| | |
|---|---|
| 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 |

# ТЕХНОЛОГИЧНИ 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 технологичните 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 технологичните механизми за контрол, съгласно клауза 8 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. ДЕЙСТВИЯ И МЕТОДИ

Изборът на технологичните механизми за контрол е съгласно клауза 8 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.

### А.8.1 ПОТРЕБИТЕЛСКИ КРАЙНИ УСТРОЙСТВА

**Механизъм за контрол:** *Информацията, съхранявана на, обработвана от или достъпна чрез потребителски крайни устройства трябва да бъде защитена.*

Правилата за потребителските крайни устройства се отнася служителите на УНСС и обхващат всички устройства за обработка на данни, регулярно използвани за извършване на дейността. Тези устройства, свързвайки се със системите и мрежите на УНСС, попадат в обхвата на СУИС съгласно клауза А.8.1, като целта е информацията, която се съхранява, обработва или е достъпна чрез тези устройства да бъде защитена.

1. Видове устройства:
   1.1. Преносими компютри, собственост на УНСС.
   1.2. Стационарни компютри, собственост на УНСС.
   1.3. Мобилни телефони и таблети, собственост на УНСС.
2. УНСС е осигурил хранилище за служебна информация, включително такава, свързана с учебния процес, чиято цялост, наличност и конфиденциалност е гарантирана от въведените мерки за контрол и защита. Върху крайните устройства по подразбиране не се допуска съхранението на служебна информация, поради рискове от нейното непрекомерно разкриване и/или загуба. Всеки служител на университета носи персонална отговорност за генерираната, достъпваната, записваната, принтираната или споделена информация през

повереното му крайно устройство. Не се допуска съхранението на лична информация върху служебни устройства, както и такава, която може да бъде обект на защита, авторско право или специфични регулации /например лични данни/.

3. Крайните устройства на потребители по подразбиране са присъединени в домейн и се управляват централизирано. Изключения са допускат за устройства със стриктно изпитна цел, лаборатории, изпитни зали или друго по преценка на Мениджър ИС. За мобилните телефони и таблети е наложена минимална политика за сигурност при свързване с пощенската услуга на университета, която съдържа изисквания за заключване на устройството и минимална версия на мобилната операционна система.

4. В УНСС не се допуска инсталирането на софтуер, различен от одобрения, без знанието на Дирекция ИТ и разрешение от Мениджър ИС. Всеки служител, който има необходимост от допълнителен софтуер може да изправи заявка до Мениджър ИС, и при положително становище от отговорните лица, същият може да бъде инсталиран.

5. УНСС не допуска крайни устройства, които не са част от домейн група, да се свързват във вътрешна мрежа на университета. За целта е въведена автентификация чрез 801.1x за кабелна и безжична мрежа, която гарантира тази мярка. За потребители и устройства, които не са част от домейн група, е осигурен алтернативен безжичен интернет без достъп до вътрешните ресурси на университета.

6. За крайните станции в УНСС е прието да се използват само поддържани от техния производител операционни системи. При наличието на няколко поддържани версии от определени операционни системи е допустимо използването на която и да е от тях, в зависимост от разполагаемите лицензи, капацитет на хардуера или друго условие, което може да повлияе обновяването до съответната последна версия.

7. На всички компютри, част от домейн група, са наложени следните мерки за сигурност:

7.1. Задължителна автентификация с парола или биометрични данни. По преценка на Мениджър ИС и при идентифициране на висок риск за единични компютри може да се наложи и двуфакторна автентификация.

7.2. Инсталиран е антивирусен софтуер с централизирано управление ESET със специфична защита на конфигурацията, така че потребител дори с административни права да не може да деинсталира или спре действието му. Антивирусният софтуер изпраща известия за наличието на заплаха до централизирана конзола за по-нататъшно изследване и класифициране.

7.3. Всички компютри в УНСС, част от домейн група, са с инсталирани агенти, позволяващи анализ на потребителското поведение в реално време. Резултатите от този анализ са обект на непрекъснат мониторинг и ответни действия от отговорния персонал и/или от трета страна, имаща договор за осигуряване на услуги по наблюдение.

7.4. В УНСС не е забранено използването на преносими памети, преносими интернет карти, и други USB аксесоари.

7.5. За преносимите компютри, където няма технологични ограничения, се използва BitLocker за криптиране на дисковете им. Методът за криптиране са управлява централизирано от администраторите в УНСС, като същите са отговорни да съхраняват криптографските ключове.

7.6. За всеки компютър при който е технически възможно, се използва UEFI boot и TPM 2.0. При подмяна на техника, наличието на TPM 2.0 е част и задължително присъства, като част от спецификацията.

8. Допуска се използването на собствени устройства от страна на студенти, преподаватели и трети страни, но без достъп до информация, съхранявана на сървъри в DMZ зоната на университета, с изключение на информацията публикувана, в уеб приложения, достъпни за всички.

### А.8.2. УПРАВЛЕНИЕ НА ПРИВИЛЕГИРОВАНИ ПРАВА ЗА ДОСТЪП

**Механизъм за контрол:** *Предоставянето и използването на привилегирован достъп трябва да бъде ограничено и контролирано.*

В УНСС е въведен стриктен контрол над създаване и употребата на административни акаунти за системи и приложения. За да се минимизира риска, присъщ за акаунтите с високи привилегии, е създадена следната организация:

1. УНСС е идентифицирал и описал всички профили с високи права, като за отчетност и лесна проверка те са описани в криптиран файл.
2. Където е приложимо и технически възможно, административните акаунти са с друфакторна аутентификация.
3. Дължината на паролите на административните профили е минимум 12 символа, включващи главни, малки букви, число и специални символи.
4. Не се създават административни профили с имена по подразбиране, като admin, root и др. използвани от производители и разработчици за първоначално логване в система.
5. Акаунтите с високи привилегии са поставени с специфичен мониторинг режим в SIEM системата на УНСС, като всяко техно действие се логва и анализира за потенциално зловредно или злоумишлено поведение.
6. УНСС извършва преглед на административните акаунти, не по-малко от веднъж годишно, по време на вътрешния одит. За целта се проверяват всички административни акаунти, а не извадка от тях.
7. Използването на административни акаунти за аутентификация на приложения е сведена на минимум, като за целта УНСС се стреми да прилага Service Managed Accounts поради тяхното по-високо ниво на сигурност и невъзможност за интерактивно ползване от потребител.
8. Всеки нов административен акаунт се одобрява от Мениджър ИС, след одобрение на постъпило искане служител, партньор или друго лице, чиито задължения предполагат използването на акаунт с високи привилегии. Мениджър ИС има право да отхвърли постъпилата заявка или да поиска допълнителна информация за причините налагащи създаването на нов административен профил. Добавяне на нови акаунти към регистъра е задължение на служителя, който ги създава.
9. Липсата на информация за съществуващ, активен административен акаунт в регистъра, както и създаването/модифицирането/забраняването на административни акаунти, без операцията да е одобрена от Мениджър ИС, се считат за инциденти със сигурността.

