ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ-БЛАГОЕВГРАД

УТВЪРДИЛ:
Д-Р КР. МИХАЙЛОВ
ДИРЕКТОР НА ЦСМП
Дата: 31.07.2020 г.

ВЪТРЕШНА ПОЛИТИКА

ЗА УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ ПО ПОВОД ИЗТИЧАНЕ НА ИНФОРМАЦИЯ И НА ЛИЧНИ ДАННИ, СЪБИРАНИ, ОБРАБОТВАНИ, СЪХРАНЯВАНИ И ПРЕДОСТАВЯНИ ОТ ЦСМП – БЛАГОЕВГРАД

Март 2020 г.
Благоевград

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящата Вътрешна политика има за цел осигуряването на контрол при управление на работата на информационните системи в ЦСМП - Благоевград при възникване на инциденти.

Чл.2. Политиката осигурява информационна сигурност на финансовата, правната и техническата информация, както и тази, свързана с личните данни в ЦСМП - Благоевград във връзка с осъществяване на основната дейност-оказване на спешна медицинска помощ.

Чл.3. ЦСМП - Благоевград, 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

Чл.4. ЦСМП – Благоевград прилага следните основни принципи:

- защита на данни и неприкосновеност на лична информация;
- опазване на архивите на информацията;
- докладване на инциденти, свързани със сигурността;
- управление непрекъснатостта на работа;

Чл.5. Целите на настоящата вътрешна политика са:

- осигуряване на непрекъснатост на работните процеси;
- минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на ЦСМП-Благоевград;
- 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

Чл. 6. **Уязвимости (Vulnerabilities)**

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

Примери от БДС ISO/IEC 27005:2009

Таблицата по-долу дава примери за уязвимости в различни области на сигурността, 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**
Хардуер	Недостатъчна поддръжка/ погрешно инсталиране на носител	Пробив в поддръжката на информационната система
	Липса на схеми за периодично възстановяване	Разрушаване на устройства или носител
	Податливост на влажност, прах, мръсотия	Прах, корозия, замръзване
	Чувствителност към електромагнитно излъчване	Електромагнитно излъчване
	Недостатъчно ефективен контрол за промени 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

Тип	**Примери за уязвимости**	**Примери за заплахи**
Софтуер	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	Грешка при ползване

	интерфейс	
	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

Тип	**Примери за уязвимости**	**Примери за заплахи**
Мрежа	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

Чл. 7. **Заплахи (Threats)**

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

Примери от БДС ISO/IEC 27005:2009

Таблицата по-долу дава примери за типични заплахи. Списъкът може да бъде използван по време на процеса за оценяване на активите. 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 слу-чайно 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 вода	A, D, E
	Замърсяване	A, D, E
	Голяма катастрофа/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.	• Компютърно престъпление (например cyber stalking) • Акт на измама

	Спечелване на пари. Неразрешена промяна на данни	(например повторение, деперсонификация, подслушване, заглушаване) • Продажба на информация • Измама • Проникване в система
Терорист	Изнудване. Разрушаване. Експлоатация. Отмъщение. Политически ползи. Медийно покритие.	• Бомба/тероризъм • Информационна война • Атака в системата (например разпределен отказ на услуга) • Проникване в системата • Фалшифициране на системата
Промишлен шпионаж (разузнаване, компании, чуждестранни правителства, други правителствени интереси)	Конкурентно предимство. Икономически 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 технологично свързана информация
Вътрешни за организацията лица (лошо обучени, недоволни, злонамерени, небрежни, нечестни или уволнени служители)	Любопитство Его Разузнаване Спечелване на пари Отмъщение Неумишлени грешки и пропуски (например грешка при въвеждане на данни, 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

Чл. 8. Атаката е техника, действие или събитие, което се възползва от уязвимостта в даден ресурс, за да нанесе поражения върху информационната сигурност. Атаките са срещу физическата и логическата сигурност в ЦСМП-Благоевград.

Чл. 9. Рискът за сигурността на информацията в ЦСМП-Благоевград представлява възможността дадена заплаха да използва уязвимостите на актив или група активи и по този начин да причини вреда на организацията.

Чл. 10. Контролите са мерките, които се внедряват за да се защити даден ресурс или информация.

Чл. 11. Категории контроли в ЦСМП - Благоевград:

- Превантивни контроли;
- Контроли за установяване на събитието;
- Коригиращи контроли;
- Административни;
- Физически;
- Технически;
- Възпиращи;
- Компенсиращи;

Чл. 12. Ключови термини и определения в информационна система :

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

Чл.13. Практики и принципи в информационна система :

- 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;
- Рестрикции по време - ограничаване достъпа до ресурси;
- Управление на привилегиите – управление правата на достъп на служителите.

