УТВЪРДИЛ: ...../п/.....

Д-Р ГЕНАДИ СТРАНДЖЕВ

/УПРАВИТЕЛ/

ПОЛИТИКА УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ ПО ПОВОД МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, СЪБИРАНИ, ОБРАБОТВАНИ, СЪХРАНЯВАНИ И ПРЕДОСТАВЯНИ ОТ МБАЛ „СВЕТИ МИНА”- ПЛОВДИВ ЕООД

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Настоящите правила имат за цел осигуряването на контрол при управление на работата на информационните системи в МБАЛ „Свети Мина”-Пловдив ЕООД при възникване на инциденти.

Политиката осигурява информационна сигурност на финансовата, правната и техническата информация, както и тази, свързана с личните данни в организацията във връзка с осъществяване на основната дейност.

МБАЛ „Свети Мина”-Пловдив ЕООД, наричана по-долу за краткост МБАЛ, основава управлението на сигурността на информацията на базата на превенция на потенциални неблагоприятни събития чрез систематичен анализ на средата, изискванията на заинтересовани страни, риска по отношение на сигурността и прилагане на комплекс от технически и организационни мерки за управление на риска.

РАЗДЕЛ ВТОРИ

ПРИНЦИПИ И ЦЕЛИ

Ръководството ще прилага следните основни принципи:

- защита на данни и неприкосновеност на лична информация;
- опазване на архивите на информацията;
- защита на клиентска, търговска информация;

- докладване на инциденти, свързани със сигурността;
- управление непрекъснатостта на работа;

Целите на настоящата политика са:

- осигуряване на непрекъснатост на работните процеси;
- минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на МБАЛ;
- минимизиране на степента на загуби или вреди, причинени от пробиви в информационната сигурност;
- осигуряване на необходимите ресурси за поддържане на ефективно управление на информационната сигурност;
- информиране на служителите за техните отговорности и задължения по отношение на информационната сигурност;
- осигуряване на съответствие с нормативни изисквания.

РАЗДЕЛ ТРЕТИ

УЯЗВИМОСТИ И ЗАПЛАХИ ПРИ УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Уязвимости (Vulnerabilities)

Дефиниция – всяка една слабост в една система, която я оставя отворена на атака

Таблицата по-долу дава примери за уязвимости в различни области на сигурността в МБАЛ, включвайки примери на заплахи, които могат да използват тези уязвимости. Списъкът може да бъде в помощ при оценяването на заплахите и уязвимостите, за да се определят съответни сценарии на инциденти, например щети или загуба на услуги от първа необходимост. Наблегнато е на това, че в някои случаи други заплахи могат също да използват тези уязвимости.

Примери за уязвимости в различни области на сигурността – ХАРДУЕР

ТИП	Примери за уязвимости	Примери за заплахи
	Недостатъчна поддръжка/ погрешно инсталиране на	Пробив в поддръжката на информационната система

	носител	
	Липса на схеми за периодично възстановя-ване	Разрушаване на устройства или носител
	Податливост на влажност, прах, мръсотия	Прах, корозия, замръзване
	Чувствителност към електромагнитно излъч-ване	Електромагнитно излъчване
Хардуер	Недостатъчно ефективен контрол за проме-ни в конфигурацията	Грешка при ползване
	Податливост на промени в напрежението	Загуба на захранващо напрежение
	Податливост на промени в температура	Метеорологично явление
	Незащитено хранилище	Кражба на носител или документи
	Недостатъчна грижа при изхвърляне	Кражба на носител или документи
	Неконтролирано копиране	Кражба на носител или документи

Примери за уязвимости в различни области на сигурността – СОФТУЕР

Софтуер	Липса или недостатъчно тестване на софтуер	Злоупотреба с права
	Добре познати недостатъци в софтуера	Злоупотреба с права
	Без 'logout' при „излизане" от работна станция	Злоупотреба с права
	Изхвърляне или повторна употреба на носители без подходящо изтриване	Злоупотреба с права
	Липса на записи от одит	Злоупотреба с права
	Грешно определяне на права за достъп	Злоупотреба с права
	Широко разпространен софтуер	Разрушаване на данни
	Прилагане на приложни програми към грешни данни в смисъл на време	Разрушаване на данни
	Объркан потребителски интерфейс	Грешка при ползване
	Липса/недостиг на документация	Грешка при ползване
	Неправилна настройка на параметри	Грешка при ползване
	Неправилни дати	Грешка при ползване

Примери за уязвимости в различни области на сигурността – МРЕЖА

Мрежа	Липса на доказателства за изпращане или получаване на съобщение	Отказ на услуги
	Незащитени комуникационни линии	Подслушване
	Незащитен чувствителен трафик	Подслушване
	Некачествено свързани кабели	Авария на телекомуникационни устройства
	Единична точка на авария	Авария на телекомуникационни устройства
	Липса на идентификация и автентификация на подател или получател	Фалшифициране на права
	Незащитена мрежова архитектура	Отдалечено шпиониране
	Трансфер на пароли в „чист" вид	Отдалечено шпиониране
	Неправилно мрежово управление (гъвкавост на рутирането)	Насищане на информационната система
	Незащитени връзки на обществената мрежа	Неоторизирано ползване на устройства

Заплахи (Threats)

Дефиниция – всяко събитие или действие, в резултат на което се нарушава CIA на даден ресурс или данни.

