Европейски съюз

ОПАК. Експерти в действие

Европейски социален фонд
Инвестиции в хората

Проект „**Подобряване на административното обслужване на потребителите чрез надграждане на централните системи на електронното правителство**”” с рег. № К11-32-1/ 20.9.2011 г., осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет”

Проектът се финансира от Европейския социален фонд и от държавния бюджет на Република България

СЪЗДАВАНЕ НА УНИФИЦИРАНИ ИЗИСКВАНИЯ КЪМ ЦЕНТРОВЕТЕ ЗА ОСОБЕНО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ

УКАЗАНИЯ И ПРОЦЕДУРИ ЗА ПРИЛОЖЕНИЕ НА МЕТОДИКАТА ЗА ПРИЛОЖЕНИЕ НА ЕДИННИТЕ ДЪРЖАВНИ ИЗИСКВАНИЯ ЗА ИЗГРАЖДАНЕ, СЕРТИФИЦИРАНЕ И ПОДДЪРЖАНЕ НА НИВОТО НА СИГУРНОСТ НА ЦЕНТРОВЕ ЗА СЪХРАНЕНИЕ НА ОСОБЕНО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ ЗА НУЖДИТЕ НА ЦЕНТРАЛНА ДЪРЖАВНА АДМИНИСТРАЦИЯ

Съдържание

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

ДМА	**Дълготрайни материални активи**
ДНМА	**Дълготрайни нематериални активи**
ЕУИЦСОЧИ	**Единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация**
ИС	**Информационна сигурност**
ИТСОЦСОЧИ	**Отговорник сигурност на информацията на Център за съхранение на особено чувствителна информация**
КВ	**Коефициент на въздействие**
КС	**Коефициент на съответствие**
МДВП	**Максимално време на прекъсване**
МИС	**Мениджър информационна сигурност**
ОСР	**Остатъчна стойност на риска**
ПСР	**Първична стойност на риска**
СВК	**Стойност на въздействие на контрола**
СУСИ	**Система за управление на сигурността на информацията**
ЦСОЧИ	**Център за съхранение на особено чувствителна информация**
BDS	**Български държавен стандарт**
IRCA	**Международен регистър на сертифицираните одитори**
ISO	**International Standard Organization**

Настоящите Указания за прилагане на Методика за изграждане и сертификация на центрове за съхранение на особено чувствителна информация указват реда за изпълнение на разработените процедури за прилагане на Методиката и обхвата на тяхното приложение.

Процедури за прилагане на Методика за изграждане и сертификация на центрове за съхранение на особено чувствителна информация:

1. ПРОЦЕДУРА ЗА АДАПТИРАНЕ НА ПРОЦЕСА ЗА ОСИГУРЯВААНЕ НА СЪОТВЕТСТВИЕ С ЕДИННАТА СИСТЕМА ОТ ДЪРЖАВНИ ИЗИСКВАНИЯ И ИЗИСКВАНИЯТА НА БДС ISO/IEC 27001:2006 КЪМ СПЕЦИФИКАТА НА ОБЕКТА ЗА ПРИЛОЖЕНИЕ

Процедурата определя реда за извършване на начален одит за съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006, както и за адаптиране на изискванията към конкретния ЦСОЧИ. Тя дава вход към процедурата за определяне на специфичния обхват на проекта за постигане и поддържане на устойчиво съответствие.

2. ПРОЦЕДУРА ЗА ОПРЕДЕЛЯНЕ НА СПЕЦИФИЧНИЯ ОБХВАТ И ПОСЛЕДОВАТЕЛНОСТТА НА ПРОЦЕДУРИТЕ ПРИ УСТАНОВЯВАНЕ И ПОДДЪРЖАНЕ НА СЪОТВЕТСТВИЕТО С ЕДИННАТА СИСТЕМА ОТ ДЪРЖАВНИ ИЗСКВАНИЯ ОТ ГЛЕДНА ТОЧКА НА ОБЕКТА ЗА ПРИЛОЖЕНИЕ.

Тази процедура указва реда и действията за дефиниране на специфичния обхват на проекта за постигане и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 в ЦСОЧИ и последователността от процедури за реализирането му.

3. ПРОЦЕДУРА УПРАВЛЕНИЕ НА ДОКУМЕНТИ И ЗАПИСИ.

Определя реда за създаване, одобрение, разпространение, изменение, съхранение на документите, изтегляне на невалидните документи в обхвата на Единните унифицирани изисквания към центрове за съхранение на особено чувствителна информация (ЕУИЦСОЧИ) и внедрената система за управление на сигурността на информацията (СУСИ), а така също и правилата за създаване, идентифициране, съхранение, възстановяване, опазване и достъп до записите от този обхват.

4. ПРОЦЕДУРА ЗА ОЦЕНКА НА МОМЕНТНОТО НИВО НА РИСКА ПРИ СЪХРАНЯВАНЕТО И ОПЕРИРАНЕТО С ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ И ОПРЕДЕЛЯНЕ НА ПРИОРИТЕТИТЕ И СПЕЦИФИЧНИТЕ МЕРКИ ЗА ПРЕВЕНЦИЯ

Определя реда за идентифициране и остойностяване на активите в обхвата на приложение на СУСИ и ЕУИЦСОЧИ за даден ЦСОЧИ; подхода за идентифициране на заплахите, уязвимостите и въздействието, което загубата на поверителност, цялостност и наличност може да окаже върху тези активи, както и начините за анализиране и оценяване на рисковете за сигурността на информацията.

5. ПРОЦЕДУРА ЗА ТЕХНИЧЕСКО И ОРГАНИЗАЦИОННО ПРОЕКТИРАНЕ НА СПЕЦИФИЧНАТА СИСТЕМА ОТ МЕРКИ ЗА ПОСТИГАНЕ И ПОДДЪРЖАНЕ НА УСТОЙЧИВА СЪВМЕСТИМОСТ СЪС СИСТЕМАТА ОТ ЕДИННИ ДЪРЖАВНИ ИЗИСКВАНИЯ

Определя реда и начините за проектиране на специфичната система от мерки за постигане и поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ.

6. ШАБЛОН ЗА РАЗРАБОТВАНЕ НА ПРОЕКТ ЗА РЕАЛИЗИРАНЕ НА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ПОСТИГАНЕ И ПОДДЪРЖАНЕ НА УСТОЙЧИВА СЪВМЕСТИМОСТ СЪС СИСТЕМАТА ЗА ЕДИННИ ДЪРЖАВНИ ИЗИСКВАНИЯ

7. ПРОЦЕДУРА ЗА МОНИТОРИНГ НА ИНДИКАТОРИТЕ ЗА ИЗПЪЛНЕНИЕ И ОСИГУРЯВАНЕ НА УСТОЙЧИВО ВЪВ ВРЕМЕТО СЪОТВЕТСТВИЕ С ЕДИННИТЕ ДЪРЖАВНИ ИЗИСКВАНИЯ И ИЗИСКВАНИЯТА НА БДС ISO/IEC 27001:2006.

Процедурата определя реда и начините за осъществяване на мониторинг на индикаторите за изпълнение и осигуряване на устойчиво във времето съответствие с Единните държавни изисквания и изискванията на БДС ISO/IEC 27001:2006.

8. ПРОЦЕДУРИ УПРАВЛЕНИЕ НА ПРОМЕНИТЕ И ИНЦИДЕНТИТЕ ПРИ ПОДДЪРЖАНЕ НА УСТОЙЧИВА СЪВМЕСТИМОСТ СЪС СИСТЕМАТА ОТ ЕДИННИ ДЪРЖАВНИ ИЗИСКВАНИЯ.

Процедурата за управление на промените определя действията за идентифициране на необходимостта, оценка, одобряване, внедряване и преглед на промените при поддържане на устойчива съвместимост с Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, стандарта BDS ISO/IEC 27001:2006 и документите на внедрената СУСИ.

Процедурата за управление на инциденти определя реда за действие при идентифициране на инциденти по отношение сигурността на информацията и за докладване за пробиви и слабости в сигурността на информацията с оглед поддържане на устойчива съвместимост с Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, стандарта BDS ISO/IEC 27001:2006 и документите на внедрената СУСИ.

9. ПРОЦЕДУРА ЗА ВЪНШЕН И ВЪТРЕШЕН ОДИТ.

Определя начина на изпълнение на процеса на планиране, извършване на одити, докладване на резултатите и съхраняване на записите от проверки на Центрове за съхранение на особено чувствителна информация, внедрените в тях системи за управление на сигурността на информацията (СУСИ) и процесите, необходими за функционирането им, с цел независимо оценяване на съответствието им спрямо изискванията на стандарта BDS ISO/IEC 27001:2006 и Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация (ЕУИЦСОЧИ).

10. ПРОЦЕДУРА РАЗРАБОТВАНЕ И ПРИЛАГАНЕ НА КОРИГИРАЩИ ДЕЙСТВИЯ ПРИ УСТАНОВЯВАНЕ НА НЕСЪОТВЕТСТВИЯ СЪС СПЕЦИФИЧНИЯ ОБХВАТ И ИНДИКАТОРИТЕ ЗА ИЗПЪЛНЕНИЕ НА ЕДИННИТЕ ДЪРЖАВНИ ИЗИСКВАНИЯ ЗА ОБЕКТА НА ПРИЛОЖЕНИЕ.

Тази процедура определя реда за изпълнение на дейностите по разработване, прилагане и преглед на коригиращи действия при установяване несъответствия със специфичния обхват и индикаторите за изпълнение на ЕУИЦСОЧИ, стандарта BDS ISO/IEC 27001:2006 или документите на внедрената СУСИ, а така също дейностите за определяне и отстраняване на причините за потенциални несъответствия.

ПРИЛОЖЕНИЯ:

ПРИЛОЖЕНИЕ 1: ПРОЦЕДУРА ЗА АДАПТИРАНЕ НА ПРОЦЕСА ЗА ОСИГУРЯВАНЕ НА СЪОТВЕТСТВИЕ С ЕДИННАТА СИСТЕМА ОТ ДЪРЖАВНИ ИЗИСКВАНИЯ И ИЗИСКВАНИЯТА НА БДС ISO/IEC 27001:2006 КЪМ СПЕЦИФИКАТА НА ОБЕКТА ЗА ПРИЛОЖЕНИЕ

1. ЦЕЛ

Тази процедура определя реда за извършване на начален одит за съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006, както и за адаптиране на изискванията към конкретния ЦСОЧИ. Тя дава вход към процедурата за определяне на специфичния обхват на проекта за постигане и поддържане на устойчиво съответствие.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща всички дейности по планиране, провеждане и документиране на начален одит за съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006, както и анализ на специфичната необходимост от постигане на това съответствие и адаптиране на изискванията за съответствие към конкретния ЦСОЧИ.

3. ОТГОВОРНОСТИ

Ръководителят на Център за съхранение на особено чувствителна информация:

• Отговаря за цялостното прилагане на настоящата процедура при извършване на одити за съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006.

Мениджърът по ИС:

- Отговаря за цялостния процес на подготовка програмата за одити, подбор на одиторски екип, разработка на планове за одити, одитиране и документиране на одита.
- Изготвя анализ на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЦСОЧИ и стандарта BDS ISO/IEC 27001:2006 към конкретния ЦСОЧИ.

Водещият одитор:

- Отговаря за оперативното управление на дейностите по провеждане на одит за съответствие.

Одиторите:

- Осъществяват безпристрастна оценка на дейностите.

Системен аналитик:

- Наблюдава данните от мониторинга на параметрите, извършван от системата за мониторинг и ранно предупреждение и прогнозира или открива тенденции в

повишаване на рисковия потенциал на един или повече основни или спомагателни елементи от инфраструктура на ЦСОЧИ, изготвя доклади.

Ролите и отговорностите по отношение стъпките на процедурата са посочени в RACI (Изпълняващ/Отговарящ/Консултиращ/Информиран) матрица в Таблица 1 по-долу:

Таблица 1

Роля: / **Стъпка:**	**Ръководтел ЦСОЧИ**	**Мениджър по ИС**	**Водещ одитор**	**Одитор**	**Системен аналитик**
Определяне обхват и цели на одита	R/A	C			
Определяне критериите на одита	R/A	C			
Назначаване на отговорник за одита	R/A	I			
Разработване програма за одита	A	R			
Определяне на методика за провеждане на одита	I	R/A			
Определяне и осигуряване на необходимите ресурси за одита	A/R	C			
Подбор на одиторски екип	A	R	I	I	
Преглед на документацията при подготовка на одита	I	C	A/R		
Подготовка на	I	C	A/R	C	

план на одита и разпределяне на работата между одиторите					
Извършване на дейности по същинския одит	I	C	A/R	R	C
Подготовка и разпространение на доклад от одита	I	I	A/R	C	I
Подготовка и документиране на анализа на специфичната необходимост от постигане на съответствие	R/A	I			
Подготовка и документиране на анализа на специфичната необходимост от постигане на съответствие	I	A/R	C		C

R= Изпълняващ A= Отговарящ C= Консултиращ I= Информиран

4. ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

Одит - систематичен, независим и документиран процес за получаване на доказателства и обективното им оценяване, за да се определи степента, до която са удовлетворени критериите на одита – в случая съответствие между Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, документираната система за управление на сигурността на информацията, и изискванията на стандарта BDS ISO/IEC 27001:2006 от една страна и съществуващите практики и състояние на проверявания ЦСОЧИ.

Критерии на одита - съвкупност от политики, процедури или изисквания, използвани за съпоставка.
Програма за одит - мерки, предназначени за съвкупност от един или повече одити, планирани за определен период от време и насочени към конкретна цел.
План на одита – описание на дейности и на необходимата подготовка за извършване на одит.
Одиторски екип – един или повече одитори, които извършват одит, подпомагани при необходимост от технически експерти. Един от одиторите в одиторския екип се определя за водещ одитор.
Доказателства от одит - записи, изявления за факт или друга информация, свързана с критериите за одит, която може да бъде проверена.
Заключения от одит - резултати от оценката на набраните доказателства от одит чрез критериите за одита.
Съответствие–изпълнение на изискване.
Несъответствие – неизпълнение на изискване.
Система за управление – рамка от политики, процедури, указания и свързаните с тях ресурси за постигане на целите на организацията.
Система за управление на сигурността на информацията (СУСИ) – част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията.
ЦСОЧИ – център за съхранение на особено чувствителна информация.
ЕУИЦСОЧИ – единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация.
ИС – информационна сигурност.

5. ОПИСАНИЕ НА ПРОЦЕДУРАТА

5.1. Планиране на начален одит за съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006

5.1.1. Обхват и цели на одита

Отговорен за определяне на обхвата и целите на първоначалния одит за съответствие е изискванията на ЕУИЦСОЧИ е Ръководител на ЦСОЧИ. Обхватът на одита може да се отнася към цялата площадка, работни звена и процеси на ЦСОЧИ или за части от тях. Целите на одита са доказване на съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006.

5.1.2. Критерии на одита

Критерии на одита са:

- ЕУИЦСОЧИ.
- Изискванията на BDS ISO/IEC 27001:2006.
- Изискванията на внедрената в ЦСОЧИ СУСИ.

Наличието на валиден, действащ сертификат за съответствие с изискванията на стандарта ISO/IEC 27001:2005, издаден от сертификационен орган, имащ европейска акредитация, се счита достатъчно доказателство за съответствие спрямо изискванията на стандарта BDS ISO/IEC 27001:2006 и внедрената СУСИ.

5.1.3. Назначаване на отговорник за одита

Ръководител на ЦСОЧИ възлага отговорността за провеждане на началния одит за съответствие с изискванията на ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006 на Мениджър по ИС.

5.1.4. Програма за провеждане на одита

Назначеният отговорник за провеждане на одит въз основа на дефинирания обхват и цели за провеждане на одита разработва Програма на начален одит за съответствие с изискванията на ЕУИЦСОЧИ (Образец 1). Програмата за одита може да включва един или повече одити за определен период от време, насочени към основните цели, определени в секция 5.1.1. Обект на отделните одити могат да бъдат отделни площадки, процеси или зони от ЦСОЧИ. Програмата за провеждане на одита се утвърждава от Ръководител на ЦСОЧИ.

Отговорникът за провеждане на одита определя и прави анализ на рисковете за програмата за одит и на тази база определя Методика за провеждане на одита.

5.1.5. Определяне на методика за провеждане на одита

Методиката за провеждане на одит включва съвкупност от процедури, методи (техники) и действия, прилагани от одиторския екип спрямо обекта на одита с цел получаване на необходимите обективни доказателства от одита. Методиката за провеждане на одита е уникална и е съобразена със съответната програма за провеждане на одит. Използват се методи за събиране на доказателства като: преглед на документи, преглед на записи, наблюдение на процеси и практики, интервю със сътрудници или външни страни и др. Като приложение към методиката за провеждане на одита се разработват въпросници, покриващи всички аспекти в рамките на обхвата на одита.

5.1.6. Определяне и осигуряване на необходимите ресурси за одита

Назначеният отговорник за провеждане на одит за установяване на съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006 прави анализ на необходимите ресурси за изпълнение на програмата за одит. На тази база подготвя доклад за необходимостта от ресурси и го предоставя на Ръководител на ЦСОЧИ за утвърждаване. След утвърждаване на доклада за необходимостта от ресурси Ръководител на ЦСОЧИ е отговорен за тяхното осигуряване.

5.1.7. Подбор на одиторски екип

Отговорникът за провеждане на одит извършва подбор на одиторския екип. Одиторите могат да бъдат сътрудници на ЦСОЧИ или компетентни външни специалисти.
Подборът на одиторския екип (брой и състав) се прави въз основа на следните критерии:

- Обхвата и сложността на одита;
- Избраната методика за одит;
- Правни и договорни изисквания;
- Цялостната компетентност на одиторския екип, необходима за постигане на целите;
- Необходимостта да се осигури независимост на членовете на одиторския екип от одитираните дейности (никой одитор няма право да одитира собствената си дейност);
- Способността на членовете на одиторския екип да взаимодействат ефикасно и да работят заедно с одитираните представители на ЦСОЧИ.