### А.8.3. ОГРАНИЧЕНИЕ НА ДОСТЪПА ДО ИНФОРМАЦИЯ

**Механизъм за контрол:** *Достъпът до информация и системните приложения трябва да бъде ограничен в съответствие с Политиката за контрол на достъпа.*

1. УНСС поддържа ограничение на достъпа до информацията въз основа на нуждите на работния процес при работа с информация. Ограниченията са изцяло синхронизирани с политиката за достъп на УНСС.
2. За да се поддържат изискванията за ограничаване на достъпа, са в сила следните правила:

- Осигуряване на менюта за контрол на достъпа до функциите на приложната система;
- Контролиране правата за достъп на потребителите, съгласно управлявания модел за контрол на достъпа;
- Контролиране правата за достъп на други приложения.
- Групи в домейн средата, които позволяват налагането на специфични ограничения на достъпа;
- Физически ограничения за достъп – карти за контрол на достъпа, ключалки, турникети, каси за документи.

### А. 8.4. КОНТРОЛ НА ДОСТЪПА ДО ПРОГРАМЕН „СОРС КОД”

**Механизъм за контрол:** *Достъпът за четене и писане на „сорс код”, инструментите за разработка и софтуер библиотеките трябва да се управляват по подходящ начин.*

1. Достъпът до изходния код на софтуера, библиотеки и свързаните с това елементи (като проекти, спецификации) са строго контролирани, за да се предотврати въвеждането на неоторизирана функционалност и да се избегнат непреднамерени изменения, както и да се поддържа поверителността на интелектуалната собственост.
2. За изходния код това е постигнато чрез контролирано хранилище със силно ограничен достъп.

### А. 8.5. ПРОЦЕДУРИ ЗА ЗАЩИТЕНА ВРЪЗКА (SECURE LOG- ON)

**Механизъм за контрол:** *Трябва да бъдат внедрени технологии и процедури за сигурно удостоверяване въз основа на ограниченията за достъп до информация и специфичната политика по контрол на достъпа.*

1. Процедурата за включване към операционна система, и/или други информационни системи, собственост на университета, гарантира минимална възможност за неоторизиран достъп. Процедурата за сигурно влизане в система включва:

1.1. Определени са групови политики за сигурно влизане в системата;

1.2. Ограничен е броя на позволените неуспешни опити за включване към системата;

1.3. Потвърждава сигурното включване към системата само след въвеждане на всички входни данни. Ако възникне грешно условие, системата показва коя част от данните е коректна или некоректна;

1.4. Регистрират се неуспешните опити за влизане в система;

1.5. Включване на време-закъснение преди да са позволени по-нататъшни опити за включване към системата или отхвърляне на всякакви по-нататъшни опити без специално упълномощаване;

1.6. След краен брой неуспешни опити за включване в системата с потребителско име и парола, акаунта се заключва за определен период от време;

1.7. Записва се следната информация за завършване на успешно включване в системата:

- дата и време на предишното успешно включване в системата;
- подробности за всякакви неуспешни опити за включване в системата от последното успешно включване към системата;

1.8. Показва на екрана въведената парола и скрива съдържанието на паролата чрез символи;

1.9. Не се предават по мрежата пароли в явен текст.

2. УНСС прилага механизми за контрол на времето на свързване за чувствителни компютърни приложения както следва:

2.1. Разглеждане на повторно упълномощаване през определени интервали от време;

2.2. Ограничаването на периода, през който са позволени свързвания към компютърни услуги, намалява възможността за неразрешен достъп. Ограничаването на продължителността на неактивни сесии предпазва потребителите от поддържане на сесиите отворени, за да се предотврати повторна автентификация.

### А. 8.6. УПРАВЛЕНИЕ НА КАПАЦИТЕТА

**Механизъм за контрол:** *Употребата на ресурси трябва да се наблюдава и регулира в съответствие с текущите и очакваните изисквания за капацитет.*

1. УНСС е определило изисквания за капацитета за информационните системи, като общото изискване е да бъде търсен допълнителен капацитет за системи, които устойчиво са натоварени над 80% . Чрез периодични наблюдение и настройване на ползваните ресурси се правят прогнози за бъдещи изисквания към капацитета, за да се гарантира налична изчислителна мощност и памет, както и да се гарантира работоспособността и ефикасността на информационните системи.
2. При внедряване на нова информационна система, изисквания за капацитет се определят при изясняване на функциите и процесите, които ще управлява. За всяка нова започваща дейност, УНСС анализира определените изискванията за производителност.
3. Процесът на планиране на нужния капацитет за информационна система се базира на потребностите на предоставяната услуга, като УНСС използва микс от on-premise и cloud базирани информационни системи:

- Екипът разглежда на вътрешна среща необходимостта от разширяване или осигуряване на капацитет за конкретно действаща или внедряване на услуга по проект, като се прилагат нужните разяснения, спецификации и се цитира крайния срок за изпълнение;
- Мениджър ИТ взима крайното решение за доклад към ръководството въз основа на документираните изисквания към всеки проект;
- След утвърждаване на изпълнението, предложението се възлага на съответните специалисти в УНСС за изпълнение.

4. УНСС провежда превантивни действия, базирани на предварителни проучвания, нови тенденции и системните изисквания, наблюдение и анализи, за да се избегнат потенциални слаби места при осигуряване на ресурси.

## А. 8.7. КОНТРОЛИ СРЕЩУ ЗЛОНАМЕРЕН СОФТУЕР

**Механизъм за контрол:** *Трябва да бъде внедрена защита срещу злонамерен софтуер, в съчетание с подходящо осъзнаване от страна на потребителите.*

УНСС прилага ефикасни средства и механизми за откриване и защита срещу злонамерен софтуер и подходящи процедури за поддържане на високо ниво на осъзнатост. Защитата срещу злонамерения софтуер е базирана на осъзнаване на сигурността, на контролиран достъп до системите и на приетите способи за управление на измененията. Внедрени следните механизми за контрол срещу злонамерен софтуер:

1. Поддържа комплексен Анти-* софтуер за откриване на вируси, червеи, локални/отдалечени троянски коне, логически бомби и възстановяване на системата, ESET, осигуряващ политики за работа, централизирано управление, сканиране, контрол на приложенията, контрол на преносими устройства, контрол на мрежов трафик;
2. Анти-* софтуер е базиран на вече известен и регистриран злонамерен софтуер и за целта се извършва автоматично обновяване на антивирусните дефиниции и сигнатури;
3. Проверка преди ползване на всички прикачени файлове към електронната поща и на всички свалени файлове за наличие на зловреден софтуер. Тази проверка се извършва на различни места: на обслужващите шлюзове за електронна поща, на сървърните системи, на настолни и преносими компютри или когато електронното съобщение постъпва в мрежата на УНСС;
4. Периодично се сканират за наличие на злонамерен софтуер части от или цели информационни системи;
5. Невъзможно е прекъсване на действието на интегрираните софтуерни продукти за откриване и защита на и от злонамерен софтуер.

