ПОЛИТИКИ ПО ИНФОРМАЦИОННА СИГУРНОСТ В МБАЛ „СВЕТИ МИНА” – ПЛОВДИВ ЕООД

Политика за контрол на достъпа

Политиката на МБАЛ „Свети Мина”-Пловдив ЕООД за контрол на достъпа е базирана на принципите „необходима е да знае” и „необходимо е да ползва” и минимализиране на привилегиите. Политиката за контрол на достъпа включва прилагането на механизми за контрол както на физическия, така и на логическия достъп.

Ръководствата на лечебното заведение прилага мерки на контрол на достъпа, които да осигуряват:

- Физическа защита на информационните активи;
- Достъп до съответните информационни активи в съответствие с установена матрица за достъп и на ръководството на организацията и само след официално оторизиране на заявките за достъп от страна на Управителя;
- Прилагане механизми за контрол на физическото влизане;
- Определяне на нивата на достъп в съответствие с ролята, която трябва да изпълняват служителите на лечебното заведение и нивата на класификация на информацията и активите;
- Отнемане на права на достъп при напускане;
- Периодичен преглед на достъпа и правата на достъп;
- Ъпгрейд на контрола на достъп в отговор на нови заплахи, възможности, изисквания на дейността или изводи от инциденти.

Политика за класифициране и обработка на информацията

Политиката за класифициране, обработване и съхранение на информацията и на физическите активи се основава на заинтересованите страни. Класификацията се извършва от собствениците на съответните активи/информация и включва три нива:

• А- Конфиденциална / критична

• В- За служебно ползване / с нормална важност

• С- Публична / не критична

Класификацията се извършва на база на стойността, чувствителността и критичността на информацията по време на целия й жизнен цикъл и потенциалните последствия, които компрометирането й би имало върху организацията.

Ниво А обхваща:

• Контакти на контрагенти/пациенти, служители

• База данни

• Информация за заплати, финансова информация от договори.

• Лични данни на служители (ЕГН/ЛНЧ, гражданство, семейно положение, постоянен адрес и копия на документи, удостоверяващи образование и квалификация, трудова дейност, банкова сметка и др.), на пациенти (ЕГН/ЛНЧ, гражданство, семейно положение, постоянен адрес, тел., имена, документ за самоличност, степен на образование)

Софтуер:

• Електронни подписи и спеиализиран софтуер.

Хардуер:

• Основен сървър, бекъп сървър, комуникационно оборудване (офиси),

Ниво В обхваща:

• Уеб сайт, възлагателни писма, договори с контрагенти и документи, необходими за сключването им, документи на пациенти (епикризи, разчитания от изследвания и др. – копия).

• Фактури, платежни, счетоводни документи, договори за външни услуги, договори доставка и др.

• Досиета на служители, архиви, документи на всички софтуери и приложения в организацията.

• административни документи

Софтуер :

• Операционна система (WINDOWS) SERVER.

• Счетоводен и ТРЗ софтуер.

Хардуер:

• Мобилни телефони

Услуги:

Ниво С обхваща:

• Операционна система (WINDOWS) работни станции, антивирусни на работните станции, офис приложения (програми)

• Стационарна комуникация, хостинг.

• Мобилни телефони и периферни устройства (Принтери, скенери и др.)

Политика по физическа сигурност и сигурност на заобикалящата среда

МБАЛ „Свети Мина”-Пловдив ЕООД провежда политика на защита на средствата за обработка и съхранение на информацията чрез определяне на граници на физическа сигурност и организация на зони за сигурност.

Политиката на МБАЛ по отношение на защита на устройствата цели намаляване на риска от неразрешен достъп до информационни активи, с всички възможни последствия, загуба, повреда, кражба, прекъсване на дейността. Прилагат се технически мерки за защита от пожар и прекъсване в електрозахранването, защита на окабеляването и комуникационните връзки.

В офис сградата са определени местата за достъп на клиенти, доставки и заре ждане. Физическата сигурност и защитата на заобикалящата среда в офис пространствата се осигурява чрез механизми за контрол на физическия достъп (ключ). В зоните с достъп на външни лица не се разполагат критични информационни активи.