Специфичната компетентност на членовете на одиторския екип се доказва както следва:

- За доказване на одиторска компетентност по отношение на изискванията на BDS ISO/IEC 27001:2006 – доказателство, че одиторът е сертифициран от Международния регистър на сертифицираните одитори IRCA одитор/вътрешен одитор на системи за управление сигурността на информацията СУСИ (IRCA регистрационен номер, карта за удостоверяване на статута);
- За доказване на одиторска компетентност по отношение на ЕУИЦСОЧИ – подходящ професионален опит в одитираната област.

При необходимост, към екипа се привличат технически експерти със съответната компетентност. Те работят под ръководството на одитор, но не могат да действат като одитори.
Броят и съставът на одиторския екип, включително определеният водещ одитор, се утвърждава от Ръководител ЦСОЧИ с изрична заповед.

5.2. Провеждане и документиране на одит за съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006

5.2.1. Преглед на документацията при подготовка на одита

Отговорникът за провеждане на одита осигурява на водещия одитор по негово искане достъп до необходимата документация в обхвата на ЕУИЦСОЧИ и внедрената СУСИ.
В своето искане водещият одитор посочва вида на документите, до които желае достъп.
Целта на предварителния преглед на документацията е да се събере информация за подготовка на одитните дейности, както и да се получи общ поглед върху обхвата на наличната документация, за да се открият възможни липси.
Документацията е необходимо да включва доколкото е възможно документи и записи от обхвата на ЕУИЦСОЧИ и СУСИ, както и доклади от последните извършени одити.
Прегледът на документацията е съобразен с обхвата и целите на одита, големината и сложността на организацията и процесите в одитирания ЦСОЧИ.

5.2.2. Подготовка на план на одита и разпределяне на работата между одиторите

Водещият одитор изготвя План на началния одит за съответствие с изискванията на ЕУИЦСОЧИ (Образец 2) на база програмата за одита и информацията от документацията, до която е получил достъп по реда от секция 5.2.1. Планът за одит следва да е съобразен с целите на одита, обхвата на одита и неговата сложност, въздействието върху одитираните процеси, компетентността на членовете на екипа, методиката за провеждане на одита и др. Степента на детайлизация на плана за одит трябва да отразява целите на одита, обхвата на одита и неговата сложност. Като минимум той трябва да съдържа следната информация:

- Цели на одита;
- Обхват на одита (включително определяне на одитираните звена, зони и процеси);
- Критерии на одита;
- Методите за одит, които ще се използват;
- Ролите и отговорностите на членовете на одиторския екип;
- Местоположение, дати, очаквани времена и продължителност на отделните дейности на одита;
- Определяне на подходящи ресурси за отделни области на одита.

Препоръчва се планът на одита да включва също информация за:

- Представители на одитираните зони/звена/процеси;
- Последващи действия от предишни одити;
- Последващи действия от планирания одит.

След изготвяне на плана на одита водещият одитор съгласува плана с отговорника за провеждане на одита и Мениджър по ИС. Съгласуват се въпросите, свързани с конфиденциалността на информацията съгласно правилата на ЦСОЧИ.
Отговорникът за провеждане на одита информира представителите на одитираните процеси, звена, зони, местоположения относно плана за одит.
След съгласуване на плана на одита и въпросите за конфиденциалност на информацията водещият одитор след консултации с одиторите възлага индивидуална отговорност за одитиране на конкретни процеси, дейности, звена или местоположения.
При възлагане на задачите водещия одитор взема предвид независимостта и компетентността на одиторите и ефикасното използване на ресурси.
Водещият одитор провежда инструктаж на членовете на екипа за разпределяне на задачите и евентуалното вземане на решение при възможни промени.

5.2.3. Извършване на дейности по същинския одит

Дейностите по същинския одит започват с откриваща среща на одита, на която присъстват:

- Ръководител на ЦСОЧИ;
- Представителите на одитираните процеси/звена/зони/местоположения;
- Одиторският екип.

Откриващата среща се провежда на място, дата и час, определени в плана на одита.
Целта на откриващата среща е да потвърди плана на одита и възможността за изпълнение на всички задачи по одита, да представи одиторския екип.
След приключване на откриващата среща се извършва преглед на документацията от обхвата на ЕУИЦСОЧИ и внедрената СУСИ. Целта на прегледа е да определи съответствието на документацията с критериите на одита, както и да се събере информация в помощ на одитните дейности.
По време на одита одиторите обменят информация за изпълнението на одитните дейности, потенциални проблеми, констатации.
Мениджър по ИС определя при необходимост придружители, които осигуряват достъп на одиторите до работни помещения и зони и съдействат за провеждане на дейностите по одита.
По време на одита одиторите събират и проверяват информация съобразно целите, обхвата, критериите и методиката на одита като използват подходяща за ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 извадка. Методите за събиране на информация са:

- Преглед на документи и записи;
- Наблюдения;
- Интервюта.

Съществена важност за доказване на съответствието играе прегледа на докладите от Системен анализатор в резултат на наблюдение системата за мониторинг и ранно предупреждение.
Като доказателства от одита се използва само информация, която може да бъде проверена. Доказателства от одита, които водят до констатации от одита след преценяването им спрямо критериите на одита, задължително се записват от одиторите. Констатациите могат да показват съответствие или несъответствие с критериите на одита (ЕУИЦСОЧИ, изискванията на BDS ISO/IEC 27001:2006 и документите на внедрената СУСИ). Констатациите, независимо за съответствие или несъответствие се подкрепят с доказателства, които преди да бъдат записани, се преглеждат съвместно с одитирания за получаване на потвърждение за истинността им.
След приключване на дейностите по събиране на информация одиторският екип се събира, за да направи преглед на констатациите и подготви заключенията от одита. Заключенията от одита обхващат степента на съответствие с критериите на одита, и постигане на целите на одита.
На закриващо заседание (на място и час, уточнени в плана на одита) водещият одитор представя пред Ръководител на ЦСОЧИ и представителите на одитираните процеси, звена, зони и местоположения (присъствието им е по преценка на Ръководител на ЦСОЧИ) констатациите и заключенията от одита. Обсъждат се и се разрешават всички разминаващи се мнения по констатации и/или заключения. Водещият одитор и Ръководител на ЦСОЧИ потвърждават срока и съгласуват начина за представяне на доклад от одита.

5.2.4. Подготовка и разпространение на доклад от одита

Водещият одитор, въз основа на собствените си и на одиторите записани доказателства и констатации и на заключенията от одита, подготвя Доклад от проведен начален одит за съответствие с изискванията на ЕУИЦСОЧИ (Образец 3). Докладът на одита трябва да бъде съобразен с методиката на одита, договорения обем и съдържание на доклада, да дава пълен, точен и кратък запис на одита. Докладът от одит като минимум трябва да съдържа:

- Цел на одита;
- Обхват на одита;
- Критерии на одита;
- Членове на одиторския екип;
- Срок на одита;
- Одитирани звена и процеси;
- Констатации от одита, подкрепени с доказателства;

- Констатирани несъответствия
- Заключения от одита за степента на изпълнение на критериите на одита;
- Дата на доклада.

Водещият одитор предава на Ръководител на ЦСОЧИ доклада от одита в договорения срок и по договорения начин. При предаване на доклада следва да се спазват добрите практики в областта на запазване на сигурността на информацията.
Одитът за съответствие се счита приключен с приемане на доклада от одит от страна на Ръководител на ЦСОЧИ.

5.3. Анализ на специфичната необходимост от постигане на съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006. Адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 към конкретния ЦСОЧИ

5.3.1. Възлагане подготовката на анализ на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 към конкретния ЦСОЧИ

Ръководител на ЦСОЧИ възлага на Мениджър по ИС изготвянето на анализ на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЦСОЧИ и стандарта BDS ISO/IEC 27001:2006 към конкретния ЦСОЧИ като му предоставя копие от доклада за извършения одит на съответствието.
Като минимум анализът съдържа диференцирани:

- Анализ на областите от ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006, по които има постигнато пълно съответствие;
- Анализ на областите, по които има постигнато частично съответствие и степен на съответствието;
- Анализ на областите, по които има пълно несъответствие;
- Анализ на спецификата на приложение в конкретния ЦСОЧИ на изискванията, по които има частично или пълно несъответствие;
- Предложение за адаптиране на изискванията, по които има частично или пълно несъответствие.

При възлагането Ръководител на ЦСОЧИ определя съдържанието на доклада и срока за неговото изготвяне.

5.3.2. Подготовка и документиране на анализа на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 към конкретния ЦСОЧИ

Мениджър по ИС детайлно проучва доклада от одита за съответствие. При необходимост се обръща с въпроси за изясняване на констатации, факти и заключения към водещия одитор и/или представители на ЦСОЧИ при извършване на одита.
Мениджър по ИС изготвя и документира анализ на специфичната необходимост от постигане на съответствие с указаното съдържание и в указания срок въз основа на:

- ЕУИЦСОЧИ;
- Изискванията на стандарта BDS ISO/IEC 27001:2006;
- Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност (ДВ 101/25.11.2008);
- Доклада от началния одит за съответствие;
- Информация от водещия одитор и представителите на ЦСОЧИ в одита за съответствие;

Предава анализа на Ръководител на ЦСОЧИ.

6. СВЪРЗАНИ ДОКУМЕНТИ

- Процедура за разработване и прилагане на коригиращи и превантивни действия при установяване на несъответствие със специфичния обхват и индикаторите за изпълнение на единните държавни изисквания за обекта на приложение;
- ISO/IEC 27001:2005;
- BDS ISO/IEC 27001:2006;
- Наредба за оперативна съвместимост и информационна сигурност.

7. ПРИЛОЖЕНИЯ

- Образец 1
- Образец 2
- Образец 3

ПРИЛОЖЕНИЕ 2: ПРОЦЕДУРА ЗА ОПРЕДЕЛЯНЕ НА СПЕЦИФИЧНИЯ ОБХВАТ И ПОСЛЕДОВАТЕЛНОСТТА НА ПРОЦЕДУРИТЕ ПРИ УСТАНОВЯВАНЕ И ПОДДЪРЖАНЕ НА СЪОТВЕТСТВИЕТО С ЕДИННАТА СИСТЕМА ОТ ДЪРЖАВНИ ИЗСКВАНИЯ ОТ ГЛЕДНА ТОЧКА НА ОБЕКТА ЗА ПРИЛОЖЕНИЕ

1. ЦЕЛ

Тази процедура има за цел да определи реда за дефиниране на специфичния обхват на проекта за постигане и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 в ЦСОЧИ и последователността от процедури за реализирането му.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща всички дейности по определяне на специфичния обхват на проекта и разработване на индивидуална версия на базовата методика за постигане и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 в ЦСОЧИ.

3. ОТГОВОРНОСТИ

Ръководителят на Център за съхранение на особено чувствителна информация:

- Отговаря за цялостното изпълнение на дейностите по настоящата процедура.

Мениджърът по ИС:

- Разработва План от мерки за постигане на съответствие;
- Разработва Методически указания за внедряване на индивидуална версия на базовата методика за установяване и поддържане на устойчиво съответствие в конкретния ЦСОЧИ;
- Извършва анализ и разработва Доклад за необходимите ресурси за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006.

Ролите и отговорностите по отношение стъпките на процедурата са посочени в RACI (Изпълняващ/Отговарящ/Консултиращ/Информиран) матрица в Таблица 1 по-долу:

Таблица 1

Роля:	**Ръководтел ЦСОЧИ**	**Мениджър по ИС**
Стъпка:		
Дефиниране на специфичен обхват на проекта за постигане и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и	A	R

BDS ISO/IEC 27001:2006		
Определяне на последователността от процедури за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001/2006	A	R
Изготвяне на анализ и доклад за необходимите ресурси за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006	A	R

R= Изпълняващ A= Отговарящ C= Консултиращ I= Информиран

4. ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

Одит - систематичен, независим и документиран процес за получаване на доказателства за съответствие между Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, документираната система за управление на сигурността на информацията, и изискванията на стандарта BDS ISO/IEC 27001:2006 от една страна и съществуващите практики и състояние на проверявания Център.

Система за управление – рамка от политики, процедури, указания и свързаните с тях ресурси за постигане на целите на организацията.

Система за управление на сигурността на информацията (СУСИ) – част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията.

ЦСОЧИ – център за съхранение на особено чувствителна информация.

ЕУИЦСОЧИ – единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация.

ИС – информационна сигурност.

5. ОПИСАНИЕ НА ПРОЦЕДУРАТА

5.1. Дефиниране на специфичен обхват на проекта за постигане и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006.

След изготвяне на Анализ на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 за конкретния ЦСОЧИ по реда на Процедура Одит за съответствие и адаптиране на

изискванията за постигане на съответствие и одобряването на предложението за адаптиране от същия анализ, Ръководител на ЦСОЧИ възлага на Мениджър по ИС изготвянето на План от мерки за постигане на съответствие (Образец 1). Планът дефинира специфичния обхват на проекта за постигане и поддържане на устойчиво съответствие с изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 и съдържа всички мерки, които следва да се приложат за постигане на желаното съответствие. Той се изготвя на базата на информация от:

- Доклада от одит за съответствие;
- Анализа на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 за конкретния ЦСОЧИ;
- ЕУИЦСОЧИ;
- BDS ISO/IEC 27001:2006;
- BDS ISO/IEC 27002:2008;
- Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност;
- Документи на внедрената СУСИ.

Планът от мерки за постигане на съответствие следва да дава информация както за необходимите мерки за постигане на съответствие, така и за свързаните с тях ресурси и срокове.

Минималната информация, която трябва да съдържа планът е както следва:

- Описание на изискването за съответствие, което трябва да се постигне;
- Документ, регламентиращ изискването (ЕУИЦСОЧИ, BDS ISO/IEC 27001:2006, Наредба за общите изисквания за оперативна съвместимост и информационна сигурност, изисквания на внедрената СУСИ);
- Тип изисквания (организационни, технологични);
- Изисквани ресурси;
- Прогнозен срок за изпълнение.

Мениджър по ИС предава подготвения План от мерки за постигане на съответствие на Ръководител на ЦСОЧИ за преглед и утвърждаване.

5.2. Определяне на последователността от процедури за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001/2006.

След утвърждаване на Плана от мерки за постигане на съответствие Ръководител на ЦСОЧИ възлага на Мениджър по ИС да определи последователността от процедури за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001/2006 като подготви Методически указания за внедряване на индивидуална

версия на базовата методика за установяване и поддържане на устойчиво съответствие в конкретния ЦСОЧИ. Методическите указания се базират на спецификата на конкретния ЦСОЧИ, установената степен на съответствие от проведения одит и следва да вземат предвид:

- Анализа на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 за конкретния ЦСОЧИ;
- Дефинирания специфичен обхват на проекта за постигане и поддържане на устойчиво съответствие (План от мерки за постигане на съответствие);
- Адаптиране и “настройка” на специфичните цели при определяне на индикаторите за измерване на съответствието с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006;
- Организационни аспекти на планирането и управлението на процеса за въвеждане на система за устойчива съвместимост с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006;
- Технологични аспекти при установяването и поддържането на съответствие с ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006 – планиране на мерките, планиране на ресурсите (при необходимост провеждане на двуфазно проектиране - идеен и работен проект на ЦСОЧИ, съгласно изискванията на Чл.4. на НАРЕДБА No 4 от 21 май 2001 г. за обхвата и съдържанието на инвестиционните проекти), изпълнение на мерките, документиране на мерките и при необходимост провеждане на двуфазно проектиране - идеен и работен проект;
- Анализа на спецификата при прилагането на процесен подход при установяването и поддържането на ЕУИЦСОЧИ за конкретния ЦСОЧИ;
- Механизми за мониторинг на индикаторите за изпълнение и осигуряване на устойчиво във времето съответствие с Единните държавни изисквания и изискванията на BDS ISO/IEC 27001:2006;
- Управление на промените и инцидентите при въвеждане и поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ и изискванията на BDS ISO/IEC 27001:2006;
- Одитиране и коригиращи мерки при установяване на несъответствия със специфичния обхват и метрика на индикаторите за изпълнение на ЕУИЦСОЧИ за обекта на приложение.

Следва да се вземе предвид необходимостта от циклично повторение на някои от процедурите с цел постигане на устойчивост и поддържане на съответствието.

Мениджър по ИС предава подготвените методически указания на Ръководител на ЦСОЧИ за преглед и утвърждаване.

5.3. Изготвяне на анализ и доклад за необходимите ресурси за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006.

След утвърждаване на методическите указания за внедряване на индивидуална версия на базовата методика за установяване и поддържане на устойчиво съответствие в конкретния ЦСОЧИ Ръководител на ЦСОЧИ възлага на Мениджър по ИС извършване на анализ и подготовка на Доклад за необходимите ресурси за установяване и поддържане на устойчиво съответствие с ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006. При извършване на анализа мениджър по ИС използва информацията от Плана от мерки за постигане на съответствие и Методическите указания за внедряване на индивидуална версия на базовата методика за установяване и поддържане на устойчиво съответствие в конкретния ЦСОЧИ, прави проучване на пазарни цени.

Докладът за необходимите ресурси трябва да съдържа задължително информация за:

- Необходимия паричен ресурс за закупуване на технически средства и материали по всяко от мерките в Плана от мерки за постигане на съответствие;
- Необходимия паричен ресурс за закупуване на услуги от външни лица по всяка от мерките в Плана от мерки за постигане на съответствие;
- Необходимия ресурс време за използване на сътрудници от ЦСОЧИ (човекодни по специалисти) за всяка от мерките в Плана;
- Необходимия ресурс време за използване на собствени технически средства (дни за всяко конкретно техническо средство) за всяка от мерките.

