни.

Чл.6 /1/ Служители, извършили нарушение в сигурността на информацията носят дисциплинарна отговорност по Кодекса на труда и Закона за държавния служител за неизпълнение на политиките и техническите и организационни мерки по сигурността на личните данни.

/2/ При проява на преднамерени нарушения се предприемат незабавни действия.

/3/ Дисциплинарният процес се прилага чрез предварителна проверка,

доказваща, че е настъпило нарушение на сигурността на информацията. Служители се информират при постъпването им на работа за предвидените в дисциплинарни наказания.

/4/ Официалният дисциплинарен процес осигурява правилно и честно третиране на служителите, които са заподозрени в извършване на нарушения на сигурността на личните данни. Той обезпечава степенуван отговор, вземащ под внимание фактори като естеството и тежестта на нарушението и неговото въздействие върху дейността, независимо дали това е първо или поредно нарушение, дали нарушителят е бил подходящо обучен или не, съответното законодателство, договорите за дейността и други фактори, ако се изисква.

Чл.7 /1/ Отговорностите и задълженията по отношение сигурността на личните данни при прекратяване на правоотношенията или промяна на заеманата длъжност /промяна на дирекция или промяна на степента/ са ясно дефинирани, оповестени на служителя, и приведени в действие.

/2/ Съобщаването за прекратяване на отговорностите включва текущи изисквания за сигурност на личните данни и информацията, и законови отговорности. В определени случаи отговорностите, задълженията и споразумението за поверителност са валидни след прекратяването на работа, като тези допълнителни условия се съдържат в сроковете и условията на наемането на работа.

/3/ Прекият ръководител на напускащия служител/ служителя, който преминава на друга позиция има задължението на 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. сградения фонд;
2. системите за обработка на личните данни и всички информационни системи на общината;
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 служба, така и при започването на нова отговорност или длъжност.

/5/ Прекият ръководител на съответния служител отговаря за цялостния процес по прекратяване отговорностите по управление на аспектите на сигурността на личните данни и информацията за конкретен служител и съответните процедури.

IV. УПРАВЛЕНИЕ НА АКТИВИ ЗА ОБРАБОТКА НА ЛИЧНИТЕ ДАННИ.

Чл.8 /1/ Всички активи, свързани с лични данни и средствата за обработка на информация са ясно идентифицирани от Община Гърмен и на тези активи е съставен и се поддържа точен опис, актуален, последователен и съответен на другите описи.

/2/ Община Гърмен 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 всеки от описаните активи е определен собственик и е извършена съответната класификация. Описите на активите гарантират, че съществува ефикасна защита и те могат да се използват и за други цели, като здраве и безопасност, застраховане или финансови /управление на активи/.

/4/ 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 /ЛД/.

/5/ Собствеността на активите се определя, когато се създават активите или когато се преместват активи в организацията. Собственикът на актив отговаря за правилното му съхранение през целия му жизнен цикъл.

/6/ Идентифицираният собственик не притежава непременно някакви права на материална собственост върху актива. В повечето случаи собственика на актива е лицето, което обичайно борави с него в процеса на обработка на лични данни.

/7/ Собственикът на актив трябва да гарантира, че активите са описани, че активите са надлежно класифицирани и защитени, като за целта задължително периодично преглежда ограниченията за достъп и класификациите на важните активи, като взема под внимание приложимите политики за контрол на достъпа и осигурява правилно обработване, когато активът бъде изтрит или унищожен.

Чл.9./1/ Служителите и потребителите от външна страна /доставчици на различни услуги по поддръжка и др./, които използват или имат достъп до активите на общината се уведомяват за изискванията за сигурност на информацията на активите на организацията, свързани с информацията, средствата и ресурсите за обработка на ЛД.

/2/ Всички служители и потребители от трета страна при прекратяване на техните правоотношения, договор или споразумение се задължават да върнат всички притежавани от тях ЛД за служители или клиенти, както и активи на Община Гърмен

на прекия си ръководител, системния администратор или на Длъжностното лице по защита на личните данни.

/3/ В случаите, когато служител или потребител от външна страна използва свое собствено устройство, се спазват процедури, които да гарантират, че цялата информация е предадена на системния администратор и на Длъжностното лице по защита на личните данни и е изтрита надеждно от устройството.

/4/ В случаите, когато служител или потребител от външна страна има познание, което е важно за текущата работа, тази информация се документира и предава на прекия ръководител.

/5/ През периода на предизвестие за прекратяване, прекият ръководител контролира неоторизираното копиране на съответна информация /например интелектуална собственост или ЛД/ от служители с договор в процес на прекратяване.

IV. 1. Класифициране на информацията.

Чл.10./1/ Информацията се класифицира според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране.

/2/ Активи извън информацията също могат да бъдат класифицирани в съответствие с класифицирането на информацията, която е съхранявана на тях, обработвана от тях или по друг начин манипулирана или защитавана от актива.

/3/ Нивото на защита се оценява чрез анализиране на поверителността, цялостността и наличността и всички други изисквания за съответната информация.

/4/ Собствениците на информационни активи носят отговорност за тяхното класифициране.

Чл. 11. /1/ Всяко ниво на класификация се определя с дефинирано име, което е смислено в контекста на прилагането на схемата за класифициране. При класифицирането и свързаните с него защитни механизми за контрол на информацията се вземат под внимание нуждите на дейността за споделяне или ограничаване на информацията, както и изискванията на нормативните актове.

/2/ Процесът по класифициране Община Гърмен се спазва така, че всеки да класифицира информацията и свързаните с нея активи по един и същ начин, като има общо разбиране за изискванията за защита и тяхното прилагане.