## А. 8.8. УПРАВЛЕНИЕ НА ТЕХНИЧЕСКАТА УЯЗВИМОСТ

**Механизъм за контрол:** *Трябва да бъде получена навременна информация за техническа уязвимост на използваните информационни системи, излагането на УНСС на такава уязвимост трябва да бъде оценено и трябва да бъдат взети мерки, за да се разгледа свързаният с това риск.*

За да е ефективен контрола, при идентифициране на потенциална техническа уязвимост се следват следните указания:

1. УНСС е определило и установило задачи и отговорности, свързани с управление на техническата уязвимост, включващи наблюдение на уязвимостта, оценка на риска от уязвимост, коригиране на уязвими места, проследяване на активи и всякакви необходими отговорности по координиране;
2. Rapid7 е определен за инструмент за идентифициране на технически уязвимости и за поддържане на осведоменост за това. Поддържа се статистика за измененията и тенденциите в броя и сериозността на откритите уязвимости;
3. За публичните и вътрешните уеб базирани приложения могат да се прилагат множество инструменти или комбинация от тях, в зависимост от спецификата и сложността на изследваното приложение. Одобрени за целта в УНСС са инструментите Burp, Qualys WAS, Rapid7 AppSpider, като посочените могат да се използват без да се налага специално одобрение.
4. Подхода при отстраняването на открити уязвимости е първо да се отстраняват тези с висока степен на опасност от системите с висока важност за университета – това са системите и услугите, присъстващи в риск регистъра.
   4.1. Отстраняването на уязвимости може да бъде разглеждането в определени случаи, като част от процеса по управление на промени, като в тези случи се реферира към изискванията на клауза А.8.32. Изключение от процеса по управление на промени представялата следните видове уязвимости:
   - Уязвимости, засягащи работни станции
   - Уязвимости, засягащи тестови среди или среди за разработка
   - Налагане на месечни и извънредни обновявания от Microsoft
   - Регулярно обновяване на приложен софтуер по работни станции – Chrome, Mozilla, Adobe и др.

   4.2. Отстраняването на уязвимости чрез hardening на операционни системи или приложения, обновяване на модули за уеб приложения и сървъри, бекъп софтуер, firmware, виртуализация, софтуер за защита или друго, което може да засегне работоспособността на системата, се извършва като част от процеса по управление на промени.
5. Осигурена е възможност за реакция на предупреждения за потенциална техническа уязвимост, чрез получаване на специализирани бюлетини за сигурност, отворени канали за докладване от трети страни, бюлетини с новини от производителите на хардуер/софтуер;
6. При регистриране на потенциална техническа уязвимост УНСС определя свързаните с нея рискове и предприема коригиращи действия;
7. В зависимост от това колко спешно трябва да бъде разгледана техническата уязвимост предприетите действия трябва да бъдат извършени в съответствие с изискванията за сигурност;
8. При актуализиране на софтуерен пакет се оценяват рисковете, свързани с актуализацията. Обновяването и/или надстройването на софтуерен пакет се изпитва и оценява преди внедряването му в експлоатационната среда;
9. Ако няма възможност за актуализиране на софтуерния пакет/firmware са предвидени други механизми за контрол:
   - Деактивират се услуги и/или функции, свързани с уязвимостта;

- Преконфигурират се или се добавят механизми за контрол на достъпа;
- Засилва се наблюдението, за да се открият или предотвратят действителни атаки;
- Повишава се вниманието към конкретна уязвимост;

10. Поддържат се контролни записи за действията, свързани с отстраняването на уязвимости;
11. Преки отговорности за процеса имат:

- Мениджър ИС – за приоритизиране на откритите уязвимости, както и последваща проверка за тяхното и успешно отстраняване.
- Мениджър ИТ – за извършването на планирани действия по отстраняване, осигуряване на непрекъсваемост на работата в УНСС при управлението на уязвимости.

12. Процесът на управление на техническа уязвимост е редовно наблюдаван и оценяван, за да се гарантира неговата резултатност и ефективност.

## А. 8.9. УПРАВЛЕНИЕ НА КОНФИГУРАЦИЯТА

**Механизъм за контрол:** *Конфигурации, включително конфигурации за сигурност, на хардуер, софтуер, услуги и мрежи трябва да бъдат установени, документирани, внедрени, наблюдавани и преглеждани.*

I. УНСС е дефинирал и внедрил минимални изисквания по отношение на конфигурациите за сигурност на системите и устройствата използвани за дейността. Специфични изисквания за сигурност може да бъдат определяни извън тази процедура в отделен документ, касаещ конкретна система, приложение или съвкупност от такива. Независимо дали се адресират общи или специфични изисквания за управление на конфигурацията, реда за вземане на решения и отговорности е следния:

1. Решения за създаване и/или промяна на базови изисквания към сигурността се взимат от СИС по предложение на Мениджър ИТ и предварително съгласувани с Мениджър ИС.
2. При промяна или създаване на нови базови изисквания за сигурност, задължение е на Мениджър ИС да уведоми всички заинтересовани страни за наличието на промени или нови изисквания по отношение сигурността.
3. Базови изисквания към конфигурациите, наложени от относима за дейността на УНСС нормативна уредба /Наредби, Закони, Директиви и др./, се приемат от СИС, без да е необходимо предварително съгласуване. Задължението да внесе в дневния ред на СИС приемането на тези промени е на Мениджър на СУИС.

II. За целите на поддържане на минимални мерки за сигурност УНСС е определила следните общи правила:

1. Firmware – допуска се използването на firmware с до 2 версии назад в хронологията с обновявания от съответния производител.
2. За всички устройства, софтуер, firmware или друго, което може да попадне в обхвата на тази точка, задължително е да се смени потребителските профили по подразбиране /admin, root, master, и т.н./ .
3. За всички устройства, софтуер, firmware или друго, което може да попадне в обхвата на тази точка, се създават минималния допустим за нормалната работа административни профили. Същите са контролирано разпространявани и описание по реда на т. 8.2.
4. Вътрешни или външни услуги /портове, приложения, сървъри/, които не се използват следва да бъдат спрени. Активирането им може да се осъществи по методите на управление на промените в т. 8.32.

5. Акаунти с високи привилегии, които не са използвани повече от 90 дни следва да бъдат спрени, а след 12 месеца изтрити от съответната система.
6. За услугите с висока важност /вътрешни или външни/ винаги да се прилага разделение контрол над мрежовия достъп, чрез сегментация. VLAN правила, PAM или друго средство, което да ограничи достъпа до тях до възможния минимум.
7. В УНСС всички часовници на IT активи и устройства, следва да са синхронизирани с един и също time server.
8. Задължение на Мениджър ИТ е да осигури съответствие между закупените лицензи /от всякакъв вид/ и реално използваните за дейността на университета. Максималното допустимо отклонение не може да надхвърля 5% /наложително поради клониране на машини, тестови машини и др/ от общия брой закупени/употребявани лицензи, като над този процент Мениджър ИТ информира ръководството за необходимостта от закупуването на нови такива.

## А. 8.10. ИЗТРИВАНЕ НА ИНФОРМАЦИЯТА

**Механизъм за контрол:** *Информацията, съхранявана в информационни системи, устройства или други носители за съхранение, трябва да се изтрива, когато вече не е необходима.*

I. Сигурното изтриване на информация, известно още като саниране на данни, е критичен процес, който гарантира, че чувствителните данни се премахват трайно и безвъзвратно от устройствата за съхранение или системите, когато вече не са необходими. В обхвата на тази точка попадат всички устройства и системи за съхранение, с изключение на оперативните и архивни данни, които УНСС трябва да съхранява, поддържа и обработва съгласно местно и между народно законодателство. Идентифицирането на тези данни е задължение на Дирекция правно и нормативно обслужване в университета, който предоставя на Мениджър ИС и на Мениджър ИТ списък с видовете, локациите и сроковете за съхранение на такива типове данни. Списъкът се обновява незабавно при промяна в законодателство или обстоятелства които могат да окажат влияние.