Докладът посочва необходимите срокове за ресурсно осигуряване с отчитане на етапите на проекта.

След изготвянето му Мениджър по ИС предава Доклада за необходимите ресурси на Ръководител на ЦСОЧИ за преглед и утвърждаване съгласно вътрешните правила на ЦСОЧИ. Реализация на проекта за установяване и поддържане на устойчиво съответствие може да започне след утвърждаване на Доклада за необходимите ресурси.

6. СВЪРЗАНИ ДОКУМЕНТИ

- ЕУИЦСОЧИ;
- BDS ISO/IEC 27001:2006;
- BDS ISO/IEC 27002:2008;
- Наредба за общите изисквания за оперативна съвместимост и информационна сигурност.

7. ПРИЛОЖЕНИЯ

- Образец 1

ПРИЛОЖЕНИЕ 3. ПРОЦЕДУРА УПРАВЛЕНИЕ НА ДОКУМЕНТИ И ЗАПИСИ.

1. ЦЕЛ

Тази процедура определя реда за създаване, одобрение, разпространение, изменение, съхранение на документите, изтегляне на невалидните документи в обхвата на Единните унифицирани изисквания към центрове за съхранение на особено чувствителна информация (ЕУИЦСОЧИ) и внедрената система за управление на сигурността на информацията (СУСИ), а така също и правилата за създаване, идентифициране, съхранение, възстановяване, опазване и достъп до записите от този обхват.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща всички дейности по създаване, одобрение за адекватност, преглед и изменение, разпространение, съхранение на документи, изтегляне на невалидни документи, идентифициране на външни документи, а така идентифициране, съхранение, възстановяване, опазване и достъп до записи от обхвата на ЕУИЦСОЧИ и внедрената СУСИ.

3. ОТГОВОРНОСТИ

Ръководител на ЦСОЧИ:

- Преглежда и утвърждава документите преди издаване;
- Преглежда и утвърждава документите при изменение.

Мениджър по ИС:

- Отговаря за цялостното управление на документите и записите в организацията.

Отговорник за създаване на документ:

- Отговаря за създаване на възложения му от Ръководител ЦСОЧИ документ съгласно изискванията на настоящата роцедура

Системен администратор:

- Отговаря за съхранението, защитата и архивирането на документи и записи, съхранявани върху управлявания от него актив (физически или виртуален).

Служители:

- Съхраняват контролираните копия на документите и ги прилагат в работата си.

Ролите и отговорностите по отношение стъпките на процедурата са посочени в RACI (Изпълняващ/Отговарящ/Консултиращ/Информиран) матрица в Таблица 1 по-долу:

Таблица 1

Роля:	Ръководтел	Мениджър	Системен	Отговорник	Служител

Стъпка:	**ЦСОЧИ**	**по ИС**	**администратор**	**за създаване на документ**	**и**
Идентифициране на необходимостта от създаването на документ/нова версия на документ	A	R/C	R	R	R
Създаване/промяна на документ		C		R/A	
Верификация на документа, одобрение, определяне нивото на класификация и достъп до документи	A	R/A		C	
Разпространение на документа и изземване на неактуални версии	I	R/A	R		
Съхранение	I	R/A	R/A		R/A
Унищожаване на документи	I	R/A	R		
Управление на външни документи	I	R/A			R
Създаване на записи	R/A	R/A	R/A	R/A	R/A
Идентифициране на записи	R/A	R/A	R/A	R/A	R/A
Съхранение и защита на записите	I	R/A	R		
Достъп до записи	I	R/A	R	I	I
Унищожаване на записи	I	R/A			

R= Изпълняващ A= Отговарящ C= Консултиращ I= Информиран

4. ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

Система за управление – рамка от политики, процедури, указания и свързаните с тях ресурси за постигане на целите на организацията.

Система за управление на сигурността на информацията (СУСИ) – част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията.

Политика на СУСИ – общи намерения и насоки на организацията по отношение на информационната сигурност, официално изразени от нейното ръководство. Основен документ на СУСИ.

Процедура - определен начин за извършване на дейност или процес.

Процедурен документ - документ, който съдържа описание на процедура.

Оперативен документ - документ, който носи конкретна информация за дейности (бланка, заповед, протокол, писмо и др.).

Документ–информация и нейните носители**.**

Запис - документ, съдържащ получени резултати или предоставящ доказателство за извършени дейности.

Обективно доказателство - данни, потвърждаващи съществуването или достоверността на нещо.

Изменение на документи - всяко поправяне, изключване или добавяне на данни в документите без промяна на означението им.

ЦСОЧИ – център за съхранение на особено чувствителна информация.

ЕУИЦСОЧИ – единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация.

ИС – информационна сигурност.

5. ПРОЦЕДУРА

5.1. Управление на документи

5.1.1. Документи, подлежащи на управление по настоящата процедура

5.1.1.1. Документи на СУСИ:

- Политика и цели по сигурността на информацията;
- Обхват на СУСИ;
- Описание на методиката за оценка на риска;
- Доклад за оценка на риска;
- План за третиране на риска;
- Декларация за приложимост;
- Процедури;

- Инструкции;
- Оперативни документи – форми.

Документите от тази категория са обект на създаване, одобрение за адекватност, преглед и изменение, разпространение, съхранение, изтегляне на невалидни документи. При наличие на документи, чието управление е обект на законов или подзаконов акт, те се управляват в съответствие с него.

5.1.1.2. Външни документи

За външни документи се считат всички документи, които са свързани с ИС, но не са част от обхвата на ЕУИЦСОЧИ или СУСИ. Те могат да бъдат например:

- Закони;
- Подзаконови нормативни актове;
- Отраслови нормали;
- Стандарти;
- Документи на ЕУИЦСОЧИ;
- Инструкции и указания;
- Договори;
- Други външни документи, от които произтичат задължения или предоставят информация, свързана с ЕУИЦСОЧИ и СУСИ.

Документите от тази категория са обект на идентифициране, разпространение, съхранение и изземване. При наличие на документи, чието управление е обект на законов или подзаконов акт, те се управляват в съответствие с него.

5.1.1.3. Записи на ЕУИЦСОЧИ и СУСИ

Управлението на записите като особен тип документи става съгласно изискванията на 5.2 от настоящата процедура.

5.1.2. Идентифициране на необходимостта от създаването на документ/нова версия на документ

Разработване на документ или нова версия на документ се извършва след писмено предложение от сътрудник на ЦСОЧИ (в частност от Мениджър по ИС), идентифицирал необходимостта от създаването му към Мениджър по ИС. Мениджър по ИС поставя писмена резолюция със свое становище относно предложението и докладва на Ръководител на ЦСОЧИ за направеното предложение като излага и становището си по него. Разработването на нов документ/нова версия на документ започва след писмена резолюция на Ръководител на ЦСОЧИ като в нея посочва и отговорник за създаването му.

5.1.3. Създаване/промяна на документ

Отговорникът за създаване на новия документ (нова версия на документ) започва разработка след детайлно запознаване с направеното предложение за създаването му, резолюциите на Мениджър по ИС и Ръководител на ЦСОЧИ. При създаване на документа се спазват следните правила:

Оформяне на Header на документа:

Всички страници на документите съдържат Header с информация за документа, собственика на документа, принадлежност към група документи и др. както следва:
За първа или заглавна страница на документа се използва следната структура и съдържание на Header:

Лого	**Единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация (ЕУИЦСОЧИ)**	Версия	Стр.
		поредна	*Пор./всичко*
	Център за съхранение на особено чувствителни данни към ……		
Разработил:	Мениджър по ИС	**Подпис**	*дд.мм.гггг*
Утвърдил:	Ръководител на ЦСОЧИ	**Подпис**	*дд.мм.гггг*

За втора и следващи страници на документа се използва следната структура и съдържание на Header

Лого	**Единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация (ЕУИЦСОЧИ)**	Версия	Стр.
		поредна	*Пор./всичко*
	Център за съхранение на особено чувствителни данни към ……		
	НАИМЕНОВАНИЕ НА ДОКУМЕНТА		

Оформяне на заглавна страница на документа:

Политиката по ИС и процедурите на СУСИ имат заглавна страница, която съдържа Header за първа страница и заглавие със следното съдържание, големина и форматиране:

ТИП НА ДОКУМЕНТА

НАИМЕНОВАНИЕ НА ДОКУМЕНТА

Останалите документа не изискват наличие на заглавна страница.

Структура на документите:

Процедурните документи на СУСИ имат следната структура:

- Цел;
- Област на приложение;
- Отговорности;
- Термини, определения и използвани съкращения;
- Процедура;
- Свързани документи;
- Приложения.

В раздел ЦЕЛ се посочват целите/предназначението на документа.
В раздел ОБЛАСТ НА ПРИЛОЖЕНИЕ се посочва съвкупността от дейности, към които се отнася документа.
В раздел ОТГОВОРНОСТИ се посочват лицата, отговорни за изпълнение на основните дейности от процедурата и обхвата на техните отговорности.
В раздел ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЕ се дефинират специфичните думи, изрази и съкращения, използвани в процедурния документ (ако има такива).
В раздел ПРОЦЕДУРА се описва структурата и съдържанието на процедурата, като ясно се описва последователността от действия, които трябва да бъдат предприети - какво, от кого, кога, къде и как трябва да бъде направено, какви документи се използват, как се управляват дейностите, ред за записване.
В раздел СВЪРЗАНИ ДОКУМЕНТИ се посочват наименованията на външни или процедурни документи, на които в разработвания документ е направено позоваване или са свързани с него.
В раздел ПРИЛОЖЕНИЯ се посочват оперативните документи (образци), генерирани от разработвания документ, които ще бъдат използвани за създаване на записи по ИС.

Структурата на документите, посочени в Модела за разработване на проект за реализиране на техническите и организационни мерки за постигане и поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ е задължителна.

Останалите документи на СУСИ имат индивидуална структура, определена според изискванията на ЕУИЦСОЧИ, стандарта BDS ISO/IEC 27001:2006, приложимите нормативни документи, изискванията на заинтересованите страни и практиките на ЦСОЧИ.

5.1.4. Верификация на документа, одобрение, определяне нивото на класификация и достъп до документи.

След приключване на разработката отговорникът за създаване на новия документ (новата версия на документ) предава документа на Мениджър по ИС за преглед, верификация и евентуално редактиране. След оформяне на документа Мениджър по ИС го представя на Ръководител на ЦСОЧИ за одобрение и утвърждаване. След утвърждаване на документа Мениджър по ИС го включва в **Регистър на документите на СУСИ и техните ползватели** (актуализира Регистъра) (Образец 1). Регистърът задължително съдържа: наименование на документите, версия, дата на утвърждаване, ниво на класификация, ползватели на документите (сътрудници с достъп до документа) с обозначен носител на използваното копие (контролирано хартиено копие или електронно копие). В ЦСОЧИ са приети 4 нива на класификация, в съответствие с Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (ДВ 101/25.11.2008):

- Ниво „0“ или „D” – ниво на свободен достъп;
- Ниво „1“ или „C“ – ниво на свободно управление на достъпа;
- Ниво „2“ или „B“ – ниво на принудително управление на достъпа;
- Ниво „3“ или „A“ – ниво на проверена сигурност,

като Ръководител на ЦСОЧИ с изрична заповед определя принадлежността на типове и видове документи към съответното ниво. Правата на достъп до документи се определят от Мениджър по ИС на база тяхното ниво на класификация и нуждата от достъп до тях, свързана с особеностите в задълженията на съответния сътрудник. Допуска се даване на временен достъп до документи.

За документите с нива „1“ (C). „2“ (B) и „3“ (A) върху носителя на документа се поставя съответния гриф.

5.1.5. Разпространение на документа и изземване на неактуални версии. Контролирани копия на документи

Мениджър по ИС отговаря за разпространение на утвърдените документи (нови версии на документи) до имащите право ползватели съгласно **Регистър на документите на СУСИ и техните ползватели.** Контролирани копия на документи на хартиен носител се предават лично от Мениджър по ИС на имащото право лице срещу подпис. Едновременно с това се изземват контролираните копия на неактуалната вече версия.

Електронната версия на документа се записва върху изрично определен от Ръководител на ЦСОЧИ актив от информационната система (сървър, дисков масив) с осигурено ниво на информационна сигурност съгласно заповедта на Ръководител на ЦСОЧИ. Достъпът до различните документи се организира съобразно правата за достъп от **Регистъра на документите на СУСИ и техните ползватели.** Прекратява се достъпа на служителите до старата неактуална версия на електронния документ, като той се премества в архивна папка и остава видим само за Мениджър по ИС. Новият документ и архивираното копие на неактуалния документ се включват в плана за бекъп на информационните активи.
Не се допуска разпечатване на електронната версия на документа от служители.

5.1.6. Съхранение

Отговорен за съхранението на контролираното хартиено копие на документа е сътрудникът, на когото е връчен срещу подпис от Мениджър по ИС. Отговорният сътрудник е задължен да осигури сигурно съхранение на документа по начин, определен за съответната група на класификационно ниво до момента на изземването му от страна на Мениджър по ИС.
Отговорни за съхранението на електронната версия на документа са Мениджър по ИС и системният администратор, отговарящ за администриране на съответния информационен ресурс. Не се допуска разпечатване на електронната версия на документа.
Отговорен за съхранение на неактуалните хартиени версии на документа е Мениджър по ИС. Той архивира излезлите от употреба хартиени контролирани копия на документи като поставя върху тях гриф „Архив“. Съхранява се по едно контролирано копие от последните две неактуални версии на документите. Останалите копия се унищожават по реда на секция 5.1.7.
Отговорен за съхранение на неактуалните електронни версии на документа е Мениджър по ИС и системният администратор, отговарящ за информационният ресурс, на който се намира архивната папка с неактуални версии. Съхраняват се последните две неактуални версии на документа, останалите се унищожават по реда на секция 5.1.7.

5.1.7. Унищожаване на документи

За унищожаване на документите отговаря Мениджър по ИС. Унищожават се старите, неактуални версии на документи съгласно указанията на секция 5.1.6.
Контролираните хартиени копия на неактуални документи се унищожават сигурно чрез специализиран шредер в присъствие на Мениджър по ИС като за това той съставя Протокол за унищожаване на документ.

Неактуалните версии на документи съгласно указанията на секция 5.1.6 се унищожават от системен администратор, отговарящ за информационния актив, върху който са записани архивните папки с неактуални версии на документи, по разпореждане на Мениджър по ИС и под негово наблюдение. Мениджър по ИС съставя Протокол за унищожаване на документи (Образец 2).
В протокола за унищожаване на документи задължително се посочват:

- Наименование на унищожения документ;
- Версия;
- Дата на утвърждаване;
- Вид на носителя (хартиено или електронно копие);
- Собственик на копието;
- Дата и място на унищожаване;
- Имена, длъжност и подпис на лицето, извършило унищожаването;
- Подпис на Мениджър по ИС.

Мениджър по ИС води Регистър на унищожените документи (Образец 3), в който вписва всички унищожени документи (хартиени и електронни версии). В Регистъра задължително се вписват:

- наименование на унищожения документ;
- Версия;
- Дата на утвърждаване;
- Вид на носителя (хартиено или електронно копие);
- Собственик на копието;
- Номер и дата на протокола за унищожаване;
- Имена и длъжност на лицето, извършило унищожаването;
- Подпис на Мениджър по ИС.

5.1.8. Управление на външни документи

Управлението на външни документи, обект на нормативни актове, се осъществява по реда, указан в съответните нормативни актове.
Управлението на външни документи, попадащи в класификационни нива „1“ (С). „2“ (В) и „3“ (А) съгласно Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност, се осъществява по следния ред:
Идентификацията на документите се осъществява чрез тяхното съдържание. Мениджър по ИС включва документите в Регистър на външните документи по ИС и техните ползватели (Образец 4). Регистърът задължително съдържа: наименование на документите, версия, дата на утвърждаване, ниво на класификация, ползватели на документите (сътрудници с достъп до документа) с обозначен носител на използваното

копие (контролирано хартиено копие или електронно копие). Документите се маркират от Мениджър по ИС с грифа за съответното класификационно ниво. Разпространението и съхранението им е по реда за разпространение и съхранение на вътрешни документи. Изземването на документи се извършва от Мениджър по ИС по реда за изземване на неактуални копия на документи.
За документите от класификационно ниво „0“ (D) се използват общите правила и практики в ЦСОЧИ за управление на документи със свободен достъп.

5.2. Управление на записи

5.2.1. Записи, които подлежат на управление по настоящата процедура

На управление по настоящата процедура подлежат всички записи в обхвата на ЕУИЦСОЧИ и внедрената СУСИ, записани на хартия или в електронен вид.

5.2.2. Общи изисквания към създаването на записи

Основно предназначение на записите от обхвата на настоящата процедура е, че те са носители на информация, която служи за доказателство за съответствие с изискванията и ефективното прилагане на ЕУИЦСОЧИ и внедрената СУСИ. Записите се създават при пълно съблюдаване на приложимото законодателство, изискванията на ЕУИЦСОЧИ и внедрената в ЦСОЧИ СУСИ. Всички записи от обхвата на настоящата процедура трябва да са ясни, четливи, лесно идентифицируеми и лесни за откриване от съответните служители, имащи право на достъп до тях. Записите следва да са с попълнени всички предвидени реквизити.

5.2.3. Идентифициране на записи

Когато записът се съдържа в оперативен документ (утвърден образец), за идентификация на записа служат:

- Наименование на документа;
- Версия на документа;
- Дата на утвърждаване на документа;
- Имена и подпис на автора на записа;
- Дата на създаване на записа.