Политика по управление на активите

Политиката се отнася до служители, външни експерти, временно работещи за фирмата и други, включително и персонал на трети страни. Тази политика се отнася до цялото информационно оборудване, собственост или използвано от МБАЛ „Свети Мина”-Пловдив ЕООД или нейни клиенти, както и до наличната информация.

Политиката на фирмата за използване на активите е свързана с налагане на стриктен контрол по отношение на всички физически и логически действия.

Политиката на фирмата за използване на активите цели не да налага ограничения, противоречащи на установената фирмена култура на откритост и доверие, а да защитава служителите на МБАЛ, нейните партньори и самата фирма от незаконни и увреждащи действия, извършени предумишлено или несъзнателно.

Системите свързани с Интернет, Локална мрежа, включително компютърното оборудване, приложния софтуер, операционните системи, средствата за съхранение на информация, електронната поща и други са собственост на МБАЛ. Тези системи са предназначени да се използват за целите на дейността в интерес на фирмата, нейните контрагенти и потребители, което налага въвеждане на правила за употреба.

Поради необходимостта да се защитава информационната система на МБАЛ, Ръководството по отношение на конфиденциалност на личната информация, съхранявана на което и да е устройство, задължава служителите да правят добра преценка относно разумността на личната употреба.

За целите на сигурността и поддръжката на мрежата, системният администратор наблюдава оборудването, системите и мрежовия трафик по всяко време.

Политика за „чисто бюро и чист екран“

Политиката за „чисто бюро и чист екран“ цели да намали рисковете свързани с неоторизиран достъп, загуба или повреда на информация по време или извън обичайното работно време.

Политиката взема предвид класификацията на информацията, законовите и договорните изисквания към сигурността на информацията.

Изискванията на тази политика са свързани с:

• Ограничаване на физическия и логическия достъп до конфиденциална информация чрез:

- ✓ изключване или заключване на компютрите, когато са ненадзиравани
- ✓ недопускане на съхранение на конфиденциална информация в зони с достъп на външни лица. Политиката се прилага задължително в зоните с достъп на външни лица.

Политика за обмен на информацията и сигурност на комуникациите

Политиката на организацията не налага органичения за използване на средства за обмен на информация, но въвежда следните механизми за контрол:

• При използване на електронна поща, конфиденциална информация и информация за служебно ползване да се изпраща в прикачен файл

• Забрана за използване на незащитени мрежи при предаване конфиденциална информация и информация за служебно ползване

• Използване на антивирусни програми

• Забрана за оставяне на съобщения съдържащи конфиденциална информация и информация за слу ебно ползване на телефонни секретари.

• Ограничаване на въвеждането на е-мейл адреси по подразбиране и автоматично препращане на съобщения

• Забрана за водене на служебни разговори на обществени места, отворени офис пространства или по несигурни информационни канали.

Организацията, работи само с одобрени куриерски служби и доставчици на комуникационни услуги.

Политика за работа с мобилни устройства и работа от разстояние

Организация разрешава работата с мобилни устройства и работа от разстояние при спазване на следните мерки за сигурност:

• Достъпът до сървър и други приложения на организацията единствено от системния администратор;

• Техника не следва да се оставя без наблюдение или на видно място в автомобили;

• Забранено е използване на опции „запомни паролата“ за достъп до служебна поща и сървър;

• Забранено е използването на свободни Wi Fi зони за трансфер на информация;

• Забранена е работата по служебни документи от публични зони (заведения,

бензиностанции, летища);

• В случай на загуба / кражба на компютър незабавно следва да се уведоми Ръководството;

• За подобряване сигурността при работа с мобилни телефони и предаваната информация са въведени следните правила:

о Съхранението на конфиденциални данни и лична данни в мобилния си телефон са забранени;

о Телефоните, на които е конфигурирана служебна поща следва да са с активирани пароли за отключване или друг начин на заключване.

Политика за инсталиране и използване на софтуер

Политиката на МБАЛ „Свети Мина”-Пловдив ЕООД по разработване, внедряване, изменение и поддържане на информационните системи е базирана на принципа на превантивната оценка на риска от измененията, включително ъпгрейд на съществуващи и внедряване на нови елементи от системата, разделение на средата за изпитване от действащата информационна система и планирана поддръжка на цялата информационна система.