1. Ръководната роля при управлението на процеса на планирано изтриване на информация е на Мениджър ИС, като в него участват още:
    - Собственици на данни – за да идентифицират и класифицират чувствителните данни за изтриване.
    - ИТ администратори - изпълняват процеса на сигурно изтриване.
    - Служител от правна дирекция за осигуряване спазването на разпоредбите за защита на данните и вътрешните политики.
2. Избрани методи подходящи за сигурно изтриване на данни в зависимост от типа на устройството за съхранение или системата са:
    - Презаписване - презаписване на данните с произволни стойности или нули, за да не могат да бъдат възстановени. Този метод се използва от УНСС при преинсталиране/нулиране на операционни системи и специфични устройства.
    - Сигурно изтриване - използват се софтуерни или хардуерни инструменти, предназначени за сигурно изтриване на данни. Този метод се използва от УНСС при системи, съхраняващи данни с висока чувствителност, в случаите в които те ще се бракуват, продават, преотстъпват или при друго обстоятелство, което може да позволи достъп до тези данни.
    - Физическо унищожаване - физическо унищожаване на носителите за съхранение (напр. нарязване, унищожаване). Този метод се използва от УНСС при унищожаване на

устройства за съхранение на информация – дискове, CD, флаш памети, хартиени копие и др.

- Изтриване на ключове за криптиране – при наличието на опасност от компрометиране на криптирани данни /например след кражба, загубва, и др./ като част от мерките за сигурност, може да се използват и изтриването на ключовете за криптиране, съхранявани от УНСС. Решението за използване на този метод е на Мениджър ИС.

3. Документация и записи за процеса на безопасно изтриване включва само планирани, координирани и одобрени от Мениджър ИС действия. Изтриването на информация при извършване на ежедневна поддръжка на мобилни и стационарни компютри, мобилни телефони, преносими памети и др., при преинсталиране, смяна на диск, заплаха от зловреден код, НЕ са обект на регулации от тази клауза. За планираните действия следва да се документира минимум:
   - Дата и час на изтриването.
   - Описание на изтритите данни.
   - Метод, използван за изтриване.
   - Резултати от проверката.
   - Персонал, отговорен за изтриването.
4. Задължение за уведомяването на заинтересованите страни за успешно извършено планирано изтриване на данни е на Мениджър ИС.

## А. 8.11. МАСКИРАНЕ НА ИНФОРМАЦИЯТА

**Механизъм за контрол:** *Маскирането на данни трябва да се използва в съответствие със специфичната политика на УНСС за контрол на достъпа и други свързани специфични политики и бизнес изисквания, като се вземе предвид и приложимото законодателство.*

1. В УНСС се ползва подход за маскирането на данни, известно още като псевдонимизирани и анонимизиране на данни, в съответствие с актуалната „Политика по защита на лични данни“. Отговорност за изпълнение изискванията на тази клауза носят:
   - Служител по защита на данните (DPO, като единствено отговорен за надзора на дейностите по защита на данните, включително маскиране на данни
   - Мениджър ИС за одобряване и проверка за адекватност на мерките за защита на данните.
   - Мениджър ИТ за прилагането им по отношение на информационните системи.
2. В УНСС могат да се използват различни мерки за маскиране на данни в зависимост от конкретните технически или функционални ограничения. Избраните подходи са следните:

- Токенизация – при замяна на персонална информация данни с токени;
- Замяна на личните данни с фиктивни, но структурно подобни данни – подходящи за целите на тестове и разработки на нови системи, особено когато са привлечени трети страни в този процес.
- Обобщаване на данни с цел довеждане до невъзможност да се идентифицира единичен субект от тях – за изготвяне на статистически анализи за обучение, движения на студенти и преподаватели в университета, настанявания в общежития, изпити или за други цели.
- Криптиране на данни, като универсален начин да се запази тяхната конфиденциалност. Метода е особено подходящ в случаите, в които се налага УНСС да съхранява чувствителни данни за свои кандидат студенти, студенти, преподаватели, административни служители и др. Минималната използвана криптография в тези случаи следва да е AES-256.

### А. 8.12. ПРЕДОТВРАТЯВАНЕ ИЗТИЧАНЕТО НА ДАННИ

**Механизъм за контрол:** *Мерките за предотвратяване изтичането на данни трябва да се прилагат към системи, мрежи и всякакви други устройства, които обработват, съхраняват или предават чувствителна информация*

1. В УНСС са въведени комбинация от контролни механизми, които имат за цел да предотвратят или да известят отговорните служители за потенциален риск от изтичане информация и/или неоторизиран достъп. Те включват следните мерки:
    - Акаунтите на потребителите и техните действия се наблюдават от специализирана система за анализ на поведението им /SIEM/;
    - Въведени са ограничения за достъп до известни публични услуги, които биха могли да се използват за нерегламентирано споделяне на данни;
    - Чувствителната/конфиденциалната информация се съхранява на определени за това места, с ограничен достъп до нея – само до служителите имащи работа с тази информация.
    - Криптирани са дисковете на преносимите компютри собственост на УНСС, за да се предотврати възможността от изтичане на данни в случай на кражба или загуба им.

### А. 8.13. РЕЗЕРВИРАНЕ НА ИНФОРМАЦИЯТА

**Механизъм за контрол:** *Трябва да бъдат направени и редовно проверявани резервни копия на информация и софтуер в съответствие с договорената политика за резервиране.*

1. УНСС е внедрил подходящи средства за резервиране, с което се гарантира, че цялата критичната информация и софтуер могат да бъдат възстановени след инцидент по сигурността, злополука или повреда в оперативните носители. Процеса на резервиране на информацията е изцяло съобразен с хардуерни отпадания, софтуерни сривове, инцидентни изтривания на информация, некоректни или неоторизирани модификации на информацията и злонамерени действия. Ръководството на УНСС осъзнава, че тези заплахи са неизбежни.

2. Процеса на резервиране и възстановяване се извършва в съответствие с актуалната версия на График за архивиране и унищожаване да данни. Но включва минимум следното:
    - Осигуряване на наличност на оперативната информация, съхранявана и обработвана от системите чрез осигуряване на допълнителни дублиращи твърди дискови носители;
    - Динамичното разпределяне на информацията върху няколко носителя и поддържане на повече от едно актуално копие увеличава толеранса при грешка;
    - Работните файлове от всички локални значими за УНСС системи се резервират периодично върху определено за целта пространство;
    - Резервирането на информация може да се извършва, както в реално време, така и в пакетен режим при зададено събитие или дефинирано време по според преценката на Мениджър ИТ и Мениджър ИС;
    - Достъпа до резервните копия е стриктно контролиран и ограничен до малък брой служители;
    - Резервните копия се проверяват автоматично за интегритет, а когато е възможно се изпитват периодично, за да е сигурно, че може да се разчита на тях за използване при спешни и непредвидени случаи, когато е необходимо;
    - Избраните методи за резервиране гарантират възстановяване на системите;

- Избрана е схема, при която определена информация с ниво на чувствителност Ниво 0, 1, 2, 3, налична на определени системи, се резервира;
- Поддържат се точни и пълни описи на версиите и локациите на резервните копия;
- Резервните копия се съхраняват по начин, осигуряващ нужната степен на физическа защита и защита от влияние на околната среда, включително в изнесена облачна среда;
- Възстановяването на информация се извършва от Специалист/Системен администратор, имащ право да борави с конкретното ниво на класификация;
- Процеса за резервиране е редовно проверяван и изпитван, за да е сигурно, че последователността и действията в него са ефективни и че могат да бъдат завършени за времето, определено в плана за непрекъсваемост;