Таблицата по-долу дава примери за типични заплахи. Списъкът може да бъде използван по време на процеса за оценяване на активите на МБАЛ. Заплахите могат да бъдат преднамерени, случайни или от обкръжаващата среда (природни) и могат да имат за резултат например щети или загуба на услуги от първа необходимост. Списъкът по-долу показва всяка заплаха, където съответно преднамерените заплахи са означени с D (deliberate), случайните - с A (accidental), природните - с E (environmental). D се използва за всички преднамерени действия, насочени срещу информационните активи, A се използв за всички човешки действия, които могат случайно да увредят информационните активи и E се използва за

всички инциденти, които не са основани на човешки действия. Групите от заплахи не са подредени по приоритет.

ТИП	ЗАПЛАХИ	ПРОИЗХОД
Физически щети	Огън	A, D, E
	Щети от вонда	A, D, E
	Замърсяване	A, D, E
	Голяма злополука	A, D, E
	Разрушаване на устройства или носител	A, D, E
	Прах, корозия, замръзване	A, D, E
Природни събития	Климатични явления	E
	Сеизмично явление	E
	Вулканично явление	E
	Метеорологично явление	E
	Наводнение	E
Загуба на услуги от първостепенна важност	Повреда на климатична или водоснабдителна система	A, D
	Загуба на електроснабдяване	A, D, E
	Повреда на телекомуникационни устройства	A, D
Смущения от излъчване	Електромагнитно излъчване	A, D, E
	Термично излъчване	A, D, E
	Електромагнитни импулси	A, D, E
Компрометиране на информация	Подслушване на компрометирани интерфейсни сигнали	D
	Отдалечено шпиониране	D
	Подслушване	D
	Кражба на носител или документи	D
	Кражба на устройства	D
	Възстановяване на рециклирани или изхвърлени носители	D
	Разкриване	A, D
	Данни от недостоверни източници	A, D
	Фалшифициране с хардуер	D
	Фалшифициране със софтуер	A, D

	Разкриване на позиция	D

Специално внимание трябва да се обърне на **човешките източници** на заплахи. Те са конкретно изредени по точки в следната таблица:

Произход на заплахата	**Мотивация**	**Възможни последствия**
Хакер, кракер	Предизвикателство Его Недоволство Състояние Пари	• Хакерство • Социален инженеринг • Проникване в система, • Неразрешен достъп до системата
Компютърен престъпник	Разрушаване на информацията Противозаконно разкриване на информация Спечел-ване на пари Неразрешена промяна на данни	• Компютърно престъпление (например cyber stalking) • Акт на измама (например повторение, деперсонификация, подслушване, заглушаване) • Продажба на информация • Измама • Проникване в система
Терорист	Изнудване Разрушаване Експлоатация От-мъщение Политически ползи Медийно пок-ритие	• Бомба/тероризъм • Информационна война • Атака в системата (например разпреде-лен отказ на услуга) • Проникване в системата • Фалшифициране на системата

Произход на заплахите

Произход на заплахата	**Мотивация**	**Възможни последствия**
Промишлен шпионаж (разузнаване, компа-нии, чуждестранни правителства, други правителствени интереси)	Конкурентно предимство Икономичес-ки шпионаж	•Отбранително предимство • Политическо предимство • Икономическа разработка • Кражба на информация • Нарушаване на личното пространство • Социален инженеринг • Проникване в системата • Неразрешен достъп до системата (достъп до

		класифицирана, лична и/или технологич-но свързана информация)
Вътрешни за органи-зацията лица (лошо обучени, недоволни, злонамерени, небрежни, нечестни или уволнени служители)	Любопитство Его Разузнаване Спечелване на пари От-мъщение Неумишлени грешки и пропуски (например грешка при въвеждане на дан-ни, грешка при програмиране)	• Нападение на служител • Изнудване •Разглеждане на частна информация • Злоупотреба с компютър • Измама и кражба • Продажба на информация • Въвеждане на фалшиви, опорочени данни • Подслушване •Злонамерен код (например вирус, логичес-ка бомба, троянски кон) • Продажба на лична информация • Дефекти в системата • Влизане в системата • Саботаж на системата •Неразрешен достъп до системата

РАЗДЕЛ ЧЕТВЪРТИ

КОНТРОЛИ

Атаката е техника, действие или събитие, което се възползва от уязвимостта в даден ресурс, за да нанесе поражения върху информационната сигурност. Атаките биват срещу физическата и логическата сигурност в МБАЛ „Свети Мина” – Пловдив ЕООД.