Всички изменения в хардуера и в софтуера на системата се извършват само с предварително разрешение.

Политиката на организацията е създадена с цел да се спазват всички авторски права на компютърния софтуер, както и условията по софтуерните лицензи, по които тя е страна.

Организацията предприема всички необходими действия за предотвратяване на копирането на лицензиран софтуер от потребителите, както и използването на свързана с него документация в офисите на организацията или на друго място, освен ако не съществува изрично разрешение за това съгласно договора с ли ензодателя. Забранява се на служителите да използват софтуера по начин, който не съответства на лицензионния договор, включително предоставяне или получаване на софтуер или шрифтове от контрагенти, изпълнители по договори, потребители и други.

Целият софтуер, придобит от организацията, трябва да бъде закупен след съгласуване със системния администратор и Ръководството. Каналите за придобиване на софтуер са ограничени, за да гарантират, че организацията поддържа пълна документация за закупения софтуер и може да регистрира, поддържа и актуализира съответния софтуер. Това включва софтуер, който може да бъде свален и/или закупен от интернет.

Компютрите на МБАЛ са активи собственост на организацията трябва да бъдат защитени от вируси. Забранява се на потребителите да внасят софтуер отвън и да го инсталират на своите компютри в организацията.

Притежаваният от организацията софтуер не може да бъде изнасян от потребителите и качван на други компютри. Забранява се инсталирането на софтуер, различен от разрешения без съгласуване със системния администратор.

Политика по резервиране

Политиката на резервиране е базирана на оценка на риска от загуба на информация, като се цели трикратна резервираност, както следва:

- Резервиране на проекта информация на сървъра

- Резервиране на виртуално копие извън организацията

- Резервиране на електронната поща

За реализацията на политиката е разработена Схема на back-up - част от процедурата за управление на IT инфраструктура

Политика по защита от злонамерен софтуер

Политиката е насочена към навременно откриване на злонамерен софтуер и възстановяване на работоспособността, както и осъзнаване на механизмите за контрол от злонамерен софтуер от страна на служителите. За целта се налагат следните правила за работа:

• използване на антивирусни програми за защита на сървър и работни станции

о сканиране на всички файлове чрез външни памети или по мрежа

о сканиране на интернет страници

о сканирани на прикачени файлове

о ежедневна актуализация на антивирусни дефиниции

• използване на защитни стени (Firewall)

• контрол на входящия трафик

• провеждане на редновни прегледи в рамките на профилактика на системите

• Използване само на лицезиран софтуер и/или freeware, забрана за използване на неоторизиран софтуер

• Редовна инсталация на updates на операционни системи

• Незабавно докладване според утвърдена процедура за управление на инциденти (политика управление при инциденти)

Политика за управление на техническата уязвимост

Управлението на техническата уязвимост в организацията се базира на:

• Поддържане на описи (регистри) на активите, включително информация за доставчици, версии на софтуер, отговорности за поддръжка;

• Извършване на изменения на системите под контрола на системния администратор и след оторизация от страна на Управителя;

• Редовна профилактика на системите;

• Договор за поддрж ка с регламентирани времена за реакция;

• Процедури за докладване на събития инциденти и уязвимости в информационните системи;

• Контрол върху инсталация на актуализации и security patches на софтуер;

• Редовен анализ на идентифицираните уязвимости и докладвани слабости / събития свързани със сигурността на информацията.

Политика по сигурност, свързана с човешките ресурси

Политиката по сигурността на човешките ресурси на МБАЛ „Свети Мина”- Пловдив ЕООД е насочена основно към осъзнаване на необходимостта от

осигуряване на информационната сигурност чрез адекватно дефиниране на отговорности и обучение.

Всички служители на организацията в съответствие с техните функции на работа, преминават подходящо обучение и редовно актуализиране на знанията по политиката и процедурите на организацията.

Всички служители на МБАЛ и други физически лица, които използват ресурсите на Организацията, подписват Декларация за конфиденциалност, която представлява част от трудовите договори.