/3/ Класифицирането е последователно съгласуван процес, който е част от процесите на Община Гърмен. В него се включва, задаване на критерии за преглед на

класифициране във времето, както и подписване на споразумения за поверителност. Резултатите от класифицирането отчитат стойността на активите в зависимост от тяхната чувствителност и критичност /напр. гледна точка на поверителност, цялостност и наличност/ и се обновяват в съответствие с измененията на стойността, чувствителността и критичността на активите през техния жизнен цикъл.

/4/ Класифицирането на информацията предоставя на оторизираните лица сбита индикация как да работят с нея или да я защитават. Създаването на групи от информация със сходна необходимост от защита и специфицирането на процедури за сигурност на информацията, които са приложими за цялата информация във всяка група, улеснява това. Този подход намалява необходимостта от оценяване на риска за всеки отделен случай и от създаване на собствени механизми за контрол.

Чл.12. /1/ Класифицирането на информацията в Община Гърмен се извършва в съответствие със Закона за защита на класифицираната информация. За всяка информационна ценност се препоръчва да бъде описана следната информация:

1. Тип: оборудване, програма, данни оборудване, програма, данни.
2. Използва се в система с общо предназначение или в критично приложение.
3. Отговорният за дадената информационна.
4. Нейното физическо или логическо местоположение.

/2/ Нивата на класификация за сигурност на информацията и техният гриф за сигурност са:

1. "Строго секретно";

2. "Секретно";

3. "Поверително";

4. "За служебно ползване".

/3/ Информацията, класифицирана като държавна тайна, се маркира с гриф за сигурност:

1. *"Строго секретно"* - в случаите, когато нерегламентиран достъп би застрашил в изключително висока степен суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на непоправими или изключително големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

2. *"Секретно"* - в случаите, когато нерегламентиран достъп би застрашил във висока степен суверенитета, независимостта или териториалната цялост на Република

България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на трудно поправими или големи вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред;

3. *"Поверително"* - в случаите, когато нерегламентиран достъп би застрашил суверенитета, независимостта или териториалната цялост на Република България или нейната външна политика и международни отношения, свързани с националната сигурност, или би могъл да създаде опасност от възникване на вреди, или да причини такива вреди в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

4. Информацията, класифицирана като служебна тайна, се маркира с гриф за сигурност "*За служебно ползване".*

/4/ Информацията може да престане да бъде чувствителна или критична след определен период от време /напр. когато информацията стане обществено достъпна/. Тези аспекти се вземат под внимание, тъй като прекалено класифицираната информация води до внедряването на ненужни механизми за контрол, в резултат на което може да се получат допълнителни разходи или обратно, недостатъчно класифицираната информация може да застраши постигането на целите на дейността.

IV. 2. Работа с информационни носители.

Чл.13./1/ Процесите за сигурно унищожаване на носители са управляеми, за да се намали до минимум рискът от изтичане на поверителна информация и лични данни към неоторизирани лица.

/2/ Прилаганите способи за сигурно унищожаване на носители, съдържащи поверителна информация, са пропорционални/съизмерими на чувствителността на тази информация.

/3/ Носителите, съдържащи поверителна информация, включително специална категория лични данни, се съхраняват и унищожават по сигурен начин /напр. чрез изгаряне, нарязване или изтриване на данни/.

/4/ Периодично се извършва идентификация на обектите, които изискват сигурно унищожаване. Всяко унищожаването на чувствителна информация се документира.

/5/ За повредените устройства, съдържащи чувствителни данни или специална категория лични 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 внимателно като се отчитат редица фактори като опита, прилагането на адекватни механизми за контрол и др.

/8/ Задължително да се документира с протокол избора на външна страна/ доставчик за унищожаване на носители на информация и лични данни.

V. ПОЛИТИКА ЗА КОНТРОЛ НА ДОСТЪПА.

Чл.14./1/ Кметът на Община Гърмен, секретарят на Община Гърмен, системният администратор, длъжностното лице по защита на данните или друго определено лице, определят подходящи правила за достъп, права за достъп и ограничения за специфични/конкретни потребителски права по отношение на техните активи с необходимото количество механизми за контрол, отразяващи свързаните със сигурността на информацията рискове.

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

/3/ На потребителите и доставчиците на услуги ясно са изложени изискванията, на които трябва да отговарят механизмите за контрол на достъпа.

/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, например принципът „необходимо е да знае” и нивата на сигурност на информацията и класифицирането на информацията;
3. правата за достъп и политиките за класифициране на информацията за системи и мрежи;
4. съответното законодателство и всички договорни задължения, отнасящи се до ограничаване на достъпа до данни или услуги;
5. управлението на правата на достъп в разпределена и мрежова среда;

6. разделянето на ролите за контрол на достъпа /напр. заявка, оторизиране на достъпа, администриране на достъпа/;
7. изискванията за официално оторизиране на заявките за достъп;
8. изискванията за периодичен преглед на правата на достъп;
9. отнемането на права на достъп;
10. архивирането на записите на всички значими събития, засягащи използването и управлението на идентичността на потребителите и тайната информацията за автентификация;
11. ролите с привилегирован достъп.

/5/ Когато се специфицират правилата за контрол на достъпа се отчитат следните изисквания:

1. да се прилагат правила основани на предпоставката „всичко е забранено, освен ако не е изрично разрешено”, а не на правилото „всичко е разрешено, освен ако не е изрично забранено”;
2. измененията в етикетите на информацията, които са автоматични от средствата за обработка на лични данни и информация и тези по усмотрение на потребителя;
3. измененията в разрешенията за потребителя, които са автоматични от информационната система и тези, които са от системния администратор;
4. правилата, които изискват специално одобрение преди да влязат в сила и тези, които не изискват одобрение.