Чл.14. Състоянието на информационна "сигурност" в ЦСМП-Благоевград 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 или касети.
- 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, контраатаки, 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

Чл.15. **Потребители са всички служители с достъп до информационната система в ЦСМП-Благоевград и се задължават да следват процедурите и инструкциите по информационна сигурност, да докладват за проблеми и инциденти.**

Ал. (1) Информационна система на ЦСМП - Благоевград включва, следните програми и уеб базирани приложения:

- Национална система за спешни повиквания 112,
- Програмен продукт Терес за ТРЗ и ЛС,
- Телемедицина Corpulus 3,
- Уеб базирани информационни системи: Система за електронен документооборт Eventis 7, Система за контрол и управление на транспортни средства Fleet Expert, Уеб базирана електронна система електронна система за закупуване на лекарства, Уеб базирана електронна система СЕВОП, НАП, НОИ, НСИ и други

Ал. (2) Нива на достъп:

Национална система за спешни повиквания 112

1 Най-ниско – роля "Оператор" – Медицински специалисти. Операторът приема подадените към център 112 повиквания и събира за най-кратко време максимално точна и подробна информация относно инцидента. Информацията

включва причина за повикването, точен адрес на обаждащия се и на инцидента, име на обаждащия се и име на пострадалия/те, телефон за обратна връзка, ориентир за мястото на инцидента, съществуваща опасност за пострадалия/те, за служителите на службите за спешно реагиране и/или за населението, както и друга важна информация, свързана с инцидента. Операторът локализира обаждащия се, като сравнява получената информация с географската информационна система. Операторът при необходимост осъществява конферентна връзка между обаждащия се в център 112 и службите за спешно реагиране.

2 По-високо ниво – координатор Роля "HR" - Зав. ФСМП, Гл. Счетоводител, Икон. ТРЗ, Служител ЧР, Технически сътрудник, Инж. ДВГ - добавяне, преглед и редактиране на Номенклатурите на ЦСМП (транспорните средства на ЦСМП, консумативи), управление на графици и смени, управление на екипи

3 Най-високо ниво – Роля "Administrator" - IT специалист ЦСМП, Главна медицинска сестра, директор ЦСМП - пълен достъп, всички права

Терес - програмен продукт за ТРЗ и ЛС, работни заплати, личен състав, хонорари, трудови и граждански договори, платежни документи.

Достъп до тази система имат икон. ТРЗ, служител човешки ресурси и касиер на АСС – Благоевград.

Нива на достъп:

1. Администратор – икон. ТРЗ, - пълен достъп, всички права
2. Оператор – служител човешки ресурси и касиер на АСС – ограничен достъп

Уеб базирана система за електронен документооборот Eventis 7

Достъп до тази система имат всички служители на АСС – Благоевград и завеждащите филиали в ЦСМП – Благоевград.

Той се осигурява посредством персонален компютър на интернет адрес, с потребителски профил и парола и/или електронен подпис (КЕП).

Нива на достъп:

1. Пълен достъп до документите:

- Технически сътрудник – Да регистрира документи от входяща, изходяща, вътрешна и вътрешно-изходяща кореспонденция. Да контролира изпълнението им в срок.
- Главен счетоводител – Да регистрира сключени договори, свързани с ОП, дарения и др. Да резолира, насочени към главен счетоводител документи и да следи за изпълнението им в срок.
- Служител "Човешки ресурси" – Да регистрира трудови договори, допълнителни споразумения и други документи, свързани с персонала на ЦСМП-Благоевград.
- Главна медицинска сестра – Да регистрира вътрешни документи, свързани с кореспонденция, резолирана до нея.
- Касиер – Да регистрира удостоверения за доход и УП-2 на персонала на ЦСМП – Благоевград.

2. Ограничен достъп до документите:

- Икономист ТРЗ, инженер ДВГ, счетоводители, ИТ специалист и Завеждащ ФСМП – Да имат достъп до резолирани до тях или изготвени от тях документи.

Телемедицина Corpulus 3, Система за контрол и управление на транспортни средства Fleet Expert, Уеб базирана електронна система електронна система за закупуване на лекарства, Уеб базирана електронна система СЕВОП, НАП, НОИ, НСИ и други

Достъп до тези системи се осигурява посредством интернет адрес, с потребителски профил и парола и/или електронен подпис.