3. Процеса на резервиране и възстановяване включва:

- Осигуряване на наличност на оперативната информация, съхранявана и обработвана от системите чрез осигуряване на допълнителни дублиращи копия на независими системи – сториджи и сървъри;
- Динамичното разпределяне на информацията върху няколко системи и поддържане на повече от едно актуално копие;
- Въпреки че този процес на резервиране е изцяло автоматизиран, възстановяването на информация изисква допълнителна намеса на Специалист;
- Възстановяването на отделни файлове се извършва от Специалист, с поредица от команди за копиране на повредения или унищожения файл от определения за съхранение актив към засегнатата информационна система;
- Този метод на резервиране гарантира наличието на информацията на няколко различни локации.
- Поддържат се точни и пълни описи на ползваните резервни копия за основното и резервното място;
- Резервните копия се съхраняват по начин, осигуряващ нужната степен на физическа защита и защита от влияние на околната среда;
- Резервните носители се изпитват периодично на 12 месеца, за да е сигурно, че може да се разчита на тях за използване при спешни и непредвидени случаи, когато е необходимо;
- Възстановяването на информация се извършва от Специалист/Системен администратор, имащ право да борави с конкретното ниво на класификация.

4. Процеса за резервиране е редовно проверяван и изпитван, за да е сигурно, че последователността и действията в него са ефективни и че могат да бъдат завършени за времето, определено в плана за непрекъсваемост.

### А. 8.14. НАЛИЧНОСТ НА СРЕДСТВА ЗА ОБРАБОТКА НА ИНФОРМАЦИЯ

**Механизъм за контрол:** *Средствата за обработка на информацията трябва да бъдат внедрени с достатъчна наличност, за да се отговори на изискванията за наличност.*

1. При критични информационни системи оборудването е осигурено достатъчно, за да се отговори на изисквания за достъпност и наличност на системата.
2. УНСС е идентифицирал изисквания за достъпността на информационните системи. Когато наличието не може да се гарантира използването на съществуващите системи и оборудване, университета полага усилия за навременно осигуряване на компоненти или подобрения в архитектура от системата. Плановете за подобрение са отбелязани в целите на СУИС.

3. Когато е приложимо и са налични, дублираните информационни системи и оборудване са тествани, за да се гарантира, нормалната миграция при срив от един компонент към друг компонент и същите са по предвиденото предназначение.
4. Изпълнението на дейностите по достатъчно дублиране и осигуряване може да въведе рискове за целостта или поверителността на съществуващата информацията и функциониращите информационни системи, които трябва да се вземат предвид при проектирането им.
5. УНСС е осигурило резервно захранване с електроенергия чрез UPS и генератор, които позволяват университета да запази работоспособността си дори при продължителни спирания не електроподаването.
6. Осигурени са няколко доставчика на интернет свързаност с цел реализирането на висока надеждност на достъп до услугите на университета.

### А. 8.15. РЕГИСТРИРАНЕ НА СЪБИТИЯ

**Механизъм за контрол:** *Логове, които записват дейности, изключения, грешки и други съответни събития, трябва да бъдат създадени, съхранявани, защитени и анализирани.*

1. В УНСС лог файловете, съдържащи записи за действията на потребителите, изключения и пробиви в сигурността, се попълват и пазят в система Rapid7 за период от минимум 12 /дванадесет/ месеца, за да послужат като доказателство при евентуално разследване и наблюдение над контрола за достъп. Контролните записи включват:
   - Уникални потребителски имена или идентификатори;
   - Дата, време и подробности за важни събития, например включване и изключване;
   - Идентификация на крайното устройство или местоположение, ако е възможно;
   - Записи на успешни и отхвърлени от системата опити за достъп;
   - Записи за успешни и отхвърлени данни и други опити за достъп до ресурси;
   - Изменения на системната конфигурация;
   - Използване на привилегии;
   - Мрежови адреси и протоколи;
   - Активиране и деактивиране на системи на модули за защита
   - Нерегламентирано сваляне или споделяне на съдържание

2. Налични са хранилища за всички регистрирани събития. УНСС и управлението на виртуалното хранилище, както и контрола на съдържанието и анализирането на регистрираните събития, е отговорност на Мениджър ИС. Специалистите нямат право да изтриват, деактивират или модифицират записи от виртуалното хранилище.

### А. 8.16. НАБЛЮДЕНИЕ НА ДЕЙНОСТТА

**Механизъм за контрол:** *Мрежите, системите и приложенията би трябвало да бъдат подложени на мониторинг за аномално поведение и да се предприемат подходящи действия за оценяване на потенциалните инциденти, свързани със сигурността на информацията*

1. При процеса по наблюдение се акцентира на:
   - Разрешен достъп и следните подробности: уникални потребителски имена или идентификатори, дата и време на ключови събития, тип на събитията, файлове, до които е осъществен достъп, използвани програми/помощни програми;

- Всички привилегировани операции: използване на привилегировани акаунти на системен администратор, специалист и оператор, стартиране, рестартиране и спиране на информационната система;
- Всички опити за неразрешен достъп: грешни и отхвърлени действия на потребителя, грешни и отхвърлени действия, включващи данни и други ресурси, нарушения на политиката за достъп и предупреждения за междумрежови интерфейси и защитни стени, предупредителни сигнали от собствени системи за откриване на несанкциониран достъп;
- Изменения в или опити за изменение на настройките и механизмите за контрол на сигурността.

2. Внедрените механизми за защита на информационните логове предпазват регистрираните събития от неоторизирано разкриване, модификация и заличаване. При защитата на информацията от логовете се следи за:

- Достъпът до регистрираните логове да е ограничен;
- Преглед на съдържанието на логовете да се осъществява от Мениджър ИС и съответния специалист с подходяща квалификация.
- УНСС приема за достатъчна информацията, записвана в лог от съответната система в централизирано локално и/или облачно хранилище на данни. Записите включват минимум:
- Времето, когато се е случило успешно или неуспешно събитие;
- Информация за събитието или грешката;
- Кой акаунт и кой администратор / специалист са участвали.

3. УНСС е внедрил механизми за наблюдение на дейността в контекста на потребители и системи. Въведени са технически контроли за отчетност и наблюдение, които включват:

- изходящ и входящ мрежов, системен и приложен трафик;
- достъп до системи, сървъри, мрежово оборудване, система за наблюдение, критични приложения и др.;
- системни и мрежови конфигурационни файлове от критично или административно ниво;
- регистрационни файлове от инструменти за сигурност /антивирусна програма, IDS, система за предотвратяване на проникване (IPS), уеб филтри, защитни стени/;
- дневници на събития, свързани със системна и мрежова активност;
- използване на ресурсите (напр. CPU, твърди дискове, памет, честотна лента) и тяхната производителност.
- Установена е базова линия /security baseline/ на нормално поведение и се наблюдават отклоненията спрямо тази базова линия
- Преглед на използването на системите в нормални и пикови периоди;
- Обичайно време на достъп, местоположение на достъп, честота на достъп за всеки потребител или група потребители.
- поведение, като например:
- дейност, обикновено свързана със злонамерен софтуер или трафик, произхождащ от известни злонамерени IP адреси или мрежови домейни (напр. тези, свързани със сървъри за управление и контрол на ботнет);
- известни характеристики на атака /напр. отказ на услуга и препълване на буфер/;
- необичайно поведение на системата /инжектиране на процес и отклонения в използването на стандартни протоколи/;

- Тесни места и претоварвания /напр. опашка в мрежата, нива на латентност и мрежово трептене/;
- Неоторизиран достъп (действителен или опитен) до системи или информация;
- Неоторизирано сканиране на бизнес приложения, системи и мрежи;
- Успешни и неуспешни опити за достъп до защитени ресурси /напр. DNS сървъри, уеб портали и файлови системи/;
- Необичайно поведение на потребители и системи по отношение на очакваното поведение.