/6/ Правилата за контрол на достъпа се подкрепят от официални процедури и дефинирани отговорности, като прекия ръководител информира Системния администратор и длъжностното лице по защита на данните от какви права се нуждае съответния служител.

/7/ Използваните принципи, насочващи политиката по контрол на достъпа, са:

1. Необходимост да се знае: предоставя се достъп само до информация само на лица, които имат нужда, за да изпълняват своите задачи /различни задачи/роли означава различно „необходимост е да знае” и следователно различен профил за достъп/;
2. Необходимост да се ползва: предоставя се достъп на лица само до средствата за обработка на информация /ИТ устройства, приложения, процедури, стаи и помещения/, от които лицата имат нужда, за да изпълняват своите задачи/работа/роли.

/8/ 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 /например използване на VPN или безжична мрежа/;
5. изискванията за автентифициране на потребителя за достъп до различни мрежови услуги;
6. наблюдаване на използването на мрежови услуги.

Чл.15. Политиката по използване на мрежови услуги е съобразена с политиката за контрол на достъпа на Община Гърмен. Системният администратор на Община Гърмен е задължен да докладва на Секретаря на Общината за всички опити за неоторизиран достъп до мрежите на общината.

V. 1. Управление на достъпа на потребителите.

Чл.16. /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; 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;
2. незабавно забраняване или отстраняване на потребителски идентификатор за потребители, които са напуснали Община Гърмен;
3. периодично идентифициране, отстраняване или забраняване на излишни потребителски идентификатори;
4. Системният администратор на Община Гърмен гарантиране, че излишните потребителски идентификатори не са издадени на други потребители.

Чл.17. /1/ Предоставянето или отменянето на достъп до информация или средства за обработка на информация на Община Гърмен, 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/ Предоставянето или отменянето на достъп до информация или средства за обработка на информация на Община Гърмен се извършва от системния администратор на общината по нареждане на Директор дирекция, зам.-кмет, секретар на общината или Кмет на общината.

/3/ Кметовете на кметства получават или им се отнемат права от момента на избора/ назначаването им или момента на прекратяване на техните правомощия.

/4/ Процесът осигуряващ присвояване или отнемане на права на достъп, предоставен на потребителски идентификатор се управлява от системния администратор на Община Гърмен, отразява се в Дневника на администратора или използваната тикетинг системи и, включва:

1. получаване на оторизация от администратора на информационната система или услуга за използване на информационната система;
2. верифициране /проверяване/, че предоставеното ниво за достъп е в съответствие с изискванията и да е свързано с разделяне на задълженията;
3. гарантиране, че правата на достъп не са активирани, преди да бъдат завършени процедурите за оторизиране/разрешаване;
4. поддържане на дневник от системния администратор, отразяващ предоставените права на достъп на потребителските идентификатори за достъп да информационните системи и услуги;
5. адаптиране на правата на достъп на потребители, които са променили ролите или работата /службата/ си и незабавно премахване или блокиране на права на достъп на потребители, които са напуснали организацията;
6. периодично преглеждане на правата на достъп със собствениците на информационни системи и услуги –документиране на действието от администратора.

/5/ Обръща се внимание и на даването на достъп на потребители, основано на изискванията на дейността - определен брой права в типичните профили за достъп.

Чл.18. /1/ Заявките за достъп и прегледите се управляват на ниво задълженията служителите от съответния отдел/ дирекция, 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 определят съответните санкции към лицата и мерки за защита.

Чл.19 /1/ Предоставянето на привилегировани права за достъп се контролира чрез процес на оторизиране от системния администратор, които трябва да може да докаже във всеки един момент от кого е получил нареждане за даване на привилегировани права. Идентифицират се права за достъп с привилегии, свързани с всяка система или процес /приложение/.

/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/ Задължително се поддържа процес на оторизиране и запис на всички предоставени привилегии от Системния администратор.

/4/ Привилегиите за достъп не се предоставят, докато не бъде завършен процесът на оторизиране, като се дефинират изисквания за крайния срок на привилегиите за достъп.

/5/ Привилегиите за достъп се предоставят на потребителски идентификатор, който е различен от тези за редовните дейности. Редовните дейности не се изпълняват от привилегирован идентификатор.

/6/ Компетентността на потребителите с привилегии за достъп се преглеждат периодично, за да се провери дали те са в съответствие с техните задължения.

V. 2. Управление на тайната информация за автентификация на потребителите.

Чл.20. /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 наемане на работа;

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, тайна информация за автентификация;
4. временната поверителна информация за автентификация се дава на потребителите по защитен начин; използването на външни страни или незащитени /чрез явен текст/ електронни пощенски съобщения се избягва;
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.21. Паролите са общо използван тип поверителна информация за автентификация и са често срещано средство за верифициране /проверяване/ на идентичността на потребителя. Може да се използва поверителна информация за автентификация чрез криптографски ключове и други данни, съхранявани на хардуерни носители /например смарт карти/, които произвеждат кодове за автентификация.

Чл. 22. /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 назначението.

/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/ информация и услугите, се отнемат, редуцират или спират.

/5/ Промените в назначението се регистрират от системния администратор в отнемането на всички права за достъп, които не са били одобрени за новото назначение.

/6/ 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, идентификационни карти, средства за обработка на информация или абонаменти.