Ал. (3) Примери за проблеми или инцидент, свързани с наличие на вируси, вирусни атаки при работа с информационите системи са:

- компютъра често блокира;
- работи бавно;
- рестартира се без видима причина;
- прегрява;
- невъзможност на потребителя да осъществи достъп с потребителско име и парола;
- антивирусната програма издава съобщение за вирус

При тези и други инциденти, потребителя на информационни системи е длъжен да уведоми прекият си началник и Системният администратор на ЦСМП – гр. Благоевград, GSM: 0897000141, като попълни **Образец №1** от настоящата вътрешна политика

Чл.16. Системният администратор докладва на длъжностното лице по защита на личните данни в ЦСМП – Благоевград и то спазва изискването за уведомяване на регулатора в случай на пробив в защитата на информацията, в случай на пробив в системата при последващо изтичане на лични данни.

Чл.17. Уведомяването трябва да стане не по-късно от 72 часа след установяването на пробива към КЗЛД.

Чл.18. При инцидент с мрежовата и информационната сигурност системният администратор /ЦСМП –Благоевград/ , отговарящ за мрежовата и информационната сигурност уведомява Държавна агенция „Електронно управление" за инцидентите в сроковете, посочени в чл. 21, ал. 4 и 5 и чл. 22 от Закона за киберсигурност.

Чл.19. Системният администратор за уведомяването по чл.31, ал. 1 от Наредба за минималните изисквания за мрежова и информационна сигурност (Обн. ДВ. бр.59 от 26 Юли 2019г.) и по чл. 17, ал. 7 от Закона за киберсигурност използва формата, посочена в Образец № 2 (Уведомление за инцидент към секторния ЕРИКС) към настоящата вътрешна политика.

Чл.20. ЦСМП – Благоевград уведомява всички заинтересовани лица, че прилага политика за информационна сигурност чрез сайта си, както и чрез

електронния подпис, с който се подписва кореспонденцията към трети лица по електронен път.

Чл. 21. Вътрешната политика по информационна сигурност в ЦСМП – Благоевград се преглежда редовно веднъж годишно и се ревизира, с цел променящите се обстоятелства.

Чл.22. Всеки служител в ЦСМП – Благоевград следва незабавно да уведоми системния администратор при злоупотреба с настоящата вътрешна политика.

Чл.23.Всеки служител в ЦСМП- Благоевград , за когото е установено, че е нарушил тази политика, подлежи на дисциплинарна отговорност.

Чл.24. Персоналът на ЦСМП -Благоевград 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

Чл. 25. Информационните системи, които се поддържат от ЦСМП-Благоевград, притежават подходяща физическа сигурност.

Конфиденциални материали в електронен формат не се оставят в неконтролирана среда и са със защита срещу случаен достъп.

Чл.26. Оборудването в ЦСМП – Благоевград , 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.

Чл.27. Защитата на физическата сигурност в ЦСМП – Благоевград 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).

Чл.28. Изнасянето извън сградите на ЦСМП-Благоевград на информационните активи /собственост на лечебното заведение/ изисква разрешение от Директора на ЦСМП – Благоевград и подлежи на проверка.

Чл.29. На служебна информация видима на екран в ЦСМП – Благоевград се осъществява непрекъснат надзор и/или контрол.

Чл.30. Когато използването на дадено оборудване в ЦСМП – Благоевград се прекрати, всички ключове, идентификационни карти и други устройства и пароли за достъп се връщат и отчитат.

Чл.31. Когато информационната инфраструктура и/или физическата среда за разполагане, използвана от ЦСМП-Благоевград е споделена или не е под пряк контрол, се гарантира спазването на настоящата вътрешна политика.

Спазването на тези условия включва извършване на одити по сигурността.
Чл.32. Физическият достъп до ИТ съоръженията и комуникационното оборудване на ЦСМП-Благоевград се извършва от и/или в присъствие на служители на лечебното заведение.
Чл.33. Средствата за контрол на физическата сигурност се използват и при защита на копирни машини, факсове и мрежови принтери в ЦСМП – Благоевград
Чл.34. Всички информационни системи на ЦСМП-Благоевград работят във физически условия, дефинирани от техните производители.
Чл.35. Сървърите на ЦСМП-Благоевград са оборудвани със системи за климатизация, подходящо оразмерени и резервирани и системи за пожароизвестяване и пожарогасене. Сървърното помещение е оборудвано с непрекъсваеми захранващи устройства.
Чл.36. ЦСМП-Благоевград 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

Чл. 37. В ЦСМП-Благоевград събира данни и извършва анализ на вида и броя на възникнали инциденти, на направените разходи по разрешаване на инцидентите.
Чл. 38. Идентифицират се повтарящите се инциденти или инцидентите с голямо влияние, с цел ограничаване честотата, щетите и загубите от появата им.
Чл. 39. Документирането на инцидентите в ЦСМП- Благоевград е с протокол при пробив в информационната сигурност по Образец 1 – Приложение към настоящата вътрешна политика .
Чл.40. ЦСМП-Благоевград оценява и планира непрекъснатост на дейността по оказване на спешна медицинска помощ, с цел намаляване на риска за неговите критични процеси при потенциални и неочаквани разрушителни събития.
Чл.41. ЦСМП-Благоевград следи за непрекъснатост на работата на критичните ресурси на системата при настъпване на сериозни неблагоприятни условия и опасност за прекъсване, по-голямо от 8 /осем/ часа.