4. Анормалните събития се регистрират като инциденти и се съобщават на съответните заинтересовани страни след одобрение на Мениджър ИС. Крайната цел на процеса по наблюдение е подобрение на:
   - Възможностите за одит
   - Оценка на риска
   - Подобряване на процесна по реагиране на инциденти
   - Свеждане до минимум ефекта от нежелани събития
   - Идентифициране н намаляване до минимум т.н. False positives /фалшиво положителни резултати/, които могат да доведат до пренебрегване на реални заплахи за дейността на УНСС.

### А. 8.17. СИНХРОНИЗАЦИЯ НА ЧАСОВНИЦИТЕ

**Механизъм за контрол:** *Часовниците на всички системи за обработка на информация в УНСС или зоната за сигурност трябва да бъдат синхронизирани с договорен източник на точно време.*

1. Правилното настройване на системните часовници е важно за осигуряване на точност на записите от проверката, които може да се изискват за изследване или за доказателство в правни или дисциплинарни случаи. Неточните записи от проверка могат да възпрепятстват такива разследвания и да навредят на правдоподобността на такива данни.
2. За целта всички часовници за реално време на информационни системи в УНСС са сверени и синхронизирани, съгласно координирано универсално време (UTC) или местно стандартно време. Процесът на синхронизиране е изцяло автоматизиран. Използван е мрежов протокол за време с едно и също NTP за всички активи, за да се поддържат всички часовници в синхрон.

### А. 8.18. ИЗПОЛЗВАНЕ НА СИСТЕМНИ СРЕДСТВА

**Механизъм за контрол:** *Използването на обслужващи програми, които могат да прескочат контролите на системата и приложенията трябва да бъде стриктно и строго контролирано.*

1. При конфигуриране и ползване на системни средства, в УНСС се следват следните указания:
   - Прилагане на процедури за идентификация, автентификация и оторизация при ползване на всяко системно средство;
   - Отделяне на системните средства от приложния софтуер;
   - Ограничаване ползването на системни средства до минимален брой доверени упълномощени потребители;
   - Упълномощаване за инцидентно ползване на системни средства;
   - Ограничаване възможността за достъп до системни средства;
   - Регистриране на всяко ползване на системни средства;
   - Определяне и документиране на нива на упълномощаване за ползване на системни средства;

- Премахване или спиране от действие на всички ненужни, софтуерни обслужващи програми и системен софтуер;

2. Всички системни сервизни програми, които биха могли да преодолеят механизмите за контрол на системата или приложението, са контролирани.

### А. 8.19. ИНСТАЛИРАНЕ НА СОФТУЕР НА РАБОТЕЩИ СИСТЕМИ

**Механизъм за контрол:** *Трябва да бъдат внедрени процедури за контрол на инсталацията на софтуер на работещите системи.*

1. УНСС контролира измененията, направени върху експлоатационния софтуер, поддържащ конкретни бизнес функции и процеси. За да се минимизира риска при неконтролирани изменения, водещи до отказ на части от или цяла система, е акцентирано върху:
   - Инсталиране, надграждане или обновяване на експлоатационен софтуер, приложение и/или програмна библиотека се извършва само от квалифициран персонал, изрично упълномощен от ръководството на УНСС да извършва тази дейност. Упълномощаването се извършва чрез длъжностни характеристики, вътрешен правилник или други официални документи на УНСС;
   - УНСС поддържа технически ограничения, които не позволяват на потребители извън групата на Administrator/Root да извършват изменения;
   - Преди всяко изменение се разработва стратегия за сигурно и гарантирано възстановяване на състоянието на системата преди началото на измененията;
   - Всички действия по изменения присъстват в audit log на съответната платформа;
   - Всеки закупен софтуер, ползван върху експлоатационните системи, е обслужван на ниво, поддържано от доставчика.
   - Всяко решение за мигриране към по-нова версия отчита сигурността на новата версия, т.е. въвеждането на нова функционалност за сигурност или броя и сериозността на проблемите със сигурността, засягащи тази версия;
   - Физически и/или логически достъп се предоставя, на доставчиците, само за целите на поддръжката, когато е необходимо и с одобрение на ръководството на УНСС;
   - Действията на доставчика са наблюдавани;
   - Операционните системи се надграждат, когато има бизнес необходимост.

Процесите по контрол на измененията се одобряват, управляват и наблюдават от Мениджър ИС.

### А. 8.20. МЕХАНИЗМИ ЗА КОНТРОЛ НА МРЕЖИ

**Механизъм за контрол:** *Мрежите и мрежовите устройства трябва да бъдат защитени, управлявани и контролирани, за да се защити информацията в системите и приложенията.*

1. УНСС е оценило, че комуникирането на информация през не защитени мрежи е риск за сигурността. За всички външни услуги, използвани в УНСС, е форсирано използване на TLS 1.2 като не се допуска използването на по-стари версии, освен в случаите когато временно трябва да се осигури работоспособността на legacy системи. В случай, че такава мярка се налага, тя се случва с разрешението на Мениджър ИС и е ограничена по време.
2. Данните за аутентификация по подразбиране, предоставени от производителя, се сменят в момента, в който мрежово устройство се въведе в експлоатация в мрежата на университета.

### А. 8.21. СИГУРНОСТ НА МРЕЖОВИ УСЛУГИ

**Механизъм за контрол:** *Характеристиките на сигурността, нивата на услугата и изискванията за управление на всички мрежови услуги трябва да бъдат определени и включени във всяко споразумение за мрежови услуги, независимо от това дали тези услуги се предоставят от самата организация или от външна организация.*

Ръководството редовно наблюдава своите способности за управление на собствените си мрежови услуги, както и способността на доставчика на мрежови услуги да управлява договорените услуги по сигурен начин. Договорени са споразумения по сигурността, нивата на услугите, изисквания за управление и правото на одит. УНСС гарантира, че доставчиците на мрежови услуги прилагат договорените мерки.