/7/ Във всяка документация, в която се идентифицирани права за достъп на служителите и доставчиците, се отразяват отнемането и/или промяната на правата за достъп.

/8/ В случаите, когато напускащият служител или потребител от външна страна има известни пароли за потребителска идентификация, които са останали активни, те се променят при прекратяване или промяна на назначението, договора или споразумението.

/9/ Отговорност за прекратяване и промяна на права носят системния администратор, секретаря на общината и длъжностното лице по защита на личните данни.

Чл. 23. /1/ При определени обстоятелства могат да бъдат предоставяни права за достъп на основание на факта, че са валидни за повече хора /например групови идентификатори/, а не само за напускащия служител или потребител от трета страна. В такива случаи, напускащите лица се заличават от списъците за групов достъп, с указания към другите служители и потребители от трета страна повече да не споделят информация с напускащото лице.

/2/ В случаите на прекратяване по инициатива на ръководството, недоволните служители или потребители от външна страна могат преднамерено да повредят информация или да саботират средства за обработка на информация.

/3/ Ограниченията за достъп се основават на индивидуални изисквания за приложенията на дейността и в съответствие с дефинираната политика за контрол на достъпа.

/4/ За да се повишат изискванията за ограничаване на достъпа Системния администратор на общината взема под внимание следните факти:

1. предоставяне на менюта за контрол на достъпа до функции на приложната система;
2. контрол до кои данни може да има достъп конкретен потребител;
3. контрол върху правата за достъп на потребителите /напр. четене, писане, изтриване и изпълнение/;
4. контрол върху правата за достъп на други приложения;

5. ограничаване на информацията, съдържаща се на изходите и предоставяне на механизми за контрол на физическия и логическия достъп за изолиране на чувствителни приложения, данни на приложения или системи.

V. 3. Система за управление на пароли.

Чл.24. /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, когато е необходимо и поддържа запис на предишни пароли и предотвратява повторното им използване.

/4/ При въвеждане паролите не ги изобразява на екрана, не съхранява файловете с пароли отделно от данните за приложната система и съхранява и предава пароли в защитена форма.

Чл.25. /1/ Служителите на Община Гърмен използват следните правила за управление на паролите:

1. Минималната дължина на паролите за достъп до информационните ресурси на общината и до потребителските станции е осем 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. Използването на една и съща парола в срок по-дълъг от четири месеца не е позволено.
4. Настройката на паролите е отговорност на Системния администратор, а техният преглед е отговорност на ръководството или упълномощен от него служител или външен експерт – системен 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/организацията.

/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. 26. /1/ В резултат на оценката на риска се идентифицира изискваното ниво на защита, отчитайки типа, силата и качеството на допустимо използваните алгоритми за криптиране.

/2/ При внедряване на криптографската политика на общината се вземат под внимание нормативните актове и националните ограничения, които са приложими към използването на криптографски техники в различните страни, както и въпросите на трансграничния поток на криптирана информация.

Чл. 27. /1/ Методите за криптиране се използват при защита на информацията, предавана по мобилни устройства, устройства със сменяеми носители или по комуникационни линии. Също така се определят и методите за защита на криптографски ключове, както и възстановяването на криптирана информация в случай на изгубени, компрометирани или повредени ключове.

/2/ Криптографските механизми за контрол могат да се използват за постигане на различни цели на сигурността на информацията като например:

1. поверителност - криптиране на информацията за защита на чувствителна или критична информация и специални категории лични данни, съхранявана или предавана;
2. цялостност/автентичност - цифрови подписи или кодове за автентификация на съобщения, за да се проверява автентичността или цялостността на съхранената или предавана чувствителна или критична информация;
3. неотхвърляемост - криптографски техники за предоставяне на свидетелство за възникването или невъзникването на събитие или действие;
4. автентификация - криптографски техники за автентифициране на потребителите и други системни единици, които заявяват достъп до или взаимодействат със системните потребители, единици или ресурси.

Чл.28. /1/ Вземането на решение дали едно криптографско решение е подходящо, се разглежда като част от по-широкия процес на оценка на риска и избиране на механизми за контрол и се преценява от системния администратор, а при необходимост и от секретаря на общината и длъжностното лице по защита на личните данни.

/2/ Процедурата по ал.1 се използва, за да се определи дали криптографският механизъм за контрол е подходящ, какъв тип механизъм за контрол трябва да се приложи, с каква цел и за какви процеси на дейността.

/3/ Политиката по използване на криптографски механизми за контрол увеличава максимално ползите при минимизиране на рисковете при използване на криптографски техники, с което се избягва неподходяща или неправилна употреба.

/4/ Изборът на подходящи криптографски механизми за контрол се прави, за да се изпълнят целите на политиката за сигурност на информацията.

**Забележка:*

Препоръчително е да се използват доказани стандартни алгоритми като DES, Triple DES, Blowfish, RSA, AES и IDEA като основа при криптиращите технологии. Тези алгоритми представляват реалния шифър, използван за дадено одобрено приложение. Дължината на симетричните ключове при използваните системи за криптиране трябва да бъде най-малко 56 бита. Асиметричните от своя страна трябва да бъдат със съответната дължина, за да предоставят исканото ниво на защита на данните. Изискванията към дължината на ключовете периодично се преглежда и обновява.

Чл.29. /1/ Употребата на собствени алгоритми за криптиране не е позволена, докато те не бъдат прегледани и одобрени от квалифицирани експерти извън организацията, разработила алгоритмите.

/2/ Всеки служител, който наруши тази политика е обект на дисциплинарно наказание. Обучение на служителите по прилаганите от Община Гърмен криптографии се осъществява от системния администратор на общината или от външна организация.

/3/ Управление на ключове включва изисквания за управление на криптографски ключове през целия им жизнен цикъл, включително генериране, съхраняване, архивиране, възстановяване, разпределение, отмяна и унищожаване на ключове.

/4/ Процесите свързани с избирането на криптографски алгоритми, дължини на ключове се базират на широкото им използване според най-добрите практики. Подходящото управление на ключове изисква сигурни процеси за генериране, съхраняване, архивиране, възстановяване, разпределение, отмяна и унищожаване на криптографски ключове.

/5/ Всички криптографски ключове са защитени от модифициране и загуба. Личните ключове постоянно имат нужда от защита срещу неоторизирано използване и разкриване. Устройствата, използвани за генериране, съхранение и архивиране на ключове, са защитени физически.

/6/ Системата за управление на ключове се основава на съгласувано множество от стандарти, процедури и сигурни методи за:

1. генериране на ключове за различни криптографски системи и различни приложения;
2. издаване и получаване на сертификати за публичен ключ;
3. разпределяне на ключове за избрани субекти, включително как да бъдат активирани ключовете, когато бъдат получени;
4. съхраняване на ключове, включително как оторизираните потребители получават достъп до ключове;
5. промяна или обновяване на ключове, включително правила за това кога трябва да бъдат променяни ключове и как ще бъде направено това;
6. справяне с изложени на риск ключове;
7. отменяне на ключове, включително как да бъдат оттегляни или деактивирани ключове, например когато ключове бъдат изложени на риск или когато потребителят напусне организацията /като в този случай ключовете трябва да бъдат и архивирани/;
8. възстановяване на изгубени или повредени ключове;
9. резервиране или архивиране на ключове;
10. унищожаване на ключове;
11. записване и одитиране на дейностите, свързани с управлението на ключове.

Чл. 30. /1/ За да се намали вероятността от неправилна употреба, активиране и деактивиране на ключовете, се дефинират дати за ключовете, така че ключовете да могат да се използват само за периода, дефиниран в съответната политика за управление на ключове.

/2/ За да се управляват сигурно секретни и частни ключове, се взема под внимание и автентичността на публичните ключове. Този процес на автентификация се извършва като се използват сертификати на публичните ключове, които обикновено се издават от сертификационен орган. Този орган трябва да е призната организация с подходящи механизми за контрол и процедури за предоставяне на изискваната степен на доверие.

/3/ Управлението на крипотграфските ключове е от съществено значение за ефикасността на криптографските техники. ISO/IEC 11770 [2][3][4] предоставя по-нататъшна информация за управлението на ключове. Криптографските техники могат да се използват и за защита на криптографски ключове.

VII. ФИЗИЧЕСКА СИГУРНОСТ И СИГУРНОСТ НА ЗАОБИКАЛЯЩАТА СРЕДА.

Чл. 31. /1/ В община Гърмен 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/ Организира се физическа зона за достъп или други средства за контрол на физическия достъп до мястото или сградата; достъпът до местата и сгради е ограничен и е само за служители чрез карти за достъп. ?

/3/ Където е приложимо, се изграждат физически бариери за предотвратяване на неоторизиран физически достъп. Достъпът на граждани е уреден в правилата за Пропускателен режим в сградата на община Гърмен.

/4/ Всички противопожарни врати се обхващат от видеонаблюдение, за да бъдат наблюдавани и проверявани. Те действат в съответствие с правилата за противопожарна безопасност и охрана. Така се осигурява необходимото ниво на устойчивост в съответствие с приложимите местни, национални и международни стандарти.

Чл.32. /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 посетителите се дава достъп само за конкретни помещения на общината за обслужване на граждани. Самоличността на посетителите се автентифицира чрез пряка проверка на документи за самоличност.

/3/ Всички служители, доставчици и външни посетители са видимо идентифицируеми. В случаи на непридружавани посетители и липса на видима идентификация незабавно се уведомява отговорника по сигурността.

/4/ На лица от поддържащия персонал /външни организации за поддръжка, ремонт и обслужване/ се дава ограничен достъп до зоните за обработка на лични данни или до средствата за обработка на чувствителна информация, като тяхното присъствие следва да бъде наблюдавано от служител на общината, който да не ги оставя без надзор.

/5/ Правата за достъп до различните зони в общината редовно следва да се преглеждат и обновяват на 6 месеца, а при необходимост да се отнемат.

VII. 1. Сигурност на окабеляването.

Чл.33. /1/ Захранващите и телекомуникационните линии към средствата за обработка на информация се заземяват, където е възможно, или се защитават адекватно по алтернативен начин. Захранващите кабели се разделят от комуникационните кабели, за да се предотвратят смущения.

/2/ При необходимост и по решение на кмета на общината се инсталират армирани изолационни тръби и заключващи се кутии в местата за преглед и в крайните точки. При необходимост се използват електромагнитни екрани за защита на кабелите.

/3/ На 12 месеца, по утвърден план от секретаря на общината, се извършват технически и физически прегледи за неоторизирани устройства, прикачени към кабелите. При потребност от ремонт на окабеляването, се осигурява контролиран достъп за поправката винаги в присъствието на служител на общината.

VII. 2. Ненадзиравани потребителски устройства.

Чл.34. /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, 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.

/4/ Екраните на служителите са настроени за автоматично заключване при режим на неизползване на 3 минути.

