Версия:	1.0
Дата на версията:	19.10.2023 г.
В сила от:	19.10.2023 г.
Изготвени от:	АйТи Бейслайн ООД, консултант
Одобрени от:	Проф. д-р Димитър Димитров, ректор на УНСС
Ниво на поверителност:	Ниво 2 – Служебно ползване

ФИЗИЧЕСКИ МЕХАНИЗМИ ЗА КОНТРОЛ

СЪГЛАСНО ISO/IEC 27001:2022

РЕГИСТРИРАНЕ НА ИЗМЕНЕНИЯТА	
Стр.	Същност на изменението

CONTENTS

1. ЦЕЛ

- Настоящата процедура определя реда, отговорностите, както и системата от мерки, способи и средства при внедряване и прилагане на физическите механизми за контрол в УНСС;
- Осигуряване на подходящо ниво на защита, надеждно управление и ефективен контрол на активите и ресурсите на УНСС;
- Недопускане или намаляване до минимум на щетите от произшествия, свързани с контрола на процесите по управление на активите и ресурсите.

2. ОБХВАТ

Настоящия документ обхваща процесите по избор, внедряване, прилагане и мониториране на физическите механизми за контрол, съгласно клауза 7 на Приложение А от ISO27001: 2022.

3. ОТГОВОРНОСТИ

Настоящата процедура обхваща всички йерархични нива и служители на УНСС. Пряка отговорност за прилагане и спазване на настоящата процедура носят лицата от УНСС, както следва:

- **Ректор/Представител на ръководството** за непрекъснат контрол на процесите и осигуряване на необходимите ресурси;
- **Мениджър ИС** и **Мениджър ИТ** за оказване на контрол и методическа помощ в структурните звена и пряко управление на процесите в техните правомощия и функционални задължения;
- **Мениджър СУИС** за координация и правилно управление на процесите и дейностите, както и документирането им;
- **Служителите от УНСС** за прилагане на Процедурата и усъвършенстването на СУИС.

4. ТЕРМИНОЛОГИЯ И СЪКРАЩЕНИЯ

Не се въвеждат нови термини и съкращения.

5. ДЕЙСТВИЯ И МЕТОДИ

Изборът на физическите механизми за контрол е съгласно клауза 7 на Приложение А от ISO27001: 2022. Внедряването им се извършва като се вземат предвид правни, законови, регулаторни, договорни и други изисквания с цел постигане високо ниво на информационна сигурност в УНСС, както и съответствие на СУИС с изискванията на стандарта. Вземайки предвид публичната си функция, УНСС налага рестриктивни мерки по отношение на физическата сигурност, само в определени помещения/зони, които не могат да се свържат пряко с учебния процес.

1. Системата от мерки за физическа сигурност е част от общите изисквания за сигурност по защита на информацията. Способи за предотвратяване на заплахите за физическата сигурност са:
   - Анализ на риска - оценка на заплахите за физическата сигурност на категоризираната информация (съгласно приложеното класифициране на информацията);
   - Планиране и внедряване на конкретни мерки за осигуряване на физическата сигурност на категоризираната информация.
2. Мениджър ИС отговаря за прилагането и спазването на системата от мерки, способи и средства за физическа сигурност на информацията. Те се изпълняват в съдействие с другите служители, пряко ангажирани със СУИС, както и с ръководителите на структурните звена, предлага необходимата система от мерки за физическа сигурност въз основа на оценен риск. Ръководството утвърждава прилагането на съответните мерки за физическа сигурност на информацията.
3. Мерките за физическа сигурност имат за цел:

- Предотвратяване на нерегламентиран достъп или на опит за нерегламентиран такъв до активите на УНСС;
- Съгласно нивото на поверителност - разрешение за достъп до информация и в съответствие с принципа "необходимост да се знае";
- Своевременно установяване и противодействие при нарушаване или при опит за нарушаване на мерките за физическа сигурност.