РАЗДЕЛ ОСМИ
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Директора и служителите в ЦСМП-Благоевград са длъжни да спазват разпоредбите на тази вътрешна политика.
§ 2. Неразделна част от политиката е Образец №1 при пробив в информационната сигурност и Образец №2 УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ към секторния ЕРИКС
§ 3. Контролът по спазване на политиката се осъществява от системния администратор.

§ 4. 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 е утвърдена със Заповед №РД-01-185/12.03.20г на Директора на ЦСМП – Благоевград и влиза в сила от 01.04.20, съгласно с Образец №1 протокол при пробив в информационната сигурност и Образец №2 УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ към секторния ЕРИКС
§ 6. Неразделна част към политиката е Риск – регистър на мрежовата и информационната сигурност на ЦСМП - Благоевград

Образец №1

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:

Образец №2.1

представляващ Приложение № 7 към чл. 31, ал. 2 от **НАРЕДБА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ** (Обн. ДВ. бр.59 от 26 Юли 2019г., в сила от 26.07.2019 г.)

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ
към секторния ЕРИКС

Необходима информация	**Детайли**	**Данни**
(до 2 часа)		
Лице, подаващо уведомлението	Име, фамилия	
Вашият телефонен номер	(GSM)	
Вашата електронна поща		
Организация	Наименование на организацията, засегната от инцидента	
Лице за контакт (за целите на разрешаването на инцидента)	Име, телефонен номер и електронна поща на компетентно лице от предприятието, което при необходимост може да подаде допълнителна информация	
Дата и час	Вписват се датата и часът на възникване на инцидента, ако не е възможно - датата и часът на откриването му	
Тип на инцидента		0 Virus 0 Trojan 0 Botnet 0Dos/DDos 0 Malware 0 Port Scan 0 Spam 0 Phishing 0Pharming 0 Probe 0 Crack 0 Copyright 0Ransomware 0 Defacement 0 Exploiting known Vulnerabilities 0 Application Compromise 0 Login Attempts 0 SQL injections 0 Unknown 0 Other
Кратко описание на инцидента	Вписва се кратко описание на инцидента, като се включва всяка практическа/техническа информация (тази информация се	

Образец №2, 2

представляващ Приложение № 7 към чл. 31, ал. 2 от **НАРЕДБА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ** (Обн. ДВ. бр.59 от 26 Юли 2019г., в сила от 26.07.2019 г.)

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ
към секторния ЕРИКС

Необходима информация	Детайли	Данни
	предоставя, в случай че е налична)	
Трансгранично въздействие	• Вписва се информация за евентуално трансгранично въздействие и се посочват държавите • Вписва се информация за услугите, които са засегнати	
Въздействие върху други съществени услуги	Вписва се информация на кои други съществени услуги евентуално ще окаже въздействие	
Засегната система (попълва се, ако е налична информацията)	IP Address: DNS: Operating System:	
Източник на атаката (попълва се, ако е налична информацията)	IP Address: DNS:	
Предприети действия	Описват се първоначалните действия, предприети до момента - до 2 часа от засичането на инцидента	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията	
до 5 работни дни		
Механизъм на атаката	Описва се механизмът на атаката	
Предприети действия	Описват се подробно действията, предприети за разрешаване на инцидента	

Образец №2, 3

представляващ Приложение № 7 към чл. 31, ал. 2 от **НАРЕДБА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ** (Обн. ДВ. бр.59 от 26 Юли 2019г., в сила от 26.07.2019 г.)

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ
към секторния ЕРИКС

Необходима информация	Детайли	Данни
Необходимост от коригиращи действия	Има ли необходимост от промяна в настройките на защитните стени, WAF или др. Промяна на политиката за сигурност, ако се налага Обучение на персонала	
Анализ на артефаки	Описват се резултатите от анализа на артефактите, ако има установени такива, и инструментите, използвани за това. Изпраща се копие от артефактите	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията	

Забележка. Попълва се допълнителна информация в случай на необходимост.

Изготвил:
Георги Лазаров
/специалист комп. мрежи и системи/