VII. 3. Политика за чисто бюро и чист екран.

Чл.35. /1/ При спазването на Политиката за чисто бюро и чист екран се взема предвид нивото на класификация на информацията, законовите и договорните изисквания, както и съответните културни и рискове аспекти на организацията.

/2/ Отчитат се следните указания:

1. личните данни, чувствителната или критичната информация, било то на хартия или на електронен носител, се съхранява 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.36. /1/ За да се предотврати неоторизираното използване на фотокопия, технология за възпроизвеждане /сканиращи устройства, цифрови камери/ или носители, съдържащи чувствителна/класифицирана информация, те незабавно се премахват от служителите печатащите устройства и се прибират на указаните места.

/2/ Забранява се на служителите на общината да оставят на бюрата си 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 съгласно практиката на общината.

/3/ Политиката за чисто бюро/чист екран намалява рисковете от неоторизиран достъп, загуба и повреда на информация по време на или извън обичайното работно време.

/4/ Сейфове или други средства за сигурно съхраняване също могат да защитят информацията, съхранявана в тях от бедствия, като пожар, земетресение, наводнение или експлозия.

/5/ 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.

VIII. 1. Инсталиране и конфигуриране на системи.

Чл.37. /1/ На служителите се забранява инсталирането на нелицензиран софтуер и използването на други продукти, което представлява нарушение на правата върху интелектуална собственост.

/2/ Системният администратор инсталира и конфигурира, като:

1. Устройството се изключва от захранването.

2. Всички допълнителни източници /ако има такива/ на захранване /батерии, акумулатори и пр./ се отстраняват.

3. Ако устройството съдържа носители на информация /карти с памет, твърди дискове, USB външни запаметяващи устройства и пр./, те се изключват или, ако това е невъзможно, информацията се бекъпва преди изпълнението на стъпка 1.

3. Извършва се промяна на конфигурацията.

4. Включват се допълнителните източници на захранване /ако има такива/.

5. Устройството се включва в захранването.

6. Извършват се тестове за работоспособността на устройството.

7. Устройството се счита за въведено в експлоатация./

/3/ Системният администратор на Общината Гърмен 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.

VIII. 2. Управление на измененията.

Чл.38 /1/ Когато прави изменения, системният администратор съхранява в дневник информация за извършените изменения.

/2/ При извършването на изменения системният администратор взема под внимание следните случаи:

1. идентифицира и записва значителните изменения;
2. планира и изпитва измененията;
3. извършва оценка на потенциалните въздействия, включително въздействия върху сигурността на личните данни и информацията на такива изменения;
4. изисква официално одобрение за предложени изменения;
5. съобщава подробностите за измененията на всички съответни лица;
6. в състояние е да извърши прекратяване и възстановяване от неуспешни изменения и непредвидени събития;

7. извършва извънредни изменения за гарантиране на бързо и контролирано внедряване на измененията, необходими за разрешаване на инцидент.

VIII. 3. Механизми за контрол срещу злонамерен софтуер.

Чл. 39. /1/ Системният администратор на общината осъществява откриване и възстановяване от злонамерен софтуер, и управлението на измененията.

/2/ 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, с 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;

10. изолиране на среди, където могат да се получат катастрофални въздействия.

/3/ Използването на два или повече софтуерни продукти, които предпазват от злонамерен софтуер в средата за обработка на лични данни и информация могат да подобрят ефикасността на защитата от злонамерен софтуер.

**Забележка:*

При определени условия защитата от злонамерен софтуер може да причини смущение в работата. Използването единствено на софтуер за откриване на злонамерен софтуер и софтуер за възстановяване има нужда от придружаващи работни процедури, които предотвратяват въвеждането на злонамерен софтуер.

VIII. 4. Резервиране на информация.

Чл.40 /1/ При извършване или организиране действието резервиране, системният администратор на общината прилага строго определени правила.

/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 общината, изискванията за сигурност на включената информация и критичността на информацията за непрекъснатост на работа;
3. резервните копия да се съхраняват на отдалечено място, на достатъчно разстояние, за да се избегне повреда от бедствие на главното място;
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/ проверяват, 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. 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;
7. в случаи когато е важна поверителността, резервирането може да бъде защитено чрез криптиране.

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

администратор отразява извършената проверка в Дневника на администратора или по друг подходящ начин, определен от него.

/4/ В случай на критични системи и услуги резервирането обхваща цялата системна информация, приложения и данни, необходими за възстановяване на цялата система в случай на бедствие. Периодът на запазване на съществената информация за дейността се определя, като се вземат под внимание изискванията за постоянно запазване на архивни копия.

VIII. 5. Регистриране на събития.

Чл.41. /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/ Прието е правилото системните администратори да не изтриват или деактивират дневници /записите/логовете/ за своите собствени действия.

/3/ Дневниците на събития включват:

1. идентификатори на потребителите;
2. работа /дейности/ на системата;
3. дати, време и подробности за ключови събития, например влизане и излизане;
4. идентичност на устройство или местоположение, ако е възможно, и системен идентификатор;
5. записи на успешни и отхвърлени опити за достъп до системата;
6. записи на успешни и отхвърлени опити за достъп до данни и други опити за достъп до ресурси;
7. изменения на системната конфигурация;
8. използване на привилегии;
9. използване на системни помощни програми и приложения;
10. файлове, до които е имало достъп, и вид на достъпа;
11. мрежови адреси и протоколи;
12. алармени сигнали, издадени от системата за контрол на достъпа;
13. активиране и деактивиране на защитни системи, като антивирусни системи и системи за откриване на нарушители;
14. записи на транзакции, изпълнени от потребителите в приложенията.

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

VIII. 6. Защита на регистрираната информация.

Чл.42. /1/ Целта е защита от неоторизирани изменения на регистрираната информация и проблеми в работата със средствата за регистриране.

/2/ Защита включва и изменения на:

1. видовете записвани съобщения;
2. файловете за регистриране, които се редактират или изтриват;
3. надхвърляне на капацитета за съхранение на носителите на файл за регистриране, което води или до отказ да се записват събития, или до презаписване на предишни записани събития.

Чл.43. /1/ Регистрите на системата често съдържат голям обем информация, повечето от която е странична за мониторинга на сигурността на информацията. В помощ на идентифицирането на значимите събития за целите на мониторинга на сигурността на личните данни и информацията се взема под внимание автоматичното копиране на съответни видове съобщения във втори регистър или използването на подходящи системни помощни програми/софтуер или инструменти за одит за изследване и рационализиране на файлове.

/2/ Регистрите на системата се защитават, защото ако данните могат да бъдат изменяни или изтривани, тяхното съществуване може да създаде невярно чувство за сигурност.

/3/ Копирането в реално време на регистри в система извън контрола на системния администратор или оператор може да се използва за предпазване на регистрите.

VIII. 7. Дневници на действията на системния администратор и оператора.

Чл.44. /1/ Притежателите на акаунти на привилегирован потребител може да са в състояние да манипулират дневниците /регистрите/ на средствата за обработка на информация, които са под техен пряк контрол, и затова е необходимо да се защитават и преглеждат дневниците /регистрите/, за да се поддържа отчетност за привилегированите потребители.

/2/ Може да се използвана система за откриване на нарушители, управлявана извън контрола на системните и мрежовите администратори за да се наблюдават за съответствие на дейностите на системната и мрежовата администрация.

VIII. 8. Синхронизация на часовниците.

Чл.45. /1/ Дефинирано е стандартно опорно време за използване чрез получаване на опорно време от външен/и/ източник/ци/ и надеждно синхронизирани вътрешните часовници.

/2/ Правилното настройване на компютърните часовници е важно за осигуряване на точността на дневниците от одит, което се изисква за разследване или като доказателство при правни или дисциплинарни дела.

/3/ Неточните дневници от одит може да възпрепятстват такива разследвания и да повредят достоверността на такива доказателства.

/4/ Използва се мрежов протокол за време с цел поддържане на всички сървъри в синхрон с главния часовник.

VIII. 9. Управление на техническите уязвимости.

Чл.46. /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/ Специфичната информация, необходима за поддържане на управлението на техническата уязвимост включва доставчика на софтуера, номерата на версиите, текущото състояние на разгръщането /например какъв софтуер е инсталиран на кои системи/ и лицето в организацията, отговарящо за софтуера.

/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 и за поддръжка на осъзнаването им, за софтуера и друга технология /основана на списъка на активи на Община Гърмен/; тези информационни ресурси се обновяват въз

основа на измененията в описа или когато бъдат намерени други нови или полезни ресурси;

3. след идентифицирането на потенциална техническа уязвимост общината идентифицира свързаните с нея рискове и действията, които трябва да бъдат предприети; такова действие може да включва поправка на уязвими системи или прилагане на други механизми за контрол;
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;
9. дефинира се регламент за справяне със случаи, при които е била идентифицирана уязвимост, но няма подходящи контрамерки. В такъв случай системният администратор на общината преценява рисковете, свързани с известната уязвимост и дефинира подходящи действия за откриване и коригиране.

IX. СИГУРНОСТ НА КОМУНИКАЦИИТЕ.

Чл. 47. /1/ Целта на политиката е да осигури защита на информацията в мрежите и поддържащите ги средства за обработка на информация.

/2/ Атаките насочени към компютърните мрежи на Община Гърмен могат да бъдат организирани отвън или отвътре на локалната мрежа. Поради по-лесният достъп до данни и услуги, атаките от вътрешността на локалната мрежа са по-често използваните методи за кражба на фирмени конфиденциални данни. В средата на Windows, Microsoft предлага решения и инструменти за централизирано администриране на вътрешната сигурност на корпоративната компютърна мрежа.

/3/ Груповите политики за сигурност /Group Policy/ в MS Windows предлагат конфигуриращи настройки, които могат да се прилагат централизирано върху обекти в домейна в това число работни станции и потребителски акаунти.

/4/ Груповите политики са тясно свързани със структурата в Община Гърмен и се прилагат в среда на Microsoft. Те се използват за управление на работните среди на потребителите, групирани в определен организационен модул.

/5/ Управлението на работните среди на потребителите, включва разработване и ограничения на потребителската работна площ /Desktop/, налагане на ограничения върху използваният приложен софтуер, налагане на криптирано предаване на данни по мрежа, ограничения на използваните мрежови протоколи и ограничаване на интернет достъпа.

/6/ В среда на MS Windows има предварително разработени от Microsoft групови политики наречени Default Group Policy. Тези политики налагат ограничения и започват да се прилагат независимо дали сме решили или не да използваме групови политики. Администраторът на груповите политики има възможност да създава нови Group Policy като ги настройва в зависимост от изискванията за сигурност в компанията и нейната организационна структура.

/7/ За правилното планиране и разработване вътрешната сигурност в Windows е препоръчително да се създаде структура в Active Directory на базата на организационни модули /Organizational Unit/ отговаряща на организационната структура. Organizational Unit могат да отговарят на бизнес структурата или на регионално разпределение на офисите.

/8/ Разделянето на служителите в отделни Organizational Units обединява потребителите с еднакви служебни задължения и отговорности. Налагането на политики за сигурност върху добре организирана структура от Organizational Units подобрява администрирането, намалява вероятността от администраторски грешки и увеличава ефективността от груповите стратегии за сигурност.

/9/ Използването на групови политики за сигурност позволяват централизирано да се менажират работните станции и потребителските акаунти. Налагането на ограничения увеличава ефективното използване на интернет връзката, повишава работната ефективност на служителите и намалява риска от кражба на конфиденциални данни.

IX. 1. Механизми за контрол на мрежите.

Чл.48. /1/ Защита на информацията в мрежите и поддържащите ги средства за обработка на информация, се извършват по определен ред.

/2/ За изпълнение на задължението по ал.1 се взимат под внимание следните дейности:

1. установяват се отговорностите и процедурите за управление на мрежовите средства;
2. разделяне на оперативната отговорност за мрежите от компютърните операции, където е приложимо;
3. установяват се специални механизми за контрол, за да се предпазва поверителността и цялостността на данните, преминаващи по обществени мрежи или по безжични мрежи и да се защитават свързаните системи и приложения;
4. прилагат се регистриране и мониторинг, за да се позволи записването и откриването на действия, които могат да засегнат или се отнасят за сигурността на информацията;
5. дейностите на ръководството се координирани както за оптимизиране на услугата/обслужването за организацията, така и за да е сигурно, че механизмите за контрол са последователно прилагани в инфраструктурата за обработка на информация;
6. системите по мрежите да бъдат автентифицирани;
7. системната връзка към мрежата да бъде ограничена.

IX. 2. Сигурност на мрежови услуги.

Чл.49. /1/ Мрежовите услуги включват предоставянето на връзки, услуги от частни мрежи и мрежи с добавена стойност и управлявани решения на мрежовата сигурност, като защитни стени и системи за откриване на нарушители. Тези услуги могат да обхващат от проста неуправлявана ширина на честотната лента до сложни предложения с добавена стойност.

/2/ Характеристиките на сигурността на мрежовите услуги са - технологията, приложена за сигурност на мрежовите услуги, като автентификация, криптиране и механизми за контрол на мрежовата връзка; техническите параметри, изисквани за сигурна връзка с мрежовите услуги в съответствие с правилата за сигурност и мрежова

връзка; процедури за използване на мрежовата услуга за ограничаване на достъпа да мрежови услуги и приложения, където е необходимо..

IX. 1. Обмен на информация.

Чл.50. /1/ Служителите на общината не трябва да провеждат поверителни разговори на обществени места или по несигурни комуникационни канали, отворени офиси и места за среща.

/2/ Обмен на информация става чрез използване на определен брой различни типове средства за комуникация, включително електронна поща, глас, факсимиле и видео налични в общината.

X. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ.

Чл.51. /1/ С цел намаляване на риска и произтичащите от появата на инциденти и разходи в Община Гърмен е разработена и внедрена политика за управление на инциденти.

/2/ Всички служители се осведомяват, колкото е възможно по-бързо 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 уредбата на физическата сигурност;
6. неконтролирани изменения на системата;
7. неправилна работа на софтуер или хардуер;
8. нарушения на достъпа.

X. 1. Докладване за слабости в сигурността на личните данни информацията.

Чл.52. /1/ Всички служители на Община Гърмен докладват възникнали проблеми възможно по-бързо, за да се предотвратят инциденти със сигурността на информацията.

/2/ Служителите трябва 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.53. /1/ Община Гърмен предприема марки за реакция на инциденти със сигурността на информацията.

/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 последват 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, открит/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.

Първата цел на реагирането на инцидент е да се върне „нормалното ниво на сигурност” и след това да се започне необходимото възстановяване.

Чл.54. /1/ Информацията, придобита от преценяването на инцидентите със сигурността на личните данни и информацията, се използвана 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.

/3/ При обучението за осъзнаване на служителите могат да се използват примери с действителни инциденти със сигурността на личните данни и информацията, ако не се нарушава поверителността, с цел поуки от практиката /как да се реагира на такива инциденти и как да се избягват в бъдеще/.

XI. ПЛАНИРАНЕ НА НЕПРЕКЪСНАТОСТТА НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

Чл.55. /1/ Ръководството на Община Гърмен разбира необходимостта от планиране непрекъснатостта на процесите, свързани с личните данни. Увеличаващото се развитие на процеси, базирани на технологии и силната зависимост от информационните технологии е основание за създаване на план за действие при бедствия и аварии.

/2/ Планът се поддържа и тества, с цел установяване на пропуски и слабости.

/3/ Планът за действие при бедствия и аварии се съгласува с процедурите и мерките по управление на инциденти. Действията за възстановяване след прекъсвания или нарушения на сигурността се извършват от определени служители. Изискванията за сигурност на информацията са определени, когато се планира непрекъснатостта на дейността и възстановяването след бедствие.

/4/ При отсъствие на официално планиране на непрекъснатостта на дейността и възстановяването след бедствие управлението на сигурността на информацията се приема, че изискванията за сигурност на информацията остават същите при неблагоприятни случаи, в сравнение с нормалните работни условия.

Чл. 56. /1/ Община Гърмен може да направи анализ на въздействието върху дейността за аспектите на сигурността на личните данни и информацията, за да определи изискванията за сигурност на информацията, приложими при неблагоприятни случаи.

/2/ Според изискванията за непрекъснатост на сигурността на информацията общината 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.

XII. 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 Гърмен влизат в сила от датата на тяхното утвърждаването от Кмета на община Гърмен .

§.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.