Рискът за сигурността на информацията представлява възможността дадена заплаха да използва уязвимостите на актив или група активи и по този начин да причини вреда на организацията.
Контролите са мерките, които се внедряват за да се защити CIA на даден ресурс или информация.

Категории контроли:

- Превантивни контроли;
- Контроли за установяване на събитието;
- Коригиращи контроли;

- Административни;
- Физически;
- Технически;
- Възпиращи;
- Компенсиращи;

Ключови Термини и определения в ИС:

- Невъзможност за отричане;
- Идентификация;
- Оторизация;
- Търсене на отговорност;
- Проследимост на действия и събития

Практики и принципи в ИС:
- Пълна забрана – всичко, което не е разрешено е забранено;
- Принцип на най-ниско ниво на достъп – винаги дефиниране най-ниско ниво на достъп за извършване на определена дейност;
- Разделение на задълженията – разделяне на задълженията по начин, който ще предотврати умишлени зловредни действия;
- Регулярна смяна на длъжностите – регулярна смяна на отговорностите на служителите с цел предотвратяване на умишлени зловредни действия;
- Задължителни ваканции – Задължителни отпуски (поне 1 пълна седмица);
- Рестрикции по време - ограничаване достъпа до ресурси;
- Управление на привилегиите – управление правата на достъп на служителите .

Състоянието на компютърна „сигурност“ в МБАЛ „Свети Мина” – Пловдив ЕООД е концептуално идеална, постигната чрез използването на трите процеса: превенция, разкриване и реакция. Тези процеси се основават на различни политики и системни компоненти, които включват следното:

- Потребителския достъп до акаунт и криптографията могат да защитят системите за файлове и данни;
- Антивирусният софтуер се състои от компютърни програми, които се опитват да идентифицират, заловят и премахнат компютърни вируси и друг зловреден софтуер;
- Архивите (backups) са начин за осигуряване на информация; те са още едно копие на всички важни компютърни файлове, което се съхранява

на друго място. Тези файлове се съхраняват на твърди дискове, CD-R, CD-RW дискове, касети и по-скоро на „облака“.

- Защитните стени за сега са от най-честите системи за превенция от гледна точка на сигурността на мрежата, тъй като те могат (ако правилно са конфигурирани) да предпазят достъпа до вътрешните мрежови услуги, както и да блокират някои видове атаки чрез филтриране на пакети. Защитните стени могат да бъдат както хардуерни така и на софтуерна основа.
- Системите за откриване на проникване (IDS) са предназначени за откриване на мрежови атаки.
- „Отговорът“ е задължително определен от оценените изисквания за сигурност за индивидуална система и може да покрива диапазона от прост ъпгрейд на защитата, уведомяване на правните органи, контра-атаки, и други подобни. В някои специални случаи, пълното унищожаване на компрометираната система е предпочитано, тъй като това може да стане така, че не се откриват всички компрометирани ресурси.

РАЗДЕЛ ПЕТИ
ПОТРЕБИТЕЛИ

Потребителите на информационната система в МБАЛ „Свети Мина”-Пловдив ЕООД се задължават да следват процедурите и инструкциите по информационна сигурност, да докладват за проблеми и инциденти в информационната система. Системният администратор спазва изискването

за уведомяване на регулатора в случай на пробив в защитата на информацията, в случай на пробив в системата. Уведомяването трябва да стане не по-късно от 72 часа след установяването на пробива.

Организацията е уведомила всички заинтересовани лица, че прилага политики за информационна сигурност чрез сайта си, както и чрез електронния подпис, с който се подписва кореспонденцията към трети лица по електронен път.

Политиката по информационна сигурност се преглежда редовно и се ревизира, за да се вземат под внимание променящите се обстоятелства.

Всеки служител, който прецени, че има злоупотреба с настоящата политика в организацията, трябва да уведоми системния администратор.

Всеки служител, за когото е установено, че е нарушил тази политика, подлежи на дисциплинарна отговорност.

Персоналът на МБАЛ „Свети Мина”-Пловдив ЕООД се задължава да спазва всички правила, свързани с информационната сигурност, описани в процедури, инструкции и други документи на лечебното заведение.