А. 7.1. ГРАНИЦИ ЗА ФИЗИЧЕСКА СИГУРНОСТ

Механизъм за контрол: *Границите на сигурност трябва да бъдат определени и да бъдат използвани за защита на зони, които съдържат чувствителна или критична информация и средства за обработка на информацията*

1. Физическата сигурност е организирана на база многослойния модел за защита, което означава, че всички внедрени механизми функционират заедно в поддържаната архитектура. Концепцията е, че ако един от слоевете бъде компрометиран, останалите ще осигурят нужната защита на актива. Избрания модел следва принципа:

    - Спиране на достъп до защитавания актив, ако тази защита бъде преодоляна, се преминава към;
    - Забрана на достъп до актива. Паралелно или в последствие на забраната за достъп се включва;
    - Забавяне достигането до актива. Забавянето е елемент, който дава време за;
    - Преценяване на ситуацията, за да се вземе правилното решение за;
    - Реакция.

2. Физическата защита се постига посредством създаване на целеви физически бариери около определени работни помещения и средствата за обработка на информацията. Всяка от тях повишава общата осигурявана защита.
3. УНСС управлява своите граници за физическа сигурност, като взима под внимание следните особености:

    - Физическите граници на защитените зони са ясно определени и регламентирани.
    - Защитата на всеки периметър зависи от изискванията за сигурност към активите и средствата за обработка на информацията, разположени в конкретния периметър и от резултатите от оценката на риска;
    - Сградата е лесно достъпна, разположена е в район с развита инфраструктура, в близост до важни пътни артерии, които през зимния сезон са поддържани;
    - Всички външни врати и прозорци на помещенията с наблюдаван/ограничи достъп са подходящо защитени срещу неразрешен достъп с контролни механизми;
    - Сградата е осигурена с нужните комунални услуги: електрозахранване, вода, канализация;
    - Физическия достъп до Зона 1 и Зона 2 от сградата на УНСС е ограничен само за упълномощения персонал. Външни за УНСС лица достъпват съответните зони само с придружител през целия период на престой.

4. За нуждите на физическата сигурност ръководството е определило защитените зони, както следва:

Защитена зона	Описание	Достъп
Периметър 1 Контролиран достъп	Зона с **контролиран достъп**, в която попадат сървърни помещения.	Ръководство, Служители на Дирекция ИТ, Специално упълномощени служители
Периметър 2 Контролиран достъп	Зона с **контролиран достъп**, в която попадат работни помещения.	Ръководство Всички служители
Периметър 3 Контролиран достъп	Зона с **наблюдаван достъп**, в която попадат учебни помещения.	Ръководство Всички служители Външни посетители/студенти Доставчици.

А. 7.2. КОНТРОЛ НА ФИЗИЧЕСКИЯ ДОСТЪП

Механизъм за контрол: *Сигурните зони трябва да бъдат защитени със съответни механизми за контрол на входа, за да се гарантира, че само упълномощеният персонал има разрешен достъп.*

1. Ръководството е утвърдило следните механизми за контрол на физическия достъп:
   - Физическия контрол на достъп се осъществява чрез индивидуализирани RFID чипове;
   - Случайните посетители не се оставят без придружител по време на престоя на територията на УНСС;
   - Достъпа до фиксираните защитени зони е ограничен само за служители;
   - Персоналът на трета страна, извършващ услуга по поддръжка, има ограничен достъп до защитените зони, като се изисква придружител и непрекъснато наблюдение.

2. Процесът на управление на правата за достъп до физическите зони включва предоставянето, периодичния преглед, актуализирането и отнемането на оторизации, съгласно т. А.5.18. Мерките са допълнени и от сигурно поддържане и мониторинг на физическия дневник за регистрация или електронния одитен дневник за целия достъп и защита на всичките регистрационни файлове, съгласно т. А5.33 и чувствителната информация за автентификация.

А. 7.3. ОСИГУРЯВАНЕ НА ОФИСИ, ЗАЛИ И СЪОРЪЖЕНИЯ

Механизъм за контрол: *Трябва да бъде проектирана и приложена физическа защита за офиси, зали и съоръжения.*

1. При обезопасяването на офиси, стаи и оборудване на УНСС са взети под внимание следните особености:
   - Отчетени са съответните регулации и стандарти за здраве и безопасност;
   - Осигурени са благоприятни условия за работа;
   - Поставени са средства за заключване, за да се избегне нерегламентиран достъп;
   - Липсват очевидни знаци вън или вътре в сградата, показващи наличието на дейности по обработка на информация;
   - Топологични схеми и друга документация, показваща разположенията на средства за обработка на чувствителна информация, са трудно достъпни;
   - Вратите, прозорците и периметъра като цяло са осигурени, когато няма физическо присъствие;
   - Известителните системи са редовно изпитвани в съответствие с установените стандарти;
   - Сградите, офисите и оборудването не са изложени на силни електромагнитни и радиочестотни лъчения.

А. 7.4. МОНИТОРИНГ НА ФИЗИЧЕСКАТА СИГУРНОСТ

Механизъм за контрол: *Помещенията трябва да се наблюдават непрекъснато за неоторизиран физически достъп*

1. Мониторинг на физическата сигурност на УНСС се осъществява предимно чрез видеонаблюдение в специализиран център. Картината на камерите, разположени в сградата, се наблюдава в реално време от специализиран екип на Сектор "Организация на сигурността".
2. Съгласно Закон за частната охранителна дейност /ЗЧОД/ и ОРЗД УНСС съхранява записи в системите за видеонаблюдение не повече от 60 календарни дни.
3. Съгласно Общ регламент за защита на данни са поставени информационни табели за наличието на средства за видеонаблюдение на всички входове в УНСС.
4. Сигнално-охранителната техника е редовно проверявана и изпитвана.

А. 7.5. ЗАЩИТА ОТ ВЪНШНИ ЗАПЛАХИ И ЗАПЛАХИ, ПРИЧИНЕНИ ОТ ОКОЛНАТА СРЕДА

Механизъм за контрол: *Трябва да бъде проектирана и приложена физическа защита срещу природни бедствия, злонамерени действия и инциденти.*

1. Ръководството е определило 4 /четири/ категории заплахи, с които УНСС трябва да се справя:
   - Природни заплахи: наводнения, земетресения, бури, пожари, изключително високи или ниски температури на околната среда;
   - Заплахи от осигуряващи системи: отпадане на електрозахранване, прекъсвания в телекомуникациите и прекъсване на подаването на енергийни източници;
   - Заплахи от действието на човека: Неоторизиран достъп, умишлени експлозии, вреди от разгневени служители или доставчици, грешки при работа или инциденти, вандализъм, кражби и измами;
   - Политически мотивирани заплахи: Стачки, бунтове, терористични актове и палежи.

2. Ръководството обръща специално внимание на заплахи за сигурността, произтичащи от съседни помещения, пожар в съседна сграда или офис, изтичане на вода от по-горно помещение, повреди в HVAC инсталациите, експлозия на улицата. Взети са предвид следните указания за избягване на щети от пожар, наводнение, земетресение, експлозия, гражданско вълнение и други форми на природно или предизвикано от човека бедствие:
   - Основния приоритет на ръководството при заплахи, бедствия или аварии е да се гарантира сигурността на персонала преди всичко;
   - На второ място са поставени критични системи, оборудване и помещения на УНСС;
   - Осигурени са и са поставени на подходящо място пожарогасителни устройства, чиито клас е съобразен с вида на защитаваните активи. За компютърното оборудване е осигурен пожарогасител с CO2, а за останалото оборудване прахов пожарогасител.

А. 7.6. РАБОТА В СИГУРНИ ЗОНИ

Механизъм за контрол: *Трябва да бъдат проектирани и приложени физическа защита и указания за работа в сигурни зони.*

1. Само упълномощеният персонал има достъп до средствата за обработка на информацията, намиращи се в Периметър 1.

Освен въведените контролиран достъп и видеонаблюдение в защитените зони Мерките за работа в тях включват различни видове контрол за служителите, доставчиците и потребителите от трета страна, като например:

- информиране на персонала за съществуването на защитена зона или за дейностите в нея само на
- базата на принципа „необходимо да се знае;
- избягване на безнадзорна работа в защитените зони както от съображения за безопасност, така и за
- намаляване на вероятността за злонамерени дейности;
- физическо заключване и периодична проверка на защитени зони;
- публикуване на процедурите за спешни случаи по видим или лесно достъпен начин.

А. 7.7. ЧИСТО БЮРО И ЧИСТ ЕКРАН

Механизъм за контрол: *Трябва да бъдат приети ясни правила за "чисто бюро" при съхранение на документи и преносими информационни носители и правила за чист екран за средствата за обработка на информация.*

1. Приетата политика за „чисто бюро и чист екран“ отчита класификацията на информацията, правните и договорните изисквания и съответните рискове за УНСС. Политиката е базирана на следните принципи:
   - Чувствителната или критичната бизнес информация, независимо от вида й, е подходящо защитена, когато не е необходима;
   - Компютрите и крайните устройства са оставяни неактивни и несвързани към преносната среда или защитени с механизми за заключване на екрана и клавиатурата, контролирани чрез парола, когато не са наблюдавани;
   - Местата за получаване и изпращане на пощата са защитени по подходящ начин;
   - Документи, съдържащи чувствителна информация, са прибирани незабавно от печатащите устройства;
   - Служителите са инструктирани за почистване на бюрата преди напускане, с цел да не се оставят документи или други информационни носители без надзор.

2. Ръководството на УНСС осъзнава, че воденето на успешна политика за чисто бюро/екран, намалява рисковете от неразрешен достъп, загуба и нарушаване на информацията по време на и извън нормалните работни часове.

А. 7.8. РАЗПОЛАГАНЕ И ЗАЩИТА НА УСТРОЙСТВАТА

Механизъм за контрол: *Оборудването трябва да бъдат поставено така, че да е подсигурено и защитено.*

1. За да защити адекватно своето оборудване, УНСС е внедрила следните изисквания:

- УНСС е разположила резервни копия на информацията си в клауд инфраструктура.
- Средствата за обработка на информация, обработващи и съхраняващи чувствителни данни, са подходящо разположени;;
- Сградата, в която се помещава на УНСС ползва защита срещу мълнии. Използвани са филтри за защита от мълнии на всички входящи линии на електрозахранването и на телекомуникационните трасета;

А. 7.9. СИГУРНОСТ НА УСТРОЙСТВАТА ИЗВЪН ПОМЕЩЕНИЯТА

Механизъм за контрол: *Активите, които са извън УНСС, трябва да бъдат защитени.*

1. Ръководството на УНСС допуска ползването на устройства извън работните помещения, като за защитата на оборудването се имат предвид следните особености:

- Устройствата и носителите, изнесени извън територията на УНСС, не се оставят без наблюдение на публични места, обществен, служебен или личен транспорт;
- При пътуване, преносимите компютри се носят като ръчен багаж, за да се избегне кражба на актива;
- Спазват се всички инструкции на производителите за защита на оборудването, независимо от това, че е извън територията на УНСС.
- След всяка оценка на риска се определят и прилагат подходящи механизмите за контрол при работа извън територията на УНСС.

А. 7.10. СЪХРАНЕНИЕ НА ПРЕНОСИМИ НОСИТЕЛИ

Механизъм за контрол: *Преносими носители се управляват през целия жизнен цикъл на придобиване, използване, транспортиране и изхвърляне в съответствие с класификационната схема, приета УНСС и изискванията за обработка УНСС.*

1. УНСС не съхранява конфиденциална/значима информация на преносими устройства. На служебните компютри USB портовете са разрешени, като е приложен контрол по безусловна проверка от специализиран продукт за анти-вирусна защита, всеки път когато такова устройство бъде използвано.
2. Опазването и съхранение на преносимите ел. подписи е задължение на техния собственик.
3. За резервиране на важната за УНСС информация се използва облачна платформа.

А. 7.11 ПОДДЪРЖАЩИ КОМУНАЛНИ УСЛУГИ

Механизъм за контрол: *Устройствата трябва да бъдат защитени от повреди в електрозахранването и други пробиви, предизвикани от откази в поддържащите комунални услуги.*

1. Ръководството е осигурило подходящи и надеждни комунални услуги, като електроснабдяване, водоснабдяване, канализация, отопление, вентилация и климатизация на въздуха. Спазват се следните изисквания:
   - Поддържането на комуналните услуги е редовно проверявано и изпитвано, за да се гарантира тяхното правилно функциониране и да се намали всякакъв риск от тяхното неправилно действие или отказ;
   - Осигурено е подходящо електрозахранване, което отговаря на спецификациите на производителите на устройствата;
   - Извършват се регулярни замервания за допустимите заземителни норми.

А. 7.12. СИГУРНОСТ НА ОКАБЕЛЯВАНЕТО

Механизъм за контрол: *Окабеляването за електрозахранване и телекомуникации, носещо данни или поддържащо информационни услуги, трябва да бъде защитено от прекъсване или повреда.*

1. Ползваното в УНСС окабеляване за нуждите на електрозахранването и телекомуникационния пренос е обезопасено. При обезопасяването са взети под внимание следните особености:
   - Електрозахранващите проводници за разположени в самостоятелни трасета, реализирани под земята, в ниски тавани, повдигнати подове или специални чрез PVC канали, за да се предотврати интерференция с телекомуникационните трасета;
   - Мрежовото окабеляване също ползва самостоятелни трасета реализирани под земята, в ниски тавани, повдигнати подове или чрез специални PVC канали и е защитено срещу неразрешено прекъсване, повреда или подслушване;
   - Ползвана е маркировка на кабелите и устройствата, която ясно ги определя, за да се

минимизират грешки като неочаквано временно съединяване на грешни мрежови кабели;

- Където е приложимо се ползва оптично окабеляване;
- Ползват се екранирани кабели за пренос на данни;
- Регламентиран е контролиран достъп до съединителни табла и помещенията с окабеляването.

А. 7.13. ПОДДРЪЖКА НА УСТРОЙСТВАТА

Механизъм за контрол: *Оборудването трябва да се поддържа правилно, за да се гарантира наличността, целостта и поверителността на информацията.*

1. УНСС поддържа своето оборудване съгласно следните указания:

- Всяко устройство е поддържано в съответствие с препоръките от производителя;
- Ремонтите и обслужването на устройствата се извършват само от технически компетентен персонал;
- Надзор над персонала за поддръжка при извършване на поддръжката на място;
- Упълномощаване и контролиране на достъпа за дистанционна поддръжка.

А 7.14. СИГУРНО УНИЩОЖАВАНЕ

Механизъм за контрол: *Всички елементи на устройство, съдържащо магнитни носители, трябва да бъдат проверявани, за да се гарантира, че всякакви чувствителни данни и лицензиран софтуер са били премахнати или сигурно презаписани преди унищожаването.*

1. Ръководството е приело, че устройства, съдържащи чувствителна информация и излизащи от експлоатация или определени за повторна употреба, ще бъдат физически унищожени или информацията върху тях ще бъде изтрита или почистена;
2. Прието е за дефектиралите запомнящи устройства, съдържащи чувствителни данни, да се извършва съгласуване с Мениджър ИС, за да се определи дали оборудването трябва да бъде физически унищожено, вместо изпратено за ремонт;
3. Ръководството осъзнава, че чувствителна информация може да бъде изложена на риск при небрежно изхвърляне, бракуване или повторно използване на устройствата.

6. СПРАВОЧНИ ДОКУМЕНТИ

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022

7. ПРИЛОЖЕНИЯ

- Протоколи от изпитвания

Дата: 19.10.2023 г.

Утвърдил: ……

Проф. д-р Димитър Димитров, Ректор