Особености на сигурността при използваните мрежови технологии, техники и технически параметри:

- Интернет свързаност. За нуждите на дейността се използват управлявани маршрутизиращи устройства, посредством което се осъществява Интернет свързаност на цялата организация;
- Безжични комуникации. В УНСС са използвани безжични мрежови свързвания, базирани на стандарта IEEE 802.11n/ac технология, ползващи 2.4 GHz или 5 GHz честотен спектър и WEP протокол за криптиране с алгоритъм WPA2 с AES 256bit. Служителите, работещи от разстояние /домашни условия/, са инструктирани да ползват същите сигурни протоколи за криптиране на безжичната връзка.
- Виртуални частни мрежи. УНСС използва VPN, за да изгради защитен „тунел" между инфраструктурата на свои клиенти и служители на УНСС. Реализацията на „тунела" е чрез SSL VPN или IPSec и осигурява процеса на автентификация и сигурното транспортиране на данни през незащитени и несигурни междинни комуникационни мрежи. За да осигури „тунелираната" информация, УНСС е внедрила протокола IPSec за нуждите на автентификацията и криптирането. Отдаленият достъп се реализира посредством иницииране на защитен „тунел" от отдаленото място, чрез софтуерен VPN клиент към съответното мрежово устройство /рутер, защитна стена/. За целите на автентификацията се използват уникално потребителско име с кореспондираща парола и сертификат, които се проверяват при всеки опит за връзка. Успешното терминиране дава възможност на отдалечения потребител да използва ресурси в локалната мрежа на УНСС. С трети страни обменът на данни може да се осъществява, както през SSL VPN, така и през изградени тунели по IPSec протокол.
- Маршрутизиране – вписани статични маршрути на управляваните класове мрежи и подмрежи за всеки сценарий, в който това е възможно;
- Транслиране на мрежови адреси. УНСС използва технологията за транслиране на мрежови адреси, чрез което идентичността на вътрешните ресурси остава неразкрита. Прилаганата технология, съобразена с RFC1918, позволява на УНСС да използва всички частни IP адреси, споменати в стандарта.
- Сигурност на електронните съобщения. УНСС подсигурява електронните съобщения чрез криптиране на комуникацията чрез TLS 1.3 в Microsoft 365.

### А. 8.22. РАЗДЕЛЯНЕ В МРЕЖИТЕ

**Механизъм за контрол:** *Групите информационни услуги, потребителите и информационните системи трябва да бъдат разделени в мрежи.*

1. УНСС поддържа комплексна комуникационна среда. За да се управлява и контролира прозрачно, мрежата на УНСС е приела два основни принципа:
   - Вътрешна мрежа, която притежава най-ниско ниво на сигурност;
   - Външна мрежа, която притежава най-високо ниво на сигурност.

2. Логическото поделяне е реализирано чрез маршрутизатори, които на база зададените правила, контролират целия мрежови трафик между сегментите/зоните и блокира неразрешения трафик. Допълнително виртуално разделяне е реализирано на вътрешната мрежа. Логическото поделяне е в синхрон с политиката за контрол на достъпа.
3. Поддържа се актуална схема на свързаността – мрежова диаграма, която отразява текущите правила. За удобство и прегледност и с цел проследяемост се пазят архивни копия на минимум две предходни версии на мрежовите диаграми.
4. Правилата за рутиране между различните мрежови сегменти са отразени в мрежовите диаграми.

### А. 8.23. ФИЛТРИРАНЕ НА УЕБ СЪДЪРЖАНИЕТО

**Механизъм за контрол:** *Достъпът до външни уебсайтове трябва да се управлява, за да се намали риска от злонамерено съдържание.*

1. Трафикът между отделните системи и техните подсистеми е контролиран чрез подходящо филтриране (по IP адрес, по протокол, по номер на порт от Transmission Control Protocol (TCP)/Internet Protocol (IP) стека и т. н.).
2. Филтрирането на трафика за потребителите обхваща следните задължителни направления:
   - Забранен е достъп до сайтове с лоша репутация, чрез NGFW и/или чрез endpoint софутер инсталиран на потребителските компютри;
   - Ограничаване на уеб трафик от геолокации, които не са типични за дейността на УНСС;
   - Специални внимание се обръча на известяване, анализиране и блокиране на command and control сървъри за зловредна активност;
   - Забранен е достъпа до сайтове с нелегално съдържание /торент тракери, сайтове за нелицензиран софтуер и т.б./
3. Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) са забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика. IP периметъра на университета се наблюдава непрекъснато от специализирани инструменти за да се извести Мениджър ИС за наличието на нови или променени услуги /портове/.

### А. 8.24. ИЗПОЛЗВАНЕ НА КРИПТОГРАФИЯ

**Механизъм за контрол:** *Трябва да се определят и да се прилагат правила за ефективно използване на криптография, включително управление на криптографски ключове.*

1. УНСС е утвърдило настоящата политика за ползване на криптографски контроли. Тя регламентира ползването на избрани криптографски методи и техники при съхранение и предаване на информация, във форма, възможна за четене и обработване само от пре-определен обект (информационна система, база данни, приложение, файл и т.н.) или субект (потребител, информационна система, приложение и т.н.). Политиката обхваща системи, приложения, бази данни, файлове, смарт карти и потребители, които участват в съхранението и предаването на информация в неявен вид. Отговорността за разработване, внедряване и поддържане на актуална

политика за ползване на криптографски контроли е на Мениджър ИС. С утвърждаването ѝ се определят следните правила:

- Идентифицирани са криптографски механизми с конкретни технически параметри и тяхната спецификация;
- Използваните криптографски алгоритми и протоколи трябва да отговарят на признати в индустрията стандарти, като Advanced Encryption Standard (AES), RSA и Transport Layer Security (TLS);
- Дължината на използваните криптографски ключове трябва да е подходяща за предвидения случай на използване и да е с дължина най-малко 256 бита;
- Забранено е използването на слаби алгоритми за криптиране, като например Data Encryption Standard (DES) или Triple DES (3DES). Както и TLS 1.0. По възможност се използват само TLS 1.2 и 1.3, като всяко изключение следва да е документирано като риск;
- Всички криптографски ключове се генерират, съхраняват и управляват по сигурен начин. Ключовете не се споделят или съхраняват в обикновен текст или на несигурни устройства, като например лаптопи или мобилни устройства;
- Където е приложимо, ротацията на ключовете трябва да се извършва периодично и в съответствие с политиката за управление на ключовете на УНСС;
- Всички криптографски реализации трябва да се тестват редовно за уязвимости и съответствие с политиките и стандартите на УНСС;
- Забранено е използването на криптографски софтуер, инструменти или устройства, които не са одобрени от УНСС;
- Криптографията трябва да се използва заедно с други средства за контрол на сигурността, като контрол на достъпа, сегментиране на мрежата и защитни стени, за да се осигури защита в дълбочина;
- Всички предполагаеми или потвърдени криптографски инциденти със сигурността трябва незабавно да се докладват на екипа по сигурността за разследване и отстраняване на нередностите;
- Ползваните криптографски системи осигуряват:
- Поверителност – прави информацията неразбираема за всички с изключение на адресатите, за които е предназначена;
- Цялостност – гарантира, че данните не са променени по неоторизиран начин от момента, в които са били създадени, предадени или съхранени;
- Автентичност – проверява идентичността на субекта или обекта, който е генерирал информацията;
- Невъзможност за отричане – гарантира, че автора не може да се откаже от направеното електронно изявление;
- Подходът към управление на криптографски ключове включва методи за третиране на криптографски ключове и възстановяване на криптирана информация в случай на загубени, изложени на риск или повредени ключове;
- Отговорността за управлението на криптографските ключове е изцяло под контрола на Мениджър ИС;
- УНСС е приела да ползва всички международни стандарти, регламентиращи криптографската сигурност;
- УНСС спазва действащото законодателство, относно криптографската сигурност;

- При ползване на криптирана информация е отчетено влиянието върху механизмите за контрол, които разчитат на проверка на съдържанието.