РАЗДЕЛ ШЕСТИ

ФИЗИЧЕСКА СИГУРНОСТ, СИГУРНОСТ НА ЗАОБИКАЛЯЩАТА СРЕДА И КОНТРОЛ НА ДОСТЪПА

Информационните системи, които поддържат критични за МБАЛ „Свети Мина”-Пловдив ЕООД, притежават подходяща физическа сигурност. Никакви конфиденциални материали в електронен формат не се оставят в неконтролирана среда и са защитени срещу случаен достъп.

Оборудването, което поддържа критични функции, се защитава физически от заплахи за сигурността и влияние на рискове от околната среда за предотвратяване на загуби, щети или излагане на риск на активи и прекратяване на основни дейности. Това включва информационно, комуникационно, мрежово оборудване, оборудване за съхранение на данни, захранващо оборудване и оборудване за контрол на околната среда. Определени са физически периметри (зони), в които е разположено такова оборудване и достъпът до тях е строго ограничен и контролиран.

Защитата на физическата сигурност се базира на непрекъснатостта на външната граница (конструкция от плоча до плоча) и на подходящ контрол на достъпа (ключове за ограничен достъп, входни точки за служителите, секретни ключалки).

Изнасянето извън сградите на МБАЛ „Свети Мина”-Пловдив ЕООД на информационните активи /собственост на лечебното заведение/ изисква разрешение от съответния ръководител и подлежи на проверка.

Служебна информация не се оставя без надзор или контрол, което означава видима на екран.

Когато използването на дадено оборудване се прекрати, всички ключове, идентификационни карти и други устройства и пароли за достъп се връщат и отчитат.

При всички положения, когато информационната инфраструктура и/или физическата среда за разполагане, използвана от МБАЛ е споделена или не е под пряк контрол, се гарантира с договорни условия, че настоящата политиката за информационна сигурност ще се спазва. Спазването на тези условия се проверява на място периодично и се включва в извършваните одити по сигурността.

Физическият достъп до ИТ съоръженията и комуникационното оборудване на МБАЛ се извършва от и/или в присъствие на служители на лечебното заведение.

Средствата за контрол на физическата сигурност се използват и при защита на копирни машини, факсове и мрежови принтери.

Всички информационни системи на МБАЛ работят във физически условия, дефинирани от техните производители.

Сървърите на МБАЛ са оборудвани със системи за климатизация, подходящо оразмерени и резервирани. Осигурени са със системи за пожароизвестяване и пожарогасене. Сървърното помещение следва да е оборудвано с непрекъсваеми захранващи устройства, подходящо оразмерени и резервирани.

МБАЛ „Свети Мина”-Пловдив ЕООД създава поддържа и осигурява условия за безопасна работа в съответствие със Закона за здравословни и безопасни условия на труда.

РАЗДЕЛ СЕДМИ

УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ПОДОБРЯВАНЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

В МБАЛ „Свети Мина”-Пловдив ЕООД следва да се събират данни и да се извършва анализ на вида и броя на инцидентите, на направените разходи по разрешаване на инцидентите. Целта е да се идентифицират повтарящите се инциденти или инцидентите с голямо влияние, да се ограничат честотата, щетите и загубите от появата им в бъдеще. Документирането на инцидентите става чрез протокол при пробив в информационната сигурност по Образец – Приложение към настоящите правила.

Ръководството на МБАЛ оценява необходимостта от планиране непрекъснатостта на дейността. Осъзнава, че има значителен риск за неговите критични процеси при потенциални и неочаквани разрушителни събития. Увеличаващото се развитие на процеси, базирани на технологии и силната зависимост от информационните технологии, е основание за създаване на план за непрекъснатост на работа.

МБАЛ „Свети Мина”-Пловдив ЕООД създава условия и следи за непрекъснатост на работата на критичните ресурси на системата при настъпване на сериозни неблагоприятни условия и опасност за прекъсване, по-голямо от 8 часа.

РАЗДЕЛ ОСМИ

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в МБАЛ „Свети Мина”- Пловдив ЕООД са длъжни да познават и спазват разпоредбите на тези правила.
§ 2. Неразделна част от настоящите правила представлява образец при пробив в информационната сигурност.

§ 4. Контролът по спазване на правилата се осъществява от системния администратор.
§ 5. При Управление на инцидентите CERT Bulgaria е Националният Център за действие при инциденти в Информационната Сигурност (https://govcert.bg/); ENISA CERT (Ниво Европейски Съюз) - http://www.enisa.europa.eu/activities/cert;
§ 5. Тази политика влиза в сила от деня на утвърждаването й със заповед на Управителя, както и Образец за протокол при пробив в информационната сигурност към нея.

ПРОТОКОЛ № ...../.....

Констатирал пробива:

Подпис: Дата:

Описание на пробива:

Подпис: Дата:

Становище за разпореждане:

Управител/Ръководител звено: Дата:

Уведомление за пробива към КЗЛД:

Име, подпис: Дата:

Забележки:

Име, подпис: Дата: