**Утвърдил:**

**……………………….**

 **Управител**

 **ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В …………………………………….**

**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 Домът, в които се осъществява обработка на лични данни, включително чувствителна информация /ЛД/, а също така и за структурите, осигуряващи обслужването и нормалното функциониране на Дома.

**/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 Домът.

 **/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 и разпорежданията на Управителя на Дома.

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

 **/3/** Ръководството на Домът 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 Домът лични данни и в частност за приемане на остатъчните рискове.

 /4**/** Отговорност за сигурността за личните данни в Домът носят:

1. Лице/а обработващо/и лични данни – служители, медицински персонал, на които е възложено или част от задълженията им са свързани с обработване налични данни;
2. Служител от функционална област информационни технологии и сигурност в Домът и/или външен системен администратор.

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

**III. МЕРКИ ПО ОТНОШЕНИЕ НА СИГУРНОСТТА НА ЧОВЕШКИТЕ РЕСУРСИ.**

**Чл.3. /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 Управителя на Дома.

**/4/** Информацията за всички кандидати, които са обсъждани за позиции в Дома, 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 Дома по отношение на служителите на Домът 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.4 /1/** Служители, извършили нарушение в сигурността на информацията носят дисциплинарна отговорност по Кодекса на труда 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.5 /1/** Отговорностите и задълженията по отношение сигурността на личните данни при прекратяване на правоотношенията или промяна на заеманата длъжност 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/** Измененията на отговорностите се управляват, както при прекратяването на текущата отговорност или служба, така и при започването на нова отговорност или длъжност.

**/4/** Управителят на Дома 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.6 /1/** Всички активи, свързани с лични данни и средствата за обработка на информация са ясно идентифицирани от Домът и на тези активи е съставен и се поддържа точен опис, актуален, последователен и съответен на другите описи.

**/2/** Домът 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.7./1/** Служителите и потребителите от външна страна /доставчици на различни услуги по поддръжка и др./, които използват или имат достъп до активите на Дома 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 на Управителя на Дома.

**/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 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 Управителя на Дома.

**/5/** През периода на предизвестие за прекратяване, Управителя на Дома контролира неоторизираното копиране на съответна информация от служители с договор в процес на прекратяване.

*Работа с информационни носители.*

**Чл.8./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.9./1/** Управителят на Дома определя 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. политиките за разпространение и оторизиране на информация, например принципът „необходимо е да знае” и нивата на сигурност на информацията и класифицирането на информацията;
2. правата за достъп и политиките за класифициране на информацията за системи и мрежи;
3. съответното законодателство и всички договорни задължения, отнасящи се до ограничаване на достъпа до данни или услуги;
4. разделянето на ролите за контрол на достъпа /напр. заявка, оторизиране на достъпа, администриране на достъпа/;
5. изискванията за официално оторизиране на заявките за достъп;
6. изискванията за периодичен преглед на правата на достъп;
7. отнемането на права на достъп;
8. архивирането на записите на всички значими събития, засягащи използването и управлението на идентичността на потребителите и тайната информацията за автентификация;
9. 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. правилата, които изискват специално одобрение преди да влязат в сила и тези, които не изискват одобрение.

**/6/** 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.

**Чл.10. /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.11. /1/** Служителите на Домът използват следните правила за управление на паролите:

1. Минималната дължина на паролите за достъп до информационните ресурси на Домът 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. На потребителите се забранява да записват върху хартия или на друг носител паролите си за достъп до информационните ресурси и лични данни на администратора.
5. На потребителите се забранява да споделят под каквато и да е форма паролите си за достъп до информационните ресурси на администратора/организацията.

**VI. ФИЗИЧЕСКА СИГУРНОСТ И СИГУРНОСТ НА ЗАОБИКАЛЯЩАТА СРЕДА.**

**Чл. 12. /1/** В Домът 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;

**/3/** Достъпът на граждани и уреден в правилата за Пропускателен режим в сградата на Домът.

**Чл.13. /1/** Физическият достъп, датата и часът на влизане и излизане на служители и посетители се записва в съответствие с Пропускателен режим в сградата на Дома и правилата за видеонаблюдение.

**/2/** На посетителите се дава достъп само за конкретни помещения. 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 Управителя на Дома.

**/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 наДома, който да не ги оставя без надзор.

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

**VII. ПОЛИТИКА ЗА ЧИСТО БЮРО И ЧИСТ ЕКРАН.**

**Чл.14. /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.15. /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 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 Дома.

**/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. МЕХАНИЗМИ ЗА КОНТРОЛ СРЕЩУ ЗЛОНАМЕРЕН СОФТУЕР.**

**Чл. 16. /1/** Управителят на Дома осигурява 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.*

**IX. УПРАВЛЕНИЕ НА ИНЦИДЕНТИ.**

**Чл.17. /1/** С цел намаляване на риска и произтичащите от появата на инциденти и разходи в Домът 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.

**Чл.18. /1/** Домътпредприема 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.

**Чл.19. /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.

**/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/.

**X. ПЛАНИРАНЕ НА НЕПРЕКЪСНАТОСТТА НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.**

**Чл.20. /1/** Ръководството на Дома 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. 21. /1/** Домът 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 Домът 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………………………….. и влизат в сила от датата на тяхното утвърждаването от Управителя на Дома .

**§.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.