Във всички останали случаи за идентифицируемост на записа следва да има:

- Информация относно естеството му (например наименование);
- Обективно доказателство за времето на неговото създаване;
- Обективно доказателство за автора на записа.

5.2.4. Съхранение и защита на записите

Записите се съхраняват при условия, които осигуряват подходяща среда за осигуряване на тяхната цялостност, наличност и конфиденциалност (предпазване от повреждане, влошаване на качествата, загубване, предотвратяване съзнателното им манипулиране, издаване на тяхното съдържание и др.).
Мерките за съхранение и защита на записите се определят от Мениджър по ИС в съответствие с нивото има на класификация по **Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.** Мениджър по ИС води Регистър на записите по ИС и техните ползватели (Образец 5), който задължително съдържа:

- Вид запис;
- Автор на записа;
- Дата на създаване
- Начин на съхранение (хартиено или електронно копие);
- Ниво на класификация;
- Място на съхранение;
- Достъп до записа;
- Отговорник за съхранението;
- Срок на съхранение.

За записи с ниво на класификация „1“ (С). „2“ (В) и „3“ (А) съгласно **Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност,** съхранявани в електронен вид, задължително се извършва архивиране като копие от архива се съхранява и на отдалечено място, определено от Мениджър по ИС. Видът и графика за архивиране се определя от Мениджър по ИС и системния администратор, отговорен за съответния информационен архив.

5.2.5. Достъп до записи

Достъпът до записи се определя в зависимост от квалификационното ниво на записа и необходимостта от достъп до него на съответния служител. Правата за достъп до записи се поддържат от Мениджър по ИС в Регистър на записите по ИС и техните ползватели (виж секция 5.2.5).

5.2.6. Унищожаване на записи

Мениджър по ИС предприема мерки предприема за сигурно унищожаване на записи след изтичане срока им на съхранение. Доказателства за унищожаване на записи се съхраняват минимум 6 месеца след тяхното унищожаване.

6. СВЪРЗАНИ ДОКУМЕНТИ

- Политика на СУСИ;
- Процедури на СУСИ;
- Единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация;
- Наредба за общите изисквания за оперативна съвместимост и информационна сигурност.

7. ПРИЛОЖЕНИЯ

- Образец 1
- Образец 2
- Образец 3
- Образец 4
- Образец 5

ПРИЛОЖЕНИЕ 4. ПРОЦЕДУРА ЗА ОЦЕНКА НА МОМЕНТНОТО НИВО НА РИСКА ПРИ СЪХРАНЯВАНЕТО И ОПЕРИРАНЕТО С ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ И ОПРЕДЕЛЯНЕ НА ПРИОРИТЕТИТЕ И СПЕЦИФИЧНИТЕ МЕРКИ ЗА ПРЕВЕНЦИЯ.

1. ЦЕЛ

Настоящата методика има за цел да регламентира дейностите по управление на риска за сигурността на информацията в ЦСОЧИ както и да определи критерии за приемане и приемливи нива на риска за сигурността на информацията в ЦСОЧИ за постигане на съответствие с ЕУИЦСОИ.

2. ТЕРМИНИ И ОПРЕДЕЛЕНИЯ

- **Въздействие**

Неблагоприятна промяна в нивото на постигнатите цели, свързани с дейността на ЦСОЧИ.

- **Заплаха**

Възможността определен източник на заплаха да използва (преднамерено или непреднамерено) определена уязвимост.

- **Източник на заплаха**

Наличието на намерение и метод за преднамерено използване на определена уязвимост или наличието на обстоятелство и метод, които непреднамерено биха могли да използват дадена уязвимост.

- **Уязвимост**

Всеки процес, действие или състояние, предоставят възможност на определен източник на заплаха да прояви нежелано въздействие върху определен актив.

- **Риск за сигурността на информацията**

Възможността дадена заплаха да използва определена уязвимост и по този начин да причини вреда на организацията.

- **Идентифициране на риска**

Процес на откриване, описване и характеризиране на елементите на риска.

- **Преценяване на риска**

Процес на определяне на стойности на вероятността и последствията от риска.

- **Намаляване на риска**

Дейности, предприети за намаляване на вероятността, негативните последствия, или и двете, свързани с риска.

- **Приемане на риска**

Приемане на тежестта на загубите или извлечените ползи от даден риск.

- **Трансфер на риска**

Споделяне с друга страна на тежестта на загубите или извлечените ползи от даден риск.

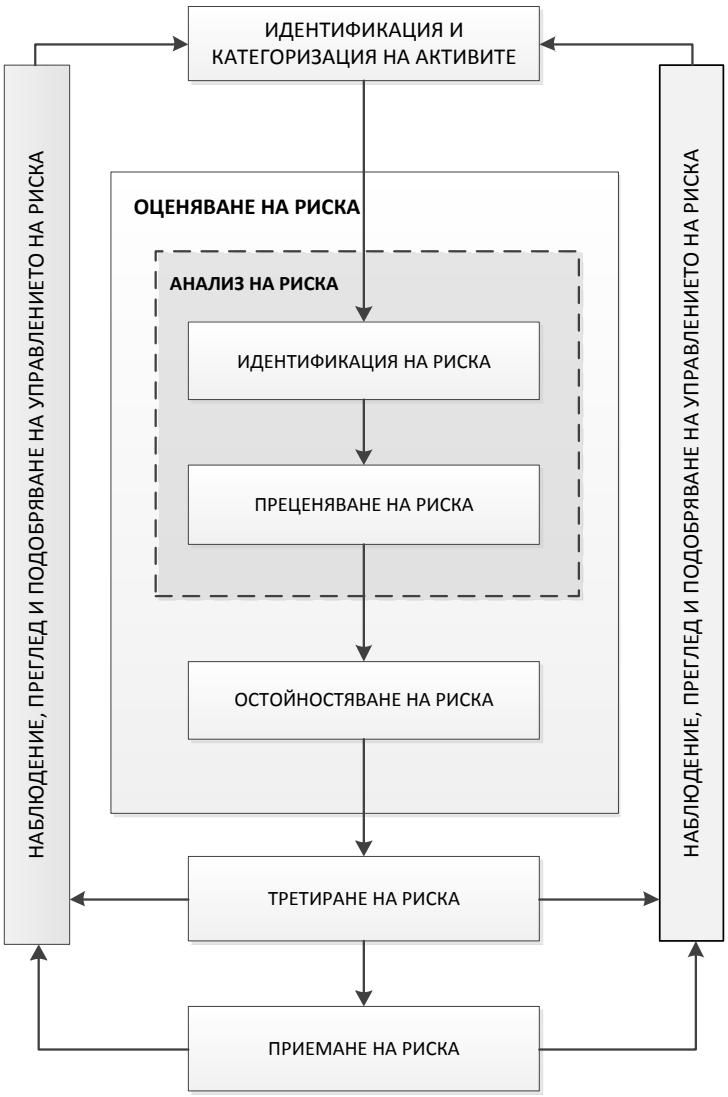
- **Избягване на риска**

Решение за неизпълнение или прекратяване на рисково действие.

3. ОПИСАНИЕ НА ДЕЙНОСТИТЕ

3.1. Процес на управление на риска.

3.1.1. Процесът на управление на риска в ЦСОЧИ се осъществява съгласно Схема на процеса по управление на риска (виж Фигура 1).



Фигура 1 - Схема на процеса по управление на риска

3.1.2. Дейностите по управление на риска се извършват от работна група, в състав определен със заповед на Ръководителя на Центъра за съхранение на особено чувствителна информация.

3.2. Идентификация и категоризация на активите

3.2.1. Определение за актив

- Всеки ресурс, контролиран или притежаван от ЦСОЧИ, съдържащ или отнасящ се до създаването, съхранението, предаването/приемането или обработването на информация.
- По смисъла на горното определение под актив следва да се разбира и всеки процес, който се осъществява чрез ресурси, определени като активи.

3.3. Идентифициране на активите

3.3.1. Активите се идентифицират съгласно ISO/IEC 27001, т. 4.2.1 d) 1)).

3.3.2. Активите се идентифицират поединично за всеки от определените в Приложение А типове и подтипове активи.

3.3.3. За идентифициране на активите на приемливо ниво на детайлност, за всеки един актив задължително се определят:

а) Наименование;

б) Тип и подтип;

в) Идентификатор (напр. инвентарен номер, персонален номер и т.н.);

г) Местоположение;

д) Категория (съобразно стойността на актива за ЦСОЧИ);

е) Класификация за сигурност;

ж) Изисквания за съответствие (съгласно приложимото законодателство и стандартите на ЦСОЧИ);

з) Собственик [1];

и) Допълнителна информация, съответстваща на типа/подтипа на актива.

3.3.4. Идентифициране на основните рискове.

[1]Терминът "собственик" означава физическо лице или обект, одобрено от Ръководителя на Центъа за съхранение на особеночувствителна информация да носи отговорността за контрол на производството, разработването, поддържането, използването и сигурността на активите. Терминът "собственик" не означава, че лицето има действителни права на собственост на актива

Идентифицирането на основните активи се извършва от съвместна работна група (ръководители на отдели, специалисти по информационни системи и потребители), определена със заповед на Ръководителя на Центъра за съхранение на особено чувствителна информация.

3.3.5. Идентифициране на поддържащите активи.
Идентифицирането на поддържащите активи се извършва чрез преглед на инвентаризационни описи и файлове с данни, съдържащи информация за ДМА/ДНМА, собственост на ЦСОЧИ, както и на всякаква друга свързана документация.

3.4. Регистриране на активите

3.4.1. Активите, идентифицирани по реда описан в т. 3.2 се вписват в Регистър на активите.

3.4.2. Регистъра на активите съдържа данни за идентифицираните активи, определени в т. 3.1.3.

3.4.3. Вписванията в регистъра на активите се извършва от Мениджър по ИС.

3.5. Оценяване на риска за сигурността на информацията

3.5.1. Идентифицирането на риска определя всички входни елементи от процеса на оценяване на риска за сигурността на информацията. Всички изходни данни, получени при идентифицирането на риска се вписват в План за третиране на риска (виж Приложение Б).

3.5.1.1. Идентифициране на заплахите.

а) Заплахите и техните източници се идентифицират съгласно ISO/IEC 27001, т. 4.2.1 d) 2).

б) Заплахите се идентифицират по произход и по тип в зависимост от типовете и подтиповете активи, върху които биха могли да въздействат и наличието на съответстващи на характера им уязвимости.

в) Идентифицирането на заплахите се извършва чрез анализ на свързана информация, получена от прегледи на инциденти, собственици на активи, потребители, специалисти по информационна сигурност, експерти по физическа сигурност, външни организации (застрахователни организации,

национални правителствени органи, правни органи, браншови камари и др.) и други източници, включително външни каталози на услуги.

3.5.1.2. Идентифициране на уязвимости.

а) Уязвимостите, които могат да се използват от заплахите се идентифицират съгласно ISO/IEC 27001, т. 4.2.1 d) 3).

б) Уязвимостите се идентифицират в съответствие със свойствата и характеристиките на обкръжаващата среда, типовете и подтиповете активи, с които се асоциират, както и със заплахите, които биха могли да ги използват.

в) Идентифицирането на заплахите се извършва чрез анализ на свързана информация, аналогично на т. 3.3.1.2 в), като за идентифициране на техническите уязвимости могат да се използват методи като:

- Автоматизирани средства за сканиране на уязвимости;
- Тестове и оценяване на сигурността;
- Тестове за проникване;
- Ревизия на софтуерен код.

3.5.2. Преценяване на риска.

3.5.2.1. Преценяване на въздействието върху идентифицирани активи.

а) Въздействието се преценява за всички активи идентифицирани съгласно ISO/IEC 27001, т. 4.2.1 d).

б) Въздействието върху идентифицирани основни активи се преценява на базата на критерий за максимално време на прекъсване (МДВП).

в) Въздействието върху основните активи се определя съгласно Матрица за определяне на въздействието върху основни активи (виж Приложение В).

г) Въздействието върху поддържащите активи се преценявана базата на критерий за оценяване на възможните последствия в резултат на загуба на поверителност, цялостност на данни, представляващи особено чувствителна информация.

д) Въздействието върху поддържащите активи се определя съгласно Матрица за определяне на въздействието върху поддържащи активи (виж Приложение В).

3.5.2.2. Преценяване на вероятността за реализиране на заплахи.

а) Вероятността за реализиране на дадена заплаха се преценява като се взема предвид колко често се реализира заплахата и колко лесно уязвимостта, съответстваща на разглеждания актив може да бъде използвана, отчитайки:

- Опита и приложимите статистики за вероятността за заплаха;

- За преднамерените източници на заплаха: мотивацията и капацитета, които се променят с времето и ресурсите, разполагаеми за възможните извършители, както и възприемането на атрактивността и уязвимостта на активите за възможния извършител;
- За случайните източници на заплаха: географски фактори, например близост на химически или петролни заводи, възможност за екстремни условия на времето и фактори, които могат да влияят на човешки грешки и на неизправност в съоръженията;
- Уязвимости - както отделни, така и с натрупване;
- Съществуващи механизми за контрол и доколко ефективно те намаляват уязвимостите.

б) Вероятността за реализиране на дадена заплаха се определя съгласно Матрица за определяне вероятността за реализиране на заплахи (виж Приложение В).

3.5.2.3. Преценяване нивото на въздействие на механизмите за контрол.

а) Въздействието на механизмите за контрол по отношение на идентифицираните рискове се преценява на базата на обобщени данни от проведени измервания и отчитайки техния тип.

б) Въздействието на механизмите за контрол се определя съгласно Матрица за определяне Въздействието на механизмите за контрол (виж Приложение В).

3.5.3. Остойностяване на риска.

а) Стойността на рисковете за всеки актив се определя разделно с/без отчитане на нивото на въздействие на механизмите за контрол като стойността на риска без отчитане на въздействието на механизмите за контрол се определя като Първична стойност на риска (**ПСР**), а при отчитане въздействието на механизмите за контрол – Остатъчна стойност на риска (**ОСР**).

б) Пълната стойност на риска за всеки актив се определя по формулата:

$$\text{ПСР} = (p + \text{s}) * v$$

където:

- ПСР е първична стойност на риска
- p е нивото на въздействие – основни активи
- s е ниво на въздействие – поддържащи активи
- v е вероятността за реализиране на дадена заплаха

б) Остатъчната стойност на риска за всеки актив се определя по формулата:

$$ОСР = ПСР - f$$

където:

- ПСР е първична стойността на риска
- ОСР остатъчна стойност на риска
- f е ниво на въздействие на механизмите за контрол

в) В случаите когато по отношение на основните активи въздейства повече от една заплаха, стойността на риска за основните активи се изчислява на базата на средно претеглена стойност отчитайки стойностите на всички елементи съставящи **ПСР** и **ОСР**

3.5.4. Определяне нивата на риска.

3.5.4.1. Нива на риска.

Нивата на риска се определят в разделно в съответствие със стойностите на ПСР **и** ОСР

а) При стойност на **ПСР** или **ОСР** <= 20 нивото на риска се определя като НИСКО (Н)

б) При стойност на **ПСР** или **ОСР** > 20 <= 50 нивото на риска се определя като СРЕДНО (С)

в) При стойност на **ПСР** или **ОСР** > 50 нивото на риска се определя като ВИСОКО (В)

3.5.5. Третиране на риска

3.5.5.1. Възможности за третиране на риска.

Възможностите за третиране на риска се определят съгласно ISO/IEC 27001, т. 4.2.1 f, като те могат да бъдат:

- Намаляване на риска;
- Избягване на риска;
- Трансфер на риска;
- Приемане на риска;

3.5.5.2. Възможностите за третиране на риска се избират на база резултата от оценяването на риска, очакваните разходи за внедряването им и очакваните ползи от тях.

3.5.5.3. Възможностите за третиране на риска се избират от Мениджър по ИС.
Същият определя и необходимите мерки за третиране на риска, които отразяват подходящите управленски действия, ресурси, отговорности и приоритети за управлението на рисковете, свързани със сигурността на информацията.

3.5.6. Възможностите за третиране на риска се записват в "План за третиране на риска".

3.5.6.1. Намаляване на риска.

а) Нивото на риска се намалява чрез избиране на механизми за контрол, така че остатъчният риск да може да бъде оценен като приемлив при повторно оценяване.

б) За намаляване на риска се избират подходящи и доказани механизми за контрол, като се вземат предвид критериите за приемане на риска (виж 4.3.4.4 б)), както и изискванията на нормативните актове и договорните изисквания и при отчитане размерът на разходите и необходимото време за внедряване на механизмите за контрол.

в) Механизмите за контрол се избират от Приложение А на ISO/IEC 27001 като по преценка е възможно да бъдат добавени и други контроли в съответствие с изискванията на ЕУИЦСОИ.

3.5.6.2. Намаляване на риска.

а) Когато идентифицираните рискове са отчетени като много големи или разходите за внедряване на други възможности за третиране на риска превишават ползите, ръководството на Ръководител ЦСОЧИ може да вземе решение за цялостно избягване на риска чрез изваждане на планирана или съществуваща дейност или набор от дейности или промяна на условията, при които се извършва дейността.

3.5.6.3. Трансфер на риска.

а) При наличие на достатъчно основания и в зависимост от остойностяването на риска, ръководството на ЦСОЧИ може да вземе решение, че рискът трябва да бъде прехвърлен към друга страна, която може много по-ефикасно да управлява конкретния риск.

3.5.6.4. Приемане на риска.

а) Когато нивото на риска отговаря на критериите за приемливост на риска (виж 4.3.4.4 б)), се приема, че не е необходимо внедряване на допълнителни механизми за контрол и рискът може да бъде поддържан.