В случаи на сериозно нарушение на политиката и правилата за сигурност на човешките ресурси се прилага дисциплинарен процес, който включва отнемане на права за достъп до информационни ресурси, на активи и ако е необходимо, отстраняване от работа.

Политика за използване на криптографски механизми за контрол

Организацията използва криптографски механизми за контрол на достъпа до критични активи.

Криптографски механизим се използват при:

• Използване на валиден електронен подпис за провеждане на онлайн операции с официални институции

Политика за управление на паролите

Политиката за управление на паролите е базирана на оценката на риска в МБАЛ „Свети Мина”-Пловдив ЕООД, която взима под внимание достъпа на слжители до класифицирана клиентска и вътрешна информация.

Всеки служител, който има достъп до тези информационни активи е длъжен да използва силни пароли според политиката на организацията. Политиката важи за всички достъпи, които един служител използва.

Служителите нямат право да споделят паролите си на никого, както и да ги съхраняват на хартиен или електронен носител.

Политика за защита на личните данни

Политиката на МБАЛ „Свети Мина”-Пловдив ЕООД за защита на личните данни е изцяло съобразена със Закона за защита на личните данни.

МБАЛ събира лични данни на клиентите – физически и юридически лица и на служители за уреждане на трудово-правните взаимоотношения. Информацията не се използва повторно за цели, несъвместими със законово установените.

Информацията, която МБАЛ може да събира, включва данни от лични карти, ЕГН-та, гражданство, семейно положение, постоянен адрес, копия на документи, удостоверяващи образование и квалификация, трудова дейност, банкова сметка, телефонни, адрес за електронна поща, регистрация на Здравна информация – чл. 27 от ЗЗ - лични данни, свързани със здравословното състояние, физическото и психическото развитие на лицата и всяка друга информация в медицинската документация - чувствителни лични данни съгл. чл.5, ал. 1, т.3 от ЗЗЛД и др.
Определените отговорни слу ители, обработващи лични данни, са задължени да третират информацията като конфиденциална.

Предприети са мерки за физическа и логическа защита на личните данни и са ограничени правата за достъп до тях.

Всеки служител, за когото се отнасят данните („субект на данни“) има право на достъп до своите данни, както и да изиска тяхното коригиране.

Политика за взаимоотношения с доставчици

С всички доставчици, имащи отношение към сигурността на информацията, съответно имащи достъп до активи на организацията или предоставящи услуги (комуникации, поддръжка, СОТ, логистични дейности и т.н) са обект на оценка на риска.

Всички външни експерти, използвани при реализацията на основните процеси подписват задължително Договори с включена Клауза за конфиденциалност.

Като допълнителни механизми за контрол се използват:

• С доставчиците на услуги/доставки се подписват при необходимост анекси

към договори относно съгласие за обработка на личните им данни, както и клауза за спазване законите за защита на личните данни, поверителността или други подобни закони, наредби и насоки.

• Физически достъп се осигурява в зависимост от специфичните нужди за реализация на услугата/доставката, но задължително в присъствието на упълномощен служител от МБАЛ.

• Договорите / споразуменията специфицират правата на одит / контрол от страна на упълномощени служители от страна на МБАЛ върху работата на трета страна или функционирането на системи на трета страна.

<u>Политика за сигурно разработване на софтуер от външни страни</u>

В случай на възлагане на разработка на софтуер от външни страни се прилагат следните контроли за защита на информационната система на МБАЛ „Свети Мина”-Пловдив ЕООД:

• Възлагат се единствено на утвърдени доставчици на услуги с подписан SLA и рамков договор;

• Параметрите на разработване се обсъждат на работна среща и се утвърж дават с Техническо задание от Доставчика;

• Техническото задание се утвърждава от Управителя;

• Разработването и тестването на софтуера се извършват извън инфраструктурата на МБАЛ;

• Тестването не се извършва с реални данни на МБАЛ;

• МБАЛ не разполага с достъп до кода на разработения софтуер и всяка желана промяна се съгласува с Доставчика.

Ръководството на МБАЛ „Свети Мина”-Пловдив ЕООД декларира своята пълна ангажираност в процесите на развитие, поддържане и усъвършенстване на мерките за защита на личните данни.