б) За целите на настоящата процедура се определят следните критерии за приемане на риска:

- Ниво на риск “НИСКО”;
- Не се нарушават изискванията на законови и/или нормативни актове;
- Не се излага на опасност персонала;
- Не се излага на опасност околната среда;
- Не се застрашава осъществяването на основните дейности на ЦСОЧИ;
- Наличие на одобрение и задължение за предприемане на действие за намаляването на риска до приемливо ниво в рамките на определен срок.

в) За приемане на рискове отговарящи на критериите за приемливост се изготвя предложение от Мениджър ИС и се утвърждава от Ръководител ЦСОЧИ.

г) Решенията за приемане на рискове се отразяват в специален доклад или нарочна заповед, както и във Плана за третиране на риска.

3.5.7. Изготвяне на Декларация за приложимост.

3.5.7.1. След определяне на възможностите за третиране на риска Мениджър ИС разработва Декларация за приложимост (Приложение Г) представяща накратко решенията, касаещи въздействието върху риска.

3.5.7.2. Разработената декларация за приложимост трябва да включва следното:

- Целите по контрола и механизмите за контроли и причините за техния избор;
- Внедрените в момента цели по контрола и механизми за контрол и
- Изключването на някои от целите по контрола или някои от механизмите за контрол, описани в ISO/IEC 27001 Приложение А, и документирана обосновка за тяхното изключване.

3.6. Наблюдение, преглед и подобряване на управлението на риска.

3.6.1. Управление на риска.

Процесът за управление на риска за сигурността на информацията е обект на непрекъснато наблюдение, преглед и подобряване съгласно ISO/IEC 27001 т. 4.2.3).

3.6.2. Наблюдение и преглед.

Дейностите по наблюдение и преглед се отнасят (но не се ограничават до):
Новите активи, които трябва да бъдат включени в обхвата на управление на риска;

- Необходимите модификации на стойностите на активите, например по време на промени в изискванията, свързани с дейността на организацията;

- Новите заплахи, които могат да бъдат активни както извън, така и вътре в ЦСОЧИ и които не са били оценени;
- Възможността нови или нараснали уязвимости да позволят на заплахите да използват тези, нови или променени уязвимости;
- Идентифицираните уязвимости, за да се определят тези, които са изложени на нови или появяващи се отново заплахи;
- Нарасналото въздействие или последствия на оценените заплахи, уязвимости и риск с натрупване, които имат за резултат неприемливо ниво на риска;
- Инциденти със сигурността на информацията.
- Нормативна рамка и заобикаляща среда;
- Конкурентен контекст;
- Подход за оценяване на риска;
- Стойност на актива и категории;
- Критерии за въздействие;
- Критерии за остойностяване на риска;
- Критерии за приемане на риска;
- Общи разходи за притежаване;
- Необходими ресурси.

3.6.3. Процесът за управление на риска за сигурността на информацията се преглежда регулярно (но не по-малко от веднъж годишно) от Мениджър ИС.

3.6.4. Констатациите от прегледа се отразяват в доклад, като същия се представя на Ръководител ЦСОЧИ за сведение.

ПРИЛОЖЕНИЯ:

ПРИЛОЖЕНИЕ А. ТИПОВЕ И ПОДТИПОВЕ АКТИВИ
ПРИЛОЖЕНИЕ Б. ПЛАН ЗА ТРЕТИРАНЕ НА РИСКА
ПРИЛОЖЕНИЕ В. МАТРИЦА ЗА ОПРЕДЕЛЯНЕ НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОСНОВНИ АКТИВИ
ПРИЛОЖЕНИЕ Г. ДЕКЛАРАЦИЯ ЗА ПРИЛОЖИМОСТ

ТИПОВЕ И ПОДТИПОВЕ АКТИВИ

ОСНОВНИ АКТИВИ (ОСНОВНИ ПРОЦЕСИ И ДЕЙНОСТИ)	
ПЪРВИЧНИ ПРОЦЕСИ (дейности отнасящи се до осъществяването на основната дейност на ЦСОЧИ)	**ВТОРИЧНИ ПРОЦЕСИ** (отнасящи се до осъществяването на административни задачи, управление на инфраструктура, поддръжка, снабдяване и т.н.)

ПОДДЪРЖАЩИ АКТИВИ (ПОДДЪРЖАЩИ ОПРЕДЕЛЕНИТЕ КАТО ОСНОВНИ АКТИВИ)					
ФИЗИЧЕСКИ АКТИВИ	**СОФТУЕРНИ АКТИВИ**	**УСЛУГИ**	**ЧОВЕШКИ РЕСУРСИ**	**ИНФОРМАЦИОННИ АКТИВИ**	**ПЛОЩАДКИ**
Настолни компютърни системи	Сървърни операционни системи	Комунални услуги	Ръководство	Лични данни	Сгради
Сървърни системи	Потребителски операционни системи	Услуги за поддържа	Мениджмънт	Договори и споразумения	Помещения
Преносими компютърни системи	Мобилни операционни системи	Услуги за достъп до Интернет	Оперативен персонал	Финансово-счетоводна информация	Зони
Мобилни компютърни устройства (смартфони, PDA и т.н.)	Софтуер за обслужване, поддръжка и администриране	Мобилни комуникационни услуги	Специализиран персонал	Регламенти (в т.ч. политики, правилници, процедури и инструкции)	
Обработващи периферни устройства (принтери, факсове, копирни устройства)	Софтуер за предоставяне на услуги	Фиксирани комуникационни услуги		Записи	

ФИЗИЧЕСКИ АКТИВИ	СОФТУЕРНИ АКТИВИ	УСЛУГИ	ЧОВЕШКИ РЕСУРСИ	ИНФОРМАЦИОННИ АКТИВИ	ПЛОЩАДКИ
Електронни носители (Ленти - DDS, LTO; Оптични дискове - DVD, CD; Флаш памети; Външни HDD)	Стандартен/пакетен софтуер	Други експертни услуги		Планове за непрекъснатост	
Архивиращи устройства	Софтуер за управление на бази данни			Оперативни анализи (в т.ч. анализ на риска)	
Системи за съхранение на данни	Защитен софтуер			Ръководства и наръчници	
Телефонни устройства (стационарни, мобилни)	Криптографски инструменти			Справки и отчети	
Маршрутизатори	Стандартни бизнес приложения			Системна документация	
Мрежови концентратори	Специфични бизнес приложения			Учебни материали	
Комутатори					
Комуникационно окабеляване					
Устройства за охлаждане и пречистване на въздуха					

ФИЗИЧЕСКИ АКТИВИ	СОФТУЕРНИ АКТИВИ	УСЛУГИ	ЧОВЕШКИ РЕСУРСИ	ИНФОРМАЦИОННИ АКТИВИ	ПЛОЩАДКИ
Вътрешни електрически инсталации					
Сигнално-охранителни системи					
Системи за видеонаблюдение					
Непрекъсваеми захранващи системи					
Противопожарни системи					
Пожарогасители					
Системи за контрол на достъпа					

ПРИЛОЖЕНИЕ Б. ПЛАН ЗА ТРЕТИРАНЕ НА РИСКА

ОСНОВЕН АКТИВ	ПОДДЪРЖАЩ АКТИВ	ЗАПЛАХИ	УЯЗВИМОСТИ	НИВО НА ВЪЗДЕЙСТВИЕ	ВЕРОЯТНОСТ	ПСР	ЕФЕКТИВНОСТ НА МЕХАНИЗМИТЕ ЗА КОНТРОЛ	ОСР	НИВО НА РИСКА	ПРИЕМЛИВО ДА/НЕ	РЕШЕНИЕ ЗА ВЪЗДЕЙСТВИЕ ВЪРХУ РИСКА	ИЗБОР НА МЕХАНИЗМИ ЗА КОНТРОЛ	ДАТА НА ПРИЛАГАНЕ НА МЕХАНИЗЪМ ЗА КОНТРОЛ	ОТГОВОРНИК ЗА ПРИЛАГАНЕ НА МЕХАНИЗМИ ЗА КОНТРОЛ

Стр. 50 от 95

Матрица за определяне на въздействието върху основни активи

МДВП	Ниво на въздействие
<= 1 минута	**5**
>1 минута <=3 минути	**4**
>3 минути <=5 минути	**3**
>5 минути <=7 минути	**2**
> 7 минути <=10 минути	**1**

Матрица за определяне на въздействието върху поддържащите активи

Наличност	Стойност
Незначително прекъсване на достъпа до особено чувствителна информация	**1**
Достъпа до особено чувствителна информация е затруднен	**2**
Загуба на особено чувствителна информация, която може да бъде възстановена. Достъпа до особено чувствителна информация е неосъществим за ограничен период	**3**
Значителна загуба на особено чувствителна информация и/или трайно ограничаване на възможността за работа с особено чувствителна информация	**4**
Необратима загуба на особено чувствителна информация	**5**

Поверителност / Цялост	Стойност
Нарушение на принципа за "необходимост да се знае" при работа с особено чувствителна информация	**1**
Неразрешено разглеждане на данни, съставляващи особено чувствителна информация. Непредвидени (случайни) изменения на данни съставляващи особено чувствителна информация	**2**
Неразрешен външен достъп и/или неправомерно изменяне на данни, съставляващи особено чувствителна информация	**3**
Неправомерна обработка и/или необратимо изменяне на данни, от съставляващи особено чувствителна информация	**4**
Неконтролируемо разгласяване/увреждане целостта на особено чувствителна информация	**5**

Матрица за определяне вероятността за реализиране на заплахи

Вероятност	Стойност
Всеки ден	**10**
Веднъж седмично	**9**
Веднъж на всеки 2 седмици	**8**
Веднъж месечно	**7**
Веднъж на всеки три месеца	**6**
Веднъж на всеки шест месеца	**5**
Веднъж годишно	**4**
Веднъж на всеки 3 години	**3**
Веднъж на всеки 5 години	**2**
Над 10 години	**1**

Матрица за определяне въздействието на механизмите за контрол

Коефициент на въздействие (КВ)	Стойност
Тип контрол	
Указателни механизми за контрол	**1**
Коригиращи механизми за контрол	**2**
Откриващи механизми за контрол	**3**
Възстановяващи механизми за контрол	**4**
Превантивни механизми за контрол	**5**

Коефициент на съответствие (КС)		Стойност	
За Механизми	**За Процеси/Дейности**	**ДА**	**НЕ**
Механизмът е внедрен и функционира	Процесът/дейността се изпълнява	**1**	-1
Внедреният механизъм функционира без очевидни отклонения от изискванията	Процесът/дейността се изпълнява без очевидни несъответствия с изискванията	**1**	-1
Функциите на внедрения контрол се наблюдават и следят за отклонения от изискванията	Изпълнението на процесът/дейността се наблюдава и следи за отклонения от изискванията	**1**	-1
Всички отклонения от функционалните изисквания се идентифицират и описват	Всички отклонения от изисквания за процеса/дейността се идентифицират и описват	**1**	-1
Всички идентифицирани отклонения от функционалните изисквания се	Всички идентифицирани отклонения от изисквания процеса/дейността се	**1**	-1

коригират и се прилагат превантивни мерки с цел недопускане повторната им поява	коригират и се прилагат превантивни мерки с цел недопускане повторната им поява		
	Коефициент на съответствие (КС)	**(1-5)+(-1- 5)**	

Стойност на въздействие на контрола (СВК) = КВ*КС

ПРИЛОЖЕНИЕ Г: ДЕКЛАРАЦИЯ ЗА ПРИЛОЖИМОСТ
(Приложение Г в xsl. Файл)

ПРИЛОЖЕНИЕ 5. ПРОЦЕДУРА ЗА ТЕХНИЧЕСКО И ОРГАНИЗАЦИОННО ПРОЕКТИРАНЕ НА СПЕЦИФИЧНАТА СИСТЕМА ОТ МЕРКИ ЗА ПОСТИГАНЕ И ПОДДЪРЖАНЕ НА УСТОЙЧИВА СЪВМЕСТИМОСТ СЪС СИСТЕМАТА ОТ ЕДИННИ ДЪРЖАВНИ ИЗИСКВАНИЯ

1. ЦЕЛ

Тази процедура определя реда и начините за проектиране на специфичната система от мерки за постигане на поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща всички дейности по проектиране на специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ.

3. ОТГОВОРНОСТИ

Ръководителят на Център за съхранение на особено чувствителна информация:

- Отговаря за цялостното прилагане на настоящата процедура.

Отговорник сигурност на информацията на ЦСОЧИ (ИТСОЦСОЧИ):

- Отговаря за цялостния процес на проектиране на специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ.

4. ОПИСАНИЕ НА ПРОЦЕДУРАТА

4.1. Създаване на организация за изпълнение и прилагане на ЕУИЦСОЧИ.

4.1.1. За изпълнение на дейностите по проектиране и прилагане на специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ се определя специализирана комисия.

4.1.2. Съставът на комисията се определя от Ръководителя на Център за съхранение на особено чувствителна информация.

4.1.3. При формирането на състава се спазва принципът на пропорционалното представителство на организационните структури в ЦСОЧИ.

4.1.4. Комисията се председателства от Отговорник сигурност на информацията на ЦСОЧИ (ИТСОЦСОЧИ).

4.1.5. Комисията обсъжда, определя и предлага за одобрение на Ръководителя на Центъра за съхранение на особено чувствителна информация всички специфични мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ.
4.1.6. Заседанията на комисията се провеждат по предварително определен дневен ред, като всички нейни обсъждания се документират, заедно с решенията и мотивите за тях.

4.2. Проектиране на специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ.

4.2.1. Специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ се определя на базата на извършена оценка на риска в съответствие с Процедурата за оценка на моментното ниво на риска при съхраняването и оперирането с чувствителна информация и определяне на приоритетите и специфичните мерки за превенция.
4.2.2. Системата от специфични мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ се проектира в съответствие с Приложение Д към настоящата процедура.
4.2.3. За реализирането на техническите и организационни мерки за постигане на поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ се изготвя проект по образец в съответствие с Шаблон за разработване на проект реализирането на техническите и организационни мерки за постигане на поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ.

5. СВЪРЗАНИ ДОКУМЕНТИ

- Процедура за оценка на моментното ниво на риска при съхраняването и оперирането с чувствителна информация и определяне на приоритетите и специфичните мерки за превенция;
- ISO/IEC 27001:2005;
- BDS ISO/IEC 27001:2006;
- Наредба за оперативна съвместимост и информационна сигурност.

6. ПРИЛОЖЕНИЯ

- Приложение Д: Референтен списък на ЕУИЦСОЧИ

ПРИЛОЖЕНИЕ Д. РЕФЕРЕНТЕН СПИСЪК НА ЕУИЦСОЧИ
(Приложение Д в xsl. Файл)

ПРИЛОЖЕНИЕ 6: ШАБЛОН ЗА РАЗРАБОТВАНЕ НА ПРОЕКТ ЗА РЕАЛИЗИРАНЕ НА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ПОСТИГАНЕ И ПОДДЪРЖАНЕ НА УСТОЙЧИВА СЪВМЕСТИМОСТ СЪС СИСТЕМАТА ЗА ЕДИННИ ДЪРЖАВНИ ИЗИСКВАНИЯ

1. Обхват на проекта

[…]

2. Свързани документи

[…]
[…]

3. Описание на проекта

3.1. Цел на проекта

3.2. Очаквани резултати

[…]
[…]

3.3. Основни задачи

Описание на задачата	Срок за изпълнение

Крайна дата за реализиране на проекта [дата].

3.4. Организация на проекта

3.4.1. Координатор на проекта

3.4.2. Ръководител на проекта

3.4.3. Проектен екип

3.4.4. Консултант

Списък на участниците в проекта

Име	Организационна единица	Длъжност	Телефон	E-mail

3.5. Основни рискове за проекта

№	Рискове	Действия за намаляване на рисковете
1		
2		
3		

3.6. Избор на доставчици

3.7. Финансова обосновка

3.8. Подробен план за изпълнение на проекта

№	ЗАДАЧА	ПРОДЪЛЖИТЕЛНОСТ	НАЧАЛО	КРАЙ	ОТГОВОРНИК

ПРИЛОЖЕНИЕ 7. ПРОЦЕДУРА ЗА МОНИТОРИНГ НА ИНДИКАТОРИТЕ ЗА ИЗПЪЛНЕНИЕ И ОСИГУРЯВАНЕ НА УСТОЙЧИВО ВЪВ ВРЕМЕТО СЪОТВЕТСТВИЕ С ЕДИННИТЕ ДЪРЖАВНИ ИЗИСКВАНИЯ И ИЗИСКВАНИЯТА НА БДС ISO/IEC 27001:2006.

1. ЦЕЛ

Тази процедура определя реда и начините за осъществяване на мониторинг на индикаторите за изпълнение и осигуряване на устойчиво във времето съответствие с Единните държавни изисквания и изискванията на БДС ISO/IEC 27001:2006.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ и БДС ISO/IEC 27001:2006 към конкретния ЦСОЧИ.

3. ОТГОВОРНОСТИ

Ръководителят на Център за съхранение на особено чувствителна информация:

- Отговаря за цялостното прилагане на настоящата процедура.

Отговорник сигурност на информацията на ЦСОЧИ (ИТСОЦСОЧИ)

- Отговаря за цялостния процес на проектиране и прилагане на методите за осъществяване на мониторинг на индикаторите за изпълнение на съответствие с ЕУИЦСОЧИ

4. ОПИСАНИЕ НА ПРОЦЕДУРАТА

4.1 Определяне на метод за мониторинг на индикаторите за изпълнение на изискванията на ЕУИЦСОЧИ и БДС ISO/IEC 27001:2006

4.1.1. Индикаторите за съответствие се определят на базата на релевантните за обекта на приложение критерии за прилагане на ЕУИЦСОЧИ и избраните цели на контрола и механизмите за контрол в съответствие с изискванията на БДС ISO/IEC 27001:2006.

4.1.2. Индикаторите за съответствие се мониторират, преглеждат и анализират на базата на формален модел за измерване ефективността на релевантните за обекта на приложение ЕУИЦСОЧИ и внедрените в съответствие с изискванията на БДС ISO/IEC 27001:2006 механизми за контрол.

4.1.3. Моделът за измерване се прилага индивидуално за всеки от критериите за ЕУИЦСОЧИ, както и за единични или групи от механизми за контрол.

4.1.4. Структурата на модела за измерване се разработва от Отговорника по сигурност на информацията на ЦСОЧИ.

4.1.5. Структурата на модела за измерване задължително трябва да включва данни за:

- Идентификацията на структурата за измерване;
- Целта на измерването;
- Обекта на измерването;
- Цел на механизма за контрол;
- Индикатор;
- Формула/Критерии за измерване;
- Аналитичен модел за оценка нивото на ефективност;
- Честотата на измерването;
- Лицето, извършващо измерването;
- Източника на данни за измерването.

4.1.4. Структурата на модела за измерване се изготвя по образец в съответствие с Приложение Е от настоящата процедура.

4.2 Осъществяване на мониторинг на индикаторите за изпълнение на изискванията на ЕУИЦСОЧИ и БДС ISO/IEC 27001:2006.

4.2.1 Мониторингът на индикаторите за изпълнение на изискванията се осъществява чрез използване на технически средства или чрез други методи за събирането на обективна информация за нивото на съответствие като:

- Оценка и анализ на риска;
- Попълване на въпросници или интервюиране на заинтересовани лица;
- Провеждане на вътрешни/външни одити;
- Анализ за инциденти в сигурността;
- Анализ на резултати от проведени тестове;
- Преглед на записи, свързани с прилагането на процедури.

4.3. Анализ на резултатите от мониторинга на индикаторите за изпълнение на изискванията на ЕУИЦСОЧИ и БДС ISO/IEC 27001:2006

4.3.1. Резултатите от мониторинга на индикаторите за изпълнение на изискванията на ЕУИЦСОЧИ и БДС ISO/IEC 27001:2006 се преглеждат и анализират на планирани интервали в съответствие с определения референтен модел на изследване.

4.3.2. Анализът на резултатите от мониторинга на индикаторите за изпълнение се изготвя от Отговорника по сигурността на информацията на ЦСОЧИ и се представя във вид на доклад на ръководителя на Център за съхранение на особено чувствителна информация за сведение и разпореждане.

5. СВЪРЗАНИ ДОКУМЕНТИ

- ISO/IEC 27001:2005;
- BDS ISO/IEC 27001:2006;
- Наредба за оперативна съвместимост и информационна сигурност.

6. ПРИЛОЖЕНИЯ

- Приложение Е: Структура на модел за измерване на ефективността на релевантните за обекта на приложение ЕУИЦСОЧИ и внедрените в съответствие с изискванията на БДС ISO/IEC 27001:2006 механизми за контрол.

ЕЛЕМЕНТ	ОПИСАНИЕ
Идентификация	
Цел на измерването	
Обект на измерването	
Цел на механизма за контрол	
Индикатор	
Формула/Критерии за измерване	
Аналитичен модел за оценка нивото на ефективност	
Честотата на измерването	
Изпълнител	
Източник на данни за изследването	
Резултат от измерването	

ПРИЛОЖЕНИЕ 8. ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ПРОМЕНИТЕ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИТЕ ПРИ ПОДДЪРЖАНЕ НА УСТОЙЧИВА СЪВМЕСТИМОСТ СЪС СИСТЕМАТА ОТ ЕДИННИ ДЪРЖАВНИ ИЗИСКВАНИЯ

1. ЦЕЛ

Процедурата за управление на промените определя действията за идентифициране на необходимостта, оценка, одобряване, внедряване и преглед на промените при поддържане на устойчива съвместимост с Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, стандарта BDS ISO/IEC 27001:2006 и документите на внедрената СУСИ.

Процедурата за управление на инциденти определя реда за действие при идентифициране на инциденти по отношение сигурността на информацията и за докладване за пробиви и слабости в сигурността на информацията с оглед поддържане на устойчива съвместимост с Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, стандарта BDS ISO/IEC 27001:2006 и документите на внедрената СУСИ.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурите обхващат всички дейности по управление на промени и инциденти при поддържане на устойчива съвместимост с изискванията на Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, стандарта BDS ISO/IEC 27001:2006 и документите на внедрената СУСИ.

3. ОТГОВОРНОСТИ

Ръководителят на Център за съхранение на особено чувствителна информация:

- Участва и председателства Съвет по промените при разглеждане на заявки за промяна с приоритет „съществена“;
- Одобрява назначението на ръководител проект;
- Одобрява решенията за внедряване на промяна;

Мениджър по ИС:

- Отговаря за цялостното управление на процеса за управление на промените;
- Отговаря за установяване на рисковия потенциал на докладвания инкубиран инцидент/слабост/пробив по отношение сигурността на информацията;
- Съгласува предприемането на неотложни мерки при инциденти/слабости/пробиви по отношение на сигурността на информацията;

- Отговаря за събиране на доказателства, разследване и анализ при инциденти/слабости/пробиви по отношение на сигурността на информацията заедно с Мениджър по управление на инциденти;
- Сътрудничи на Мениджър по управление на инциденти през целия процес на управление на инциденти/слабости, пробиви по отношение на сигурността на информацията

Системен аналитик:

- Наблюдава данните от мониторинга на параметрите, извършван от системата за мониторинг и ранно предупреждение и прогнозира или открива тенденции в повишаване на рисковия потенциал на един или повече основни или спомагателни елементи от инфраструктура на ЦСОЧИ, изготвя доклади;
- Докладва писмено на Мениджър по ИС при идентифициране на потенциални инциденти/слабости/пробиви;
- изготвя доклади за оценка на потенциалните рискове по искане на Мениджър по ИС.

Съвет по промените – прави оценка на заявките за промяна с приоритет „съществена“ и „нормална“ и на предложените решения за реализиране на промяната.

Спешен съвет по промените – прави оценка на заявките за промяна с приоритет „спешна“.

Ръководител проект – отговаря за успешното проектиране, тестване и реализиране на възложеното му решение за промяна.

Център за обслужване на ЦСОЧИ – функция на системата за управление на ЦСОЧИ, която предоставя единична точка за контакт на всички заинтересовани страни по отношение на ЕУИЦСОЧИ и управлява техните заявки за промяна и доклади за инцидент/слабост/пробив през целия им цикъл до закриването им.

Мениджър по управление на инциденти – отговаря за общото управление на инциденти/слабости/пробиви съгласно настоящата процедура.

Ролите и отговорностите по отношение стъпките на процедурата са посочени в RACI (Изпълняващ/Отговарящ/Консултиращ/Информиран) матрица в Таблица 1 по-долу:

Таблица 1

Роля: / **Стъпка:**	**Ръководител ЦСОЧИ**	**Мениджър по ИС**	**Системен аналитик**	**Съвет по промените**	**Ръководител проект**	**Център за обслужване на ЦСОЧИ**	**Мениджър управление на инцидентин**

Иницииране на промяна			R/A Служител Клиент Трета страна			I	
Оценка на заявката за промяна Етап 1			I	I		R/A	
Оценка на заявката за промяна Етап 2		R/A	I	R/A		I	
Възлагане изпълнението на промяна	A	R	I		I	I	
Разработка на решението за промяната		I			R/A	I	
Тестване на решението за промяна		R/A		I	R	I	
Оценка на решението за промяна		R/A		R/A	I	I	
Възлагане на внедряването	A	R			I	I	
Внедряване на промяната		C			R/A	I	
Преглед на промяната		R/A		R/A	I	I	
Приключване на промяната		R/A			I	I	
Установяване и докладване на възникнал инцидент по			R/A Служител			I	

отношение на сигурността на информацията							
Установяване и докладване на инкубиран инцидент, слабост (потенциал за инцидент), пробив в резултат на мониторинг		I	R/A				
Установяване на рисковия потенциал на инкубиран инцидент, слабост (потенциал за инцидент), пробив в резултат на мониторинг		R/A	C			I	
Приоритизиране на инцидента/пробива/слабостта		C				I	R/A
Регистриране на инцидента		R/A					
Предприемане на неотложни мерки		C				I	R/A
Събиране на доказателства, разследване и анализ		R				I	R/A

Предприемане на мерки за преодоляване на инцидента/пробива/слабостта (иницииране на процес на промяна)		R/A				I	R
Извличане на поуки от инцидента/слабостта/пробива, реализиране на последващи промени (подобрение) и обучение. Затваряне на инцидента	I	R				I	R/A

R= Изпълняващ A= Отговарящ C= Консултиращ I= Информиран

4. ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

Система за управление – рамка от политики, процедури, указания и свързаните с тях ресурси за постигане на целите на организацията.

Информационна сигурност (ИС) – опазване на поверителността, интегритета и наличността на информацията.

Система за управление на сигурността на информацията (СУСИ) – част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията.

Събитие, свързано със сигурността на информацията – идентифицирана поява на състояние в система, услуга или мрежа. Показваща възможно нарушаване на политиката по сигурност на информацията, пробив на защити или неизвестна до момента ситуация, засягаща сигурността.

Инцидент по отношение сигурността на информацията – отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията,

които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията.

Управление на инцидент по отношение сигурността на информацията – процеси за откриване, докладване, оценяване, реагиране, обработване и проучване от инциденти по отношение сигурността на информацията.

Заявка за промяна – формуляр или екран, използвани за записване на детайли от искане за промяна.

Библиотека Известни грешки – библиотека, съдържаща доклади за преодолени инциденти/ слабости/пробиви.

ЦСОЧИ – център за съхранение на особено чувствителна информация.

ЕУИЦСОЧИ – единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация.

5. ОПИСАНИЕ НА ПРОЦЕДУРИТЕ

5.1. Управление на промените

5.1.1. Управление на промени в обхвата на внедрената СУСИ

Управлението на промени в обхвата на внедрената СУСИ се извършва по реда на Процедура за разработване и прилагане на коригиращи и превантивни действия при установяване на несъответствие със специфичния обхват и индикаторите за изпълнение на единните държавни изисквания за обекта на приложение.

5.1.2. Управление на промени в обхвата на ЕУИЦСОЧИ

5.1.2.1. Иницииране на промяна

Основен инициатор на искането за промени е Системен аналитик, който наблюдава данните от мониторинга на параметрите, извършван от системата за мониторинг и ранно предупреждение и прогнозира или открива тенденции в повишаване на рисковия потенциал на един или повече основни или спомагателни елементи от инфраструктура на ЦСОЧИ.

Инициатор на искането за промяна може да бъде и всеки компетентен сътрудник на ЦСОЧИ, доставчик, клиент на услуги или друга заинтересована страна.

Инициаторът на промяната регистрира запис Заявка за промяна (Образец 1) към Център за обслужване на ЦСОЧИ като задължително попълва следната информация:

- Кратко описание на исканата промяна;
- Приоритет на промяната (съществена, нормална, спешна);
- Имена на инициатора на промяната;Организация/отдел/местоположение на инициатора на промяната;
- Данни за контакт (телефон, е-мейл);

- Обхват на исканата промяна (детайлно описание);
- Услуги, които ще бъдат засегнати;
- Активи, които ще бъдат засегнати;
- Причина за исканата промяна;
- Ползи от исканата промяна (технически и финансови);
- Дата и час на регистриране на Заявката.
- Статус на промяната

Прилага се техническа документация по предлаганата промяна, ако такава е налична.

5.1.2.2. Оценка на заявката за промяна

Оценката на искането за промяна се извършва на два етапа. Първоначално център за обслужване прави преглед на Заявка за промяна за пълнота и коректност на данните. При коректно попълване на необходимата информация Заявката за промяна получава статус „записано“. При некоректно попълване Заявката се връща на инициатора, като центърът за обслужване се свързва с него и изисква възможно най-бърза корекция и повторна регистрация.

Искането със статус „записано” се насочва за оценка към Съвет по промените (за промени с приоритет „съществена“ и „нормална“) или Спешен съвет по промените (за промени с приоритет „спешна“).

Съвет по промените се състои минимум от:

- Мениджър по ИС;
- Ръководител ИТ поддръжка;
- Ръководител поддръжка инфраструктура;
- Главен системен администратор.

При необходимост се включват и други членове на организацията или заинтересовани страни. Председател на Съвета по промените е Мениджър по ИС, който свиква Съвета. Съвет по промените се свиква не по-късно от 10 работни дни след подаване на Заявка за промяна с приоритет „нормална“ от страна на Центъра за обслужване. Изисква се присъствието на членовете на Съвета (физическо или видео-връзка) и се води протокол.

При разглеждане на „съществени“ промени в Съвета участва Ръководител на ЦСОЧИ, който изпълнява функциите на негов председател. Съвет по промените при подадена Заявка за „съществени“ промени се свиква не по-късно от 5 работни след подаването й от Центъра за обслужване.

Спешен съвет по промените се състои от същите членове както при Съвет по промените, организира се от Мениджър по ИС, но за провеждането му членовете не

присъстват физически, а заседанията се водят по възможните канали за комуникация (телефон, е-мейл, видео-връзка или др.). Мениджър по ИС има отговорността за отразяване на взетите решения в протокол.

Заявката за промяна се оценява въз основа на информацията в Заявката за промяна, данни от мониторинг системите и доклади на системния аналитик на база потенциалното въздействие върху организацията и услугите. Оценката е базирана на приетия подход за оценка на риска. При вземане на решение се взема предвид баланса между потенциалните ползи и рисковия потенциал на предлаганата промяна. Използват се услугите на компетентни сътрудници, като им се възлагат задачи по подготовка на експертни становища, анализи и други дейности, необходими за вземане на решение.

При положително решение относно предлаганата промяна се преминава към възлагане изпълнението на промяната със статус „одобрено“.
При отрицателно становище относно промяната се уведомява инициатора на промяната и Заявката за промяна се затваря със статус „отхвърлено“.
При липса на достатъчно информация за вземане на решение се връща Заявката за промяна към нейния инициатор за допълнително уточняване.

5.1.3. Възлагане изпълнението на промяна

При положително решение относно предлаганата промяна Мениджър по ИС определя Ръководител на проекта и след одобрение от Ръководител на ЦСОЧИ извършва възлагане подготовката на решение за изпълнението на промяната. Заявката за промяна получава статус „възложено“.

5.1.4. Разработка на решението за промяната

Ръководител проект организира и управлява процеса на планиране и разработване на решението за промяна като вътрешен проект или чрез сключване на договор с външна страна съгласно правилата за работа на ЦСОЧИ. При разработка на решението за промяна се спазват всички изисквания на ЕУИЦСОЧИ и внедрената СУСИ.
По време на целия процес на разработка на решението ръководител проект информира Мениджър по ИС за статуса на проекта и възможни проблеми.
След приключване на разработката Мениджър по ИС проверява състоянието на проекта и при положително оценка сменя статуса на Заявката за промяна на „разработено“.

5.1.5. Тестване на решението за промяна

След смяната на статуса на заявката на „разработено“ Мениджър по ИС със съдействието на Ръководител проект организира тестване на разработеното решение за

промяна. Тестването на разработеното решение се извършва след подготовка на план за тестване и критерии за оценка на резултатите. Планът за тестване трябва да гарантира предпазване на системата от възможни нежелани въздействия, резултат от тестването. По възможност се осигурява изолирана среда за тестване или тестването се планира така, че да се минимизират възможните нежелани въздействия върху системата. Резултатите от тестването се записват в протокол от тестване.

5.1.6. Оценка на решението за промяна

Оценката на решението за промяна се извършва от Съвета по промените на база постигнатите резултати от тестване, отразени в протокола от тестване. Решенията на Съвета се записват в протокол. При положително становище на Съвета Мениджър по ИС сменя статуса на промяната на „за внедряване“ и възлага на Ръководител проект внедряване на решението след одобрение от Ръководител на ЦСОЧИ.

5.1.7. Внедряване на промяната

Ръководител проект разработва план за внедряване на промяната като отчита и минимизира възможните нежелани въздействия върху системата, както и План за възстановяване от промяна в случай на нежелани събития. След одобрение от Мениджър по ИС организира внедряване на промяната като вътрешен проект или чрез сключване на договор с външна страна съгласно правилата за работа на ЦСОЧИ. Внедряването на промяната приключва с протокол от тестване в работна среда в присъствие на Мениджър по ИС. При положителен резултат Мениджър по ИС сменя статуса на промяната на „внедрена“.

5.1.8. Преглед на промяната

Минимум 30 дни след внедряване на промяната Мениджър по ИС свиква Съвет по промените, на който се извършва преглед на извършената промяна. При липса на регистрирани инциденти, пробиви или слабости, свързани с направената промяна се взема решение за приключване на промяната. При регистрирани инциденти, пробиви или слабости, свързани с направената промяна, се задейства Процедура за управление на инциденти или при необходимост Плана за възстановяване от промяна. Решенията на Съвета се отразяват в протокол.

5.1.9. Приключване на промяната

При взето решение за приключване на промяната от страна на Съвета за промени Мениджър по ИС сменя статуса на промяната на „приключен“.

5.2. Управление на инциденти по отношение сигурността на информацията, пробиви и слабости в сигурността на информацията

5.2.1. Установяване и докладване на инциденти/пробиви/слабости

Процедурата предвижда два сценария за установяване и докладване на инциденти/пробиви/ слабости по отношение сигурността на информацията:

- Установяване пост фактум на възникнал инцидент по отношение сигурността на информацията;
- Установена слабост (потенциал за инцидент), инкубиран инцидент, пробив в сигурността на информацията в резултат на мониторинг.

5.2.1.1. Установяване и докладване на възникнал инцидент по отношение на сигурността на информацията

Всеки сътрудник на ЦСОЧИ може да установи възникване на инцидент по отношение на сигурността на информацията в процеса на ежедневната си работа. Инцидентите със сигурността на информацията могат да имат много разнороден характер – организационен, технологичен, субективен и др. С цел разпознаване и установяване на възникнали инциденти всички сътрудници на ЦСОЧИ преминават встъпително обучение по информационна сигурност и ежегодни опреснителни обучения.
Всеки служител на ЦСОЧИ, установил възникнал инцидент по отношение сигурността на информацията, е задължен да го докладва писмено и незабавно към центъра за обслужване на ЦСОЧИ. За целта сътрудникът, установил инцидента попълва запис Доклад за инцидент/слабост/пробив (Образец 2) и го регистрира в центъра за обслужване. Записът съдържа минимум следната информация:

- Обект на доклада (възникнал инцидент, потенциален инцидент, слабост, пробив) – записва се възникнал инцидент;
- Кратко описание;
- Имена на установилия инцидента/потенциалния инцидент;
- Организация/отдел/местоположение на установилия инцидента;
- Данни за контакт (телефон, е-мейл);
- Детайлно описание на инцидента/потенциалния инцидент;
- Засегнати услуги;
- Засегнати активи;
- Метод за установяване;
- Дата и час на регистриране на инцидента/слабостта/пробива;
- Регистрирал доклада

Центърът за обслужване проверява коректността на попълване на информацията в Доклада. При коректно попълване Докладът за инцидент получава статус „записано“.

При установяване на некоректна информация центърът за обслужване връща Доклада към автора му и се свързва с него като изисква възможно най-бърза корекция и повторна регистрация.

5.2.1.2. Установяване и докладване на инкубиран инцидент, слабост (потенциал за инцидент), пробив в резултат на мониторинг

Установяване на инкубиран инцидент, слабост или пробив по отношение сигурността на информацията може да произтече в резултат на провеждания постоянен мониторинг от системата за мониторинг и ранна превенция. Системният аналитик въз основа на постоянно наблюдение и анализ на системата определя тенденции, потенциални рискове, слабости. При установяване на инкубиран инцидент/слабост/пробив е длъжен незабавно и писмено да уведоми за това Мениджър по ИС като опише максимално детайлно установеното.

За установени потенциални инциденти/слабости/пробиви са длъжни да докладват всички сътрудници писмено на Мениджър по ИС.

5.2.1.3. Установяване на рисковия потенциал на инкубиран инцидент, слабост (потенциал за инцидент), пробив в резултат на мониторинг

Мениджър по ИС предприема мерки за установяване на рисковия потенциал на докладвания инкубиран инцидент/слабост/пробив по отношение сигурността на информацията. За целта той изисква от системен аналитик Доклад за оценка на потенциалните рискове. Анализира предходни доклади на Системен аналитик, за да проследи тенденциите и динамиката на процесите. При оценка на потенциалния риск по приетите в ЦСОЧИ критерии над приемливите нива Мениджър по ИС регистрира потенциалния инцидент/слабост/пробив с Доклад за инцидент/слабост/пробив в центъра за обслужване като попълва изискваната информация съгласно секция 5.2.1.1. В „Обект на доклада“ попълва съответно – потенциален инцидент, слабост или пробив. Към Доклада за инцидент/слабост/пробив Мениджър по ИС прилага подготвения Доклад за оценка на потенциалните рискове.

Действията по проверка коректността на попълване на информацията от страна на центъра за обслужване и смяна на статуса са аналогични на тези от секция 5.2.1.1.

5.2.2. Приоритизиране на инцидента/пробива/слабостта

След смяна на статуса на Доклада за инцидент/слабост/пробив на „записано“ центърът за обслужване го предоставя на Мениджър по управление на инциденти за приоритизация. Мениджър по управление на инциденти анализира и оценява настъпилите и/или потенциални последствия от инцидента на база информацията в Доклада за инцидент/слабост/пробив и Доклада за оценка на потенциалните рискове (за

случаите на докладвани потенциални инциденти, пробиви или слабости). Извършва приоритизиране на инцидента и оценява необходимостта от предприемане на неотложни мерки. Мениджър по управление на инциденти сменя статуса в Доклада за инцидент/слабост/пробив на „спешно“ при необходимост от предприемане на неотложни мерки и ги възлага на квалифициран специалист (или го поема лично) след съгласуване с Мениджър по ИС. Статус „за разследване“ се поставя ако такива неотложни мерки не са необходими.

Мениджър по управление на инциденти записва инцидента/слабостта/пробива в Регистър на инциденти/слабости/пробиви (Образец 3) като отразява минимум следната информация:

- Тип на инцидента/слабостта/пробива (възникнал инцидент, потенциален инцидент, слабост, пробив);
- Кратко описание;
- Имена на установилия инцидента/потенциалния инцидент;
- Организация/отдел/местоположение на установилия инцидента;
- Метод за откриване;
- Номер и дата на Доклада за инцидент/слабост/пробив
- Дата и час на регистриране на инцидента/слабостта/пробива;
- Разработени документи по отстраняване на инцидента/слабостта/пробива и място на тяхното съхранение (попълва се през процеса на решаване на инцидента/слабостта/пробива).

Мениджър по управление на инциденти уведомява незабавно Националния център за действие при инциденти по отношение на информационната сигурност за всеки инцидент в информационните системи по реда на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност (ДВ 101/25.11.2008).

5.2.3. Предприемане на неотложни мерки

Специалистът, на когото е възложен Доклад за инцидент/слабост/пробив със статус „спешно“ (Мениджър по управление на инциденти) взема решение относно естеството и начина на предприеманите спешни мерки. В общия случай това са мерки, целящи да игнорират или ограничат нежеланото въздействие на инцидента/слабостта/пробива върху системата и цялата организация по възможно най-бързия начин и без да се наруши съществено ефективната работа на системата и съответствието с ЕУИЦСОЧИ. Такива например са решения за изключване или изолиране на отделни сегменти от системата, временно прекъсване на услуги и други. Всички решения се съгласуват с Мениджър по ИС. При необходимост се привличат и други специалисти при вземане на решенията.

Най-често срещаните сценарии за инциденти/слабости/пробиви в информационната сигурност и съответните неотложни решения са разгледани в Плана за действие при инциденти (съгласно чл.48 на Наредбата за оперативна съвместимост и информационна сигурност), одобрен от Ръководителя на ЦСОЧИ.
След предприемане на неотложните мерки и установяване на приемливо ниво на работа на системата, Мениджър по ИС сменя статуса на инцидента/слабостта/пробива на „за разследване“.

5.2.4. Събиране на доказателства, разследване и анализ.
Събирането на доказателства и разследването на инцидента/слабостта/пробива по отношение на сигурността на информацията се извършва от Мениджър по управление на инциденти в сътрудничество с Мениджър по ИС. За целта се прави преглед на техническа документация, записи на хартиен носител или в цифров вид (регистри, логове от действия в информационната система и системата за физически достъп, обмен на електронни съобщения и други), проверка на настройки, интервю със сътрудници и външни страни и др. Всички предприемани действия следва да бъдат съобразени с приложимото законодателство. Прави се преглед на докладите в **библиотека Известни грешки** за идентичност на настоящия инцидент/слабост/пробив с минали такива. Разследването завършва с Доклад от разследване на инцидент/слабост/пробив, който установява причините, виновните лица (ако има такива), хронологията на инцидента/слабостта/пробива и предложение за промяна с цел преодоляването му. При извършване на разследването и анализа се използва услугите на компетентни сътрудници при необходимост. След приключване на Доклада от разследване Мениджър по управление на инциденти регистрира Заявка за промяна в център за обслужване на ЦСОЧИ като към нея прилага така подготвения доклад.
Мениджър по ИС сменя статуса на инцидента/слабостта/пробива на „за внедряване на промяна“.
Копие от доклада от разследване се изпраща и на Мениджър човешки ресурси и юрисконсулт за евентуално предприемане на дисциплинарно и/или съдебно производство спрямо виновните лица.

5.2.5. Предприемане на мерки за преодоляване на инцидента/пробива/слабостта (иницииране на процес на промяна)
Изпълняват се стъпките от секция 5.1 за управление на промени. След затваряне на инициираната промяна Мениджър по управление на инциденти сменя статуса на промяната на „решен“.

5.2.6. Извличане на поуки от инцидента/слабостта/пробива, реализиране на последващи промени (подобрение) и обучение. Затваряне на инцидента.

След като инцидентът/слабостта/пробива получи статус „решен“ Мениджър по управление на инциденти подготвя кратък Доклад за преодоления инцидент/слабост/пробив с акцент върху причините за него и приложения метод за преодоляването му. Докладът съхранява в **библиотека Известни грешки.** Търси възможности за реализиране на последващи промени (подобрения) с оглед избягване на подобни инциденти/слабости/пробиви в бъдеще като евентуалните промени се реализират съгласно процеса за управление на промени.

Мениджър по управление на инциденти организира обучение на заинтересованите страни, на което излага естеството, причините и метода за преодоляване на инцидента/слабостта/пробива, след което сменя статуса на предприетата промяна на „приключен“.

На преглед от ръководството като входен елемент се разглеждат всички възникнали инциденти по отношение сигурността на информацията за времето след предходния преглед; докладва Мениджър по ИС.

6. СВЪРЗАНИ ДОКУМЕНТИ

- Процедура за разработване и прилагане на коригиращи и превантивни действия при установяване на несъответствие със специфичния обхват и индикаторите за изпълнение на единните държавни изисквания за обекта на приложение;
- Наредба за общите изисквания за оперативна съвместимост и информационна сигурност;
- BDS ISO/IEC 27001:2006.

- **7. ПРИЛОЖЕНИЯ**Образец 1
- Образец 2
- Образец 3

ПРИЛОЖЕНИЕ 9: ПРОЦЕДУРА ЗА ВЪНШЕН И ВЪТРЕШЕН ОДИТ

1. ЦЕЛ

Определя начина на изпълнение на процеса на планиране, извършване на одити, докладване на резултатите и съхраняване на записите от проверки на Центрове за съхранение на особено чувствителна информация, внедрените в тях системи за управление на сигурността на информацията (СУСИ) и процесите, необходими за функционирането им, с цел независимо оценяване на съответствието им спрямо изискванията на стандарта BDS ISO/IEC 27001:2006 и Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация (ЕУИЦСОЧИ).

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща всички дейности по планиране и извършване на одити спрямо изискванията на стандарта BDS ISO/IEC 27001:2006 и Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация (ЕУИЦСОЧИ) в Центрове за съхранение на особено чувствителна информация, внедрените в тях системи за управление на сигурността на информацията (СУСИ) и процесите, необходими за функционирането им, докладването на резултатите и съхраняване на записите от одитите.

3. ОТГОВОРНОСТИ

Ръководителят на Център за съхранение на особено чувствителна информация:

- Одобрява годишен план за вътрешните одити, заповед за провеждане на вътрешен одит, план за провеждане на вътрешен одит;
- Назначава одиторския екип;
- Преглежда резултатите от проведените вътрешни одити.

Мениджърът по ИС:

- Разработва годишен план за вътрешните одити;
- Подпомага екипа на вътрешните одитори;
- Преглежда резултатите от проведените вътрешни одити;
- Осъществява контрол по спазване на процедурата за вътрешни одити;
- Съхранява записи от извършените одити.

Одиторите:

- Планират провеждането на вътрешни одити;
- Осъществяват безпристрастна оценка на дейностите;
- Документират и анализират резултатите от проведените одити.

Ролите и отговорностите по отношение стъпките на процедурата са посочени в RACI (Изпълняващ/Отговарящ/Консултиращ/Информиран) матрица в Таблица 1 по-долу:

Таблица 1

Роля: / **Стъпка:**	**Ръководтел ЦСОЧИ**	**Мениджър по ИС**	**Водещ одитор**	**Одитор**	**Отговорник одитирано звено**
Създаване на годишен план за одити	A	R			
Назначаване на одит	A	R	I	I	
Планиране провеждането на вътрешния одит	A	I	R	I	I
Провеждане на одит			R/A	R	R
Документиране на несъответствия		I	R/A	R	I
Определяне на коригиращи действия			I	I	R/A
Доклад за резултатите от одита		I	R/A	C	
Разпореждане за изпълнение на коригиращи действия		R/A	I		I
Извършване на коригиращите действия	(A)	I			R/A
Преглед на предприетите коригиращи действия		R/A			
Съхранение на документи и записи	I	R/A			

R= Изпълняващ A= Отговарящ C= Консултиращ I= Информиран

4. ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

Одит - систематичен, независим и документиран процес за получаване на доказателства и обективното им оценяване, за да се определи степента, до която са удовлетворени критериите на одита – в случая съответствие между Единните унифицирани изисквания към центровете за съхранение на особено чувствителна информация, документираната система за управление на сигурността на информацията, и изискванията на стандарта BDS ISO/IEC 27001:2006 от една страна и съществуващите практики и състояние на проверявания ЦСОЧИ.

Годишен план за одити - планирани за период от една година одити.

Критерии за одит - съвкупност от политики, процедури или изисквания, използвани за съпоставка.

Доказателства от одит - записи, изявления за факт или друга информация, свързана с критериите за одит, която може да бъде проверена.

Заключения от одит - резултати от оценката на набраните доказателства от одит чрез критериите за одита.

Изводи от одит - резултати от одит, до които е стигнал екипът за одит след разглеждане на целите на одита и всички заключения от одита.

Система за управление – рамка от политики, процедури, указания и свързаните с тях ресурси за постигане на целите на организацията.

Система за управление на сигурността на информацията (СУСИ) – част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията.

ЦСОЧИ – център за съхранение на особено чувствителна информация.

ЕУИЦСОЧИ – единни унифицирани изисквания към центровете за съхранение на особено чувствителна информация.

ИС – информационна сигурност.

5. ОПИСАНИЕ НА ПРОЦЕДУРАТА

5.1. Създаване на годишен план за одити

Мениджърът по ИС изготвя **Годишен план за провеждане на вътрешни одити по ИС** (Образец 1), който се утвърждава от Ръководителя на ЦСОЧИ. В плана се залагат проверки на различни зони или процеси за определяне съответствието спрямо определените и документирани изисквания на ЕУИЦСОЧИ, стандарта BDS ISO/IEC

27001:2006 и внедрената СУСИ. В рамките на едногодишния период от плана следва да бъдат обхванати всички зони и процеси от работата на ЦСОЧИ и внедрената СУСИ. Допуска се провеждането на извънредни одити по преценка на ръководството, като причините се отбелязват в съответните програми за СУСИ. Основания за провеждане на извънредни вътрешни одити за СУСИ могат да бъдат:

- Настъпили инциденти по ИС;
- Резултати от наблюдения или докладвани слабости;
- Промени в активи, влияещи съществено върху ИС;
- Промени в законодателството;
- Промени в околната среда, довели до големи промени в СУСИ.

5.2. Планиране провеждането на вътрешния одит

Мениджър по ИС подготвя и представя за одобрение от Ръководителя на ЦСОЧИ **Заповед за провеждане на вътрешен одит по ИС**, с която се определят сроковете, обхвата на одита и одиторския екип. След одобрението свежда Заповедта до знанието на заинтересованите страни (членове на одиторския екип, отговорници на одитирани звена).

Подборът на одиторския екип се извършва въз основа на следните критерии:

- Одиторите добре да познават:
  - Изискванията на ЕУИЦСОЧИ,
  - Изискванията на стандарта BDS ISO/IEC 27001:2006,
  - Структурата и работата на ЦСОЧИ,
  - Работните процеси и използвани технологии;
- Да притежават подходящи образование, квалификация и опит;
- Да владеят техниките за провеждане на одит.

Изборът на одиторите следва да осигури обективността и безпристрастността на процеса на одит. При определяне на екипа трябва да бъде спазено изискването за обективност и независимост на одитирането. Одиторите не могат да одитират собствената си дейност.

При подбора на одиторски екип се определя Водещ одитор, който:

- подготвя и предлага за утвърждаване от Ръководителя на ЦСОЧИ **План за провеждане на вътрешен одит по ИС** (Образец 2);
- уведомява отговорниците на одитираните звена за обхвата на одита най-малко 3 работни дни предварително.

Планът за провеждане на вътрешния одит се изготвя като се вземат под внимание състоянието и важността на процесите и областите, подлежащи на одит, както и резултатите от предишни одити. Планът за провеждане на вътрешен одит по ИС включва следните задължителни атрибути:

- Цел на одита;
- Обхват на одита и основание за провеждането му;
- Критерии за провеждане на одита;
- Методи за провеждане на одита;
- Одиторски екип;
- Срок за провеждане на одита;
- План – график по звена, процеси и одитори.

Критерии за провеждане на вътрешен одит по ИС на ЦСОЧИ следва да бъдат:

- Регламентираните изисквания на ЕУИЦСОЧИ, включително цитираните в тях изисквания на стандарти;
- Изискванията на стандарта BDS ISO/IEC 27001:2005;
- Изискванията на документите на СУСИ.

Подготовката за извършване на одита включва преглед на документите на СУСИ, проучване за съществуващи или потенциални несъответствия, подготовка на въпросници и др.

5.3. Провеждане на одит

Одитиращият запознава персонала на одитирания обект с целите, обхвата, критериите, методите и организацията за провеждане на одита, преглежда документите и записите на одитираната дейност за спазване на изискванията на ЕУИЦСОЧИ, стандарта BDS ISO/IEC 27001:2006 и практиката по прилагането им. Одиторът извършва наблюдения на дейности и състояния, провежда интервю с работещите в одитираната зона, събира доказателства за съответствие.

Доказателства за съответствие се събират чрез:

- Проверка на документи и записи;
- Наблюдение на дейности и състояния;
- Наблюдение на условия и изисквания.

При установяване на несъответствие с изискванията на ЕУИЦСОЧИ, стандарта или документите на СУСИ в резултат от извършените действия при одита, доказателствата за установените факти се наричат доказателства за установени несъответствия.

Одитът завършва с кратък обобщаващ разговор, на който водещият одитор запознава ръководителите на одитираните обекти с направените констатации.
Одиторите водят записки като записват четливо своите наблюдения, доказателства и констатации. В края на одита предават записките на водещия одитор.

5.4. Документиране на несъответствия
За всяко констатирано несъответствие одиторите съставят **Протокол за несъответствие от вътрешен одит по ИС** (Образец 3)**,** който трябва да бъде подписан от одитора и отговорника на одитираното звено.

5.5. Определяне на коригиращи действия
Отговорникът на одитираното звено предлага корекция или коригиращо действие, което записва в определеното за целта място на **Протокола за несъответствие от вътрешен одит по ИС** и се подписва.

5.6. Доклад за резултатите от одита
След приключване дейностите по одитиране водещият одитор свиква среща на одиторския екип, на която всеки одитор споделя своите констатации от извършения одит и предава записките си на водещия одитор. Водещият одитор обобщава резултатите в **Доклад от проведен вътрешен одит по ИС** (Образец 4) и заедно с протоколите за несъответствие и записките на одиторите ги предава на Мениджъра по ИС за запознаване и разпореждане.

5.7. Разпореждане за изпълнение на коригиращи действия
След запознаване с **Доклада от проведен вътрешен одит по ИС** Мениджърът по ИС взема отношение по предложените коригиращи действия, като определя срок за изпълнение и отговорник за изпълнението, уведомява отговорника за изпълнение (ръководителя на одитираното звено), който потвърждава с полагане на подпис.

5.8. Извършване на коригиращите действия
В случай, че установените несъответствия са несъществени и лесно отстраними, те се отстраняват чрез незабавна корекция съгласно определения в **Протокол за несъответствие от вътрешен одит по ИС** срок. При несъответствия, за отстраняването на които са необходими по-съществени ресурси, действия, координация или намеса от страна на Ръководителя на ЦСОЧИ, се предприемат коригиращи действия съгласно изискванията на **Процедура Коригиращи и превантивни действия,** като закриването на **Протокола за несъответствие** се реферира към конкретно **Искане за коригиращо/превантивно действие.**

5.9. Преглед на предприетите коригиращи действия

След изтичане на определения в **Протокола за несъответствие от вътрешен одит по ИС/Искане за коригиращо/превантивно действие по ИС** срок Мениджър ИС извършва проверка относно изпълнението и ефикасността от изпълнението на предписаните коригиращи действия, отразява резултатите от проверката в **Протокол за несъответствие от вътрешен одит по ИС** и се подписва.

5.10. Съхранение на документи и записи.

Всички документи и записи от проведените вътрешни одити се съхраняват от Мениджъра по ИС. Резултатите от вътрешните одити служат като входни данни на прегледа за прилагане на ЕУИЦСОЧИ и състоянието на СУСИ, провеждан от ръководството на ЦСОЧИ с цел оценяване на съответствието на изискванията и ефективността на СУСИ.

5.11. Външни одити

Външни одити на ЦСОЧИ се провеждат от:

- Сертифициращата организация;
- Структури на държавната администрация, упълномощени по силата на приложимото законодателство.

Одитите от страна на сертифициращата организация се провеждат съгласно изискванията на стандарта БДС ISO/EN 19011:2011 по предварително съгласуван с ЦСОЧИ график.

Одити от страна на упълномощени структури на държавната администрация се извършват по реда и критериите, определени изрично за тези случаи.

6. СВЪРЗАНИ ДОКУМЕНТИ

- Процедура за разработване и прилагане на коригиращи и превантивни действия при установяване на несъответствие със специфичния обхват и индикаторите за изпълнение на единните държавни изисквания за обекта на приложение;
- BDS ISO/IEC 27001:2006.

7. ПРИЛОЖЕНИЯ

- Образец 1;
- Образец 2;
- Образец 3;
- Образец 4.

ПРИЛОЖЕНИЕ 10. ПРОЦЕДУРА ЗА РАЗРАБОТВАНЕ И ПРИЛАГАНЕ НА КОРИГИРАЩИ И ПРЕВАНТИВНИ ДЕЙСТВИЯ ПРИ УСТАНОВЯВАНЕ НА НЕСЪОТВЕТСТВИЕ СЪС СПЕЦИФИЧНИЯ ОБХВАТ И ИНДИКАТОРИТЕ ЗА ИЗПЪЛНЕНИЕ НА ЕДИННИТЕ ДЪРЖАВНИ ИЗИСКВАНИЯ ЗА ОБЕКТА НА ПРИЛОЖЕНИЕ.

1. ЦЕЛ

Тази процедура определя начина на изпълнение на дейностите по разработване, прилагане и преглед на коригиращи действия при установяване несъответствия със специфичния обхват и индикаторите за изпълнение на ЕУИЦСОЧИ, стандарта BDSISO/IEC 27001:2006 или документите на внедрената СУСИ, а така също дейностите за определяне и отстраняване на причините за потенциални несъответствия.

2. ОБЛАСТ НА ПРИЛОЖЕНИЕ

Процедурата обхваща всички дейности в Центъра за съхранение на особено чувствителни данни (ЦСОЧИ), при които възникват несъответствия или се идентифицират потенциални несъответствия с изискванията на ЕУИЦСОЧИ, стандарта BDS ISO/IEC 27001:2006 или документите на внедрената СУСИ.

3. ОТГОВОРНОСТИ

Ръководител на ЦСОЧИ:

- Утвърждава прилагането на коригиращи и превантивни действия;
- Оценява проведените коригиращи действия и ефекта от предприетите превантивни действия при преглед от ръководството.

Мениджър по ИС:

- Анализира съответствието спрямо изискванията на ЕУИЦСОЧИ, стандарта BDS ISO/IEC 27001:2006 и внедрената СУСИ, функционирането и ефективността на СУСИ и предлага при необходимост коригиращи или превантивни действия;
- Анализира резултатите от проведените одити и при необходимост предлага коригиращи или превантивни действия;
- Осъществява контрол по спазване на Процедура за разработване и прилагане на коригиращи и превантивни действия при установяване на несъответствие със специфичния обхват и индикаторите за изпълнение на единните държавни изисквания за обекта на приложение.

Отговорник за коригиращо/превантивно действие:

Отговаря за отстраняване на несъответствието / потенциалното несъответствие/ коренната причина за несъответствието след възлагане от Мениджър по ИС.

Ролите и отговорностите по отношение стъпките на процедурата са посочени в RACI (Изпълняващ/Отговарящ/Консултиращ/Информиран) матрица в Таблица 1 по-долу:

Таблица 1

Роля: / **Стъпка:**	**Ръководтел ЦСОЧИ**	**Мениджър по ИС**	**Служители**	**Отговорник за коригиращото/ превантивно действие**
Идентифициране на несъответствия/потенциални несъответствия и коренните причини за тях		I	R/A	
Регистриране на Искане за коригиращи/ превантивни действия		R/A		
Оценка на нуждата и определяне на необходимите коригиращи/превантивни действия	A	R		I
Подготовка и документиране на анализа на специфичната необходимост от постигане на съответствие	I	C		R/A

Преглед на предприетите коригиращи/превантивни действия	I	R/A		C

R= Изпълняващ A= Отговарящ C= Консултиращ I= Информиран

4. ТЕРМИНИ, ОПРЕДЕЛЕНИЯ И ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ.

Коригиращо действие - действие, за отстраняване на причината за съществуващо несъответствие или за друга нежелана ситуация.

Превантивно действие - действие, което се предприема за отстраняване на причината за възможно несъответствие или на друга нежелана потенциална ситуация.

Несъответствие - неизпълнение на изискване.

Корекция - действие за отстраняване на открито несъответствие.

Система за управление – рамка от политики, процедури, указания и свързаните с тях ресурси за постигане на целите на организацията.

Система за управление на сигурността на информацията (СУСИ) – част от цялостна система за управление, основана на подхода за бизнес риска, за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на сигурността на информацията.

ЦСОЧИ – център за съхранение на особено чувствителна информация.

ЕУИЦСОЧИ – единни унифицирани изисквания към центрове за съхранение на особено чувствителна информация.

ИС – информационна сигурност.

5. ПРОЦЕДУРА

5.1. Идентифициране на несъответствия/потенциални несъответствия и коренните причини за тях

Идентифициране на несъответствия може да има в резултат от:

- Извършен одит (вътрешен или външен) за съответствие с изискванията на ЕУИЦСОЧИ или стандарта BDS ISO/IEC 27001:2006;
- Възникнал инцидент с информационната сигурност;
- Наблюдения в ежедневната работа.

Идентифицирането на несъответствие може да бъде извършено от всеки компетентен в съответната област сътрудник в горепосочените случаи. При установяването на такива той е длъжен без забавяне да информира Мениджър по ИС. Сътрудникът отразява

констатираното несъответствие в **Искане за коригиращи/ превантивни действия по ИС** (Образец 1)) като попълва следните секции:

- Описание на несъответствието/потенциалното несъответствие;
- Предложение за отстраняване на несъответствието / потенциалното несъответствие;
- Коренна причина за несъответствието/потенциалното несъответствие;
- Предложение за отстраняване на коренната причина.

и се подписва, след което предава попълненото **Искане за коригиращи/ превантивни действия по ИС** на Мениджър по ИС за разглеждане. Описанието на несъответствията/потенциалните несъответствия, коренните причини и предлаганите коригиращи/превантивни действия се описват максимално точно по отношение на същност, време, местоположение и опасност от разпространение.

Когато несъответствието е в резултат на одит, проблемът е ясно и точно определен от одитора като неизпълнение на определено изискване.

Мениджърът по ИС разглежда **Искане за коригиращи/ превантивни действия по ИС,** съхранява го и го записва в **Регистър на коригиращи и превантивни действия по ИС (Образец 2).** В Регистъра задължително се водят:

- Номер и дата на Искането за коригиращи/превантивни действия по ИС;
- Имената на сътрудника, идентифицирал несъответствието/потенциалното несъответствие;
- Дата на завеждане в Регистъра;
- Статус на Искането:
- Дата на последна промяна на статуса.

Регистърът на коригиращи/превантивни действия по ИС се води в електронен вид. На етапа на регистрация Искането има статус „регистриран“ в Регистъра на коригиращи и превантивни действия по ИС.

5.2. Оценка на нуждата и определяне на необходимите коригиращи/превантивни действия

Мениджър по ИС разглежда **Искане за коригиращи/ превантивни действия по ИС** като се консултира с компетентни специалисти относно нуждата и адекватността на предложените коригиращи/ превантивни действия и предложените действия за отстраняване на коренната причина, адекватни срокове и отговорници за изпълнението им.

Критерии за предприемане на коригиращи действия могат да бъдат:

- Предложението е свързано с настъпил инцидент по ИС;
- Има регистрирани слабости и тенденции в тази насока;

- Има променени изисквания от клиенти;
- Има промяна в законови или нормативни документи;
- Има промяна в стандарти;
- Има регистриран недопустим риск за информационната сигурност.

Необходимост от прилагане на превантивни действия може да възникне вследствие на информация, получена от изпълнението на:

- Има промяна в стандарти;
- Вътрешни одити;
- Измерване на ефективността на внедрените ЕУИЦСОЧИ или СУСИ;
- Оценка на риска;
- Мониторинг на информационни системи;
- Управление на инциденти по информационната сигурност;
- Преглед на ръководството.

При установяване, че коригиращи/превантивни действия не са необходими Мениджър по ИС отразява това в секция **Становище на Мениджър по ИС**, сменя статуса на Искането за коригиращи/превантивни действия по ИС в Регистъра на коригиращи/превантивни действия по ИС на „отказан“ и архивира Искането.
При установена необходимост от коригиращи/превантивни действия и действия за отстраняване на коренната причина и след определянето им Мениджър по ИС попълва информация за тях в секции:

- Срок за отстраняване на несъответствието/потенциалното несъответствие;
- Отговорник за отстраняване на несъответствието/потенциалното несъответствие;
- Срок за отстраняване на коренната причина;
- Отговорник за отстраняване на коренната причина;
- Необходими ресурси.

на Искането за коригиращи/превантивни действия по ИС.
Следва да се има предвид, че коригиращите/превантивни действия по отношение на несъответствието/потенциалното несъответствие имат обикновено краткосрочен характер, а коригиращите/превантивни действия по отношение на коренната причина – дългосрочен характер.

Мениджър по ИС представя Искането за коригиращи превантивни действия по ИС на Ръководител ЦСОЧИ за разглеждане и одобрение (подпис).

След одобрение от Ръководител ЦСОЧИ Мениджър по ИС запознава отговорниците за изпълнение на коригиращите/превантивните действия и за отстраняване на коренните причини, което те потвърждават с подпис върху Искането.
Мениджър по ИС сменя статуса на Искането за коригиращи/превантивни действия в Регистъра за коригиращи/превантивни действия на „в изпълнение“.

5.3. Осъществяване на необходимите коригиращи/превантивни действия и записване на резултатите от предприетите действия.

Провеждането на коригиращо/превантивно действие включва:

- Оценка на значимостта на несъответствието/потенциалното несъответствие;
- Информиране;
- Документиране;
- Ангажиране на необходимите сътрудници;
- Допълнителен анализ на възможните причини и вероятността за появата им;
- Анализ на възможните методи за отстраняване на несъответствията/потенциалните несъответствия;
- Анализ на последствията;
- Вземане на решение;
- Предприемане и контролиране на действията;
- Оценка на резултатите;
- Задържане на постигнатите резултати.

Коригиращите/превантивните действия могат да изискват широк набор от мерки като:

- Обучение;
- Промени в организацията;
- Промени в процедурите;
- Промени в процесите и оборудването.
- Въвеждане на нови контроли;
- Промяна или усъвършенстване на съществуващи контроли;
- Прилагане други начини за избягване на риска.

В зависимост от обема и сложността на изискваните дейности определеният отговорник за отстраняване на несъответствието/потенциалното несъответствие/коренната причина чрез съдействие от Мениджър по ИС и одобрение от Ръководител на ЦСОЧИ привлича необходимите специалисти и създава работна група, в която участват представители на заинтересованите звена.

Необходимите промени, записите за тях и резултатите от предприемането им се извършват по реда, предвиден в съответните документи (**Процедури Управление на промени и инциденти с информационната сигурност, Процедура Управление на документи и записи и др.**).

5.4. Преглед на предприетите коригиращи/превантивни действия

Отговорникът за отстраняване на несъответствието/потенциалното несъответствие/коренната причина предава за анализ и съхранение на Мениджър по ИС всички документи, свързани с планиране, осъществяване и контрол на проведеното коригиращо/превантивно действие след неговото изпълнение.

След изтичане на предвидения в **Искането за коригиращи/превантивни действия по ИС** срок Мениджърът по ИС извършва оценка преглед на изпълнението и ефективността на коригиращото/превантивно действие по отношение на несъответствието/потенциалното несъответствие.

Ефективността на коригиращите/превантивните действия зависи от ефективността на всички етапи на извършването им – дефиниране на проблема, събирането на необходимите данни, изясняване на причините, извършване на корекциите и оценяване на ефективността.

При необходимост от по-специализирани познания и компетентност за целите на проверката Мениджър по ИС използва специалист/одитор с доказана компетентност.

Установените резултати от извършената проверка и анализ Мениджър по ИС записва в секция ПРОВЕРКА НА ЕФИКАСНОСТТА НА ИЗВЪРШЕНИТЕ КОРИГИРАЩИ / ПРЕВАНТИВНИ ДЕЙСТВИЯ ПО ОТНОШЕНИЕ НА НЕСЪОТВЕТСТВИЕТО/ ПОТЕНЦИАЛНОТО НЕСЪОТВЕТСТВИЕ на Искането за коригиращи/превантивни действия по ИС, което се потвърждава с подпис от Мениджър по ИС и съответния проверяващ специалист/одитор (ако е използван такъв).

Преглед на изпълнението и ефективността на коригиращото/превантивно действие по отношение на коренната причина се извършва по ред, аналогичен на предвидения по-горе за преглед на изпълнението и ефективността на коригиращото/превантивно действие по отношение на несъответствието/потенциалното несъответствие.

Установените резултати от извършената проверка и анализ Мениджър по ИС записва в секция ПРОВЕРКА НА ЕФИКАСНОСТТА НА ИЗВЪРШЕНИТЕ КОРИГИРАЩИ / ПРЕВАНТИВНИ ДЕЙСТВИЯ ПО ОТНОШЕНИЕ НА КОРЕННАТА ПРИЧИНА на Искането за коригиращи/превантивни действия по ИС, което се потвърждава с подпис

от Мениджър по ИС и съответния проверяващ специалист/одитор (ако е използван такъв).
При положителна оценка на изпълнението и ефективността на коригиращите/ превантивни действия по отношение на несъответствието/потенциалното несъответствие и коренната причина Мениджър по ИС приключва Искането за коригиращи/превантивни действия по ИС, подготвя кратък анализ на проблема и решението и архивира. Искането заедно с документацията по изпълнението.
Като входен елемент за преглед от ръководството на дейността на ЦСОЧИ и внедрената СУСИ Мениджър по ИС внася доклад за всички установени несъответствия и повдигнати коригиращи/превантивни действия за периода от последния преглед от ръководството, както и анализ на резултатите от приключените коригиращи/ превантивни действия за периода.

6. СВЪРЗАНИ ДОКУМЕНТИ

- Процедура Управление на документи и записи;
- Процедура за външни и вътрешни одити;
- BDS ISO/IEC 27001:2006.

7. ПРИЛОЖЕНИЯ

- Образец 1

Образец 2