2. УНСС поддържа актуална тази политика за криптографски контрол, за да минимизира рисковете при ползване на криптографски техники и за да се избегне неподходящо или неправилно ползване.

### А. 8. 25. ИНФОРМАЦИОННА СИГУРНОСТ В ПРОЦЕСА НА РАЗРАБОТКАТА

**Механизъм за контрол:** *Трябва да се създадат и да се прилагат правила за сигурно разработване на софтуер и системи.*

1. В рамките на УНСС са установени и приложени правила за разработка на софтуер и системи. В процеса се вземат под внимание следните аспекти:
   - гарантиране сигурността на средата за разработване;
   - прилагане указания за сигурността по време на жизнения цикъл;
   - изисквания за сигурност, определени във фазата на проектиране;
   - проверка на сигурността в ключови етапи на проекта;
   - защитена среда за вече разработения и проверен код;
   - сигурност при контрол на версиите;
   - разбиране от страна на разработващия екип на изискванията за сигурност към приложението;
   - използване на познанията на разработващия екип за избягване, намиране и поправяне на уязвимости
2. В процеса на разработка УНСС използва дългогодишния опит на членовете в екипа по отношение на разработката. Използва се уникално създаден за целта код, базиран на отворени стандарти и платформи /GNU GPL/. Същите позволяват да се постигне високо ниво сигурност, а уникалността на готовите продукти ограничава използването на познати средства за компрометиране на сигурността. Създадена е методология на работа, която позволява разработваните продукти да преминават задължителни тестове за работоспособност и сигурност от различни екипи.

### А. 8.26. ИЗИСКВАНИЯ ЗА СИГУРНОСТ НА ПРИЛОЖЕНИЯТА

**Механизъм за контрол:** *Изискванията за информационна сигурност трябва да се идентифицират, специфицират и одобряват при разработване или придобиване на приложения.*

1. Управляваните от УНСС информационни системи са сложна съвкупност от хардуер, операционни системи, инфраструктура и бизнес приложения. Ръководството на университета осъзнава, че сигурността на системата е най-ефективна, когато тя е планирана и управлявана през целия жизнен цикъл на информационната система, респективно на всеки един от етапите на развитие:
   - Иницииране на проект;
   - Анализ на функционалния дизайн и планиране;
   - Спецификация на информационната система;
   - Софтуерна разработка;
   - Инсталиране и внедряване;
   - Експлоатиране и поддържане;
   - Извеждане от експлоатация.

Всички изисквания за сигурност се определят на етап Планиране.

### А. 8.27. ПРИНЦИПИ НА СИГУРНОСТ В СИСТЕМНО ИНЖЕНЕРСТВО

**Механизъм за контрол:** *Принципите за сигурност трябва да бъдат определени, документирани, поддържани и прилагани за всяка информационна система.*

1. При проектиране на информационни системи за вътрешните дейности УНСС се осланя на опита и рутината на членовете на екипа и партньори. Дългогодишния им стаж в областта, както и задълбочените познания на основната дейност, в допълнение към анализа на риска, гарантират интересите на УНСС.
2. Въвеждането на новата технология се анализирана за рискове за сигурността и проектът се преглежда от Мениджър ИС за наличие на слабости по отношение на известни модели на атака.

### А.8.28. ПРИНЦИПИ ЗА СИГУРНО КОДИРАНЕ

**Механизъм за контрол:** *При разработката на софтуер трябва да се прилагат принципите на сигурно кодиране.*

1. Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните със сертификати (transparent data-at-rest encryption);
2. По възможност се предвижда система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата;
3. Не се допуска използването на Self-Signed сертификати за публични услуги;
4. Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Internet Explorer, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката; За защита на уеб сървърите да се инсталира сертификат на уеб сървърите, издаден от доверена система за сертифициране (trusted certification authority system). Сертификатът ще е издаден за съответния уеб сайт (website) или група сайтове и ще е уникален, ще използва алгоритъм за криптиране SHA2, ще е актуален, като сертификатите с изтекъл срок ще се анулират.
5. Трябва да бъдат извършени тестове за сигурност на всички уебстраници, като минимум чрез автоматизираните средства на SSL Labs за изпитване на сървърна сигурност (https://www.ssllabs.com/ssltest/). За нуждите на автентикация с КЕП трябва да се предвиди имплементирането на обратен прокси сървър (Reverse Proxy) с балансиране на натоварването, който да препраща клиентските сертификати към вътрешните приложни сървъри с нестандартно поле (дефинирано в процеса на разработка на Системата) в HTTP Header-а. Схемата за проксиране на заявките трябва да бъде защитена от Spoofing;
6. При разгръщането на всички уебуслуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на модерни алгоритми за криптография. Като минимални изисквания УНСС е приел употребата на TLS 1.2 и AES-256;
7. Трафикът между отделните модули и подсистеми да се контролира чрез филтриране по IP адрес, по протокол, по номер на порт от Transmission Control Protocol (TCP)/Internet Protocol (IP) стека и т. н.) с цел превенция на евентуални атаки и ограничаване на разпространението на инциденти.

Филтрирането на трафика да бъде по предварително разписани и одобрени правила, основаващи се на функционалността и сигурността, които ще бъдат редовно проверявани за нерегламентирани изменения и ще бъдат актуализирани с оглед на нововъзникващи заплахи. Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика в ИТ инфраструктурата на УНСС.

8. За защита на интегритета на информацията, обменяна с потребителите, системата да е достъпна само по протокол Hypertext Transfer Protocol Secure (HTTPS), като се използват само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г., или следващи по-нови версии.
9. За криптиране на информацията, обменяна между уеб сървъра и потребителите му, да се вземат предвид публикуваните в RFC на IETF забрани за използване на методи за шифриране в криптографските транспортни протоколи.
10. По възможност да се прилага подходящ Web Application Firewall (WAP), който наблюдава и филтрира трафика с цел защита от кибератаки от типа Cross-Site Request Forgery (CSRF), Cross-site Scripting (XSS), file inclusion, SQL injection и др.
11. По възможност да се прилага да не се позволява вмъкване на данни от страна на потребителя, освен на определените за това места.
12. Да се валидират всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент.
13. Да бъде избягвано използването на собствено разработени библиотеки. Вместо това следва да се използват фокусирани върху сигурността инструменти като Google KeyCzar, Bouncy Castle и/или включените функции в използваното SDK.
14. По никакъв начин да не се съхранява ключ за криптиране, заедно с криптирани данни.
15. Не трябва да прави достъпни поверителни или чувствителни данни в паметта и да не допуска записването им в места за временно съхранение или в лог файлове.
16. Сигурността на основните криптографски елементи до голяма степен зависи от генератора на произволни числа Random number generator (RNG). RNG следва да се използва от екипа по разработка за целите на криптографията се нарича криптографски сигурен генератор на псевдослучайни числа Cryptographically secure pseudorandom number generator (CSPRNG). Не се допуска използването на Math.random - тъй като той генерира случайни стойности детерминистично, и резултатите му се считат за изключително несигурни.
17. Да не се допуска въвеждане на специални символи, особено такива, които се използват в SQL заявките.
18. Всички данни, изпращани от клиента и показвани в уеб страница, да бъдат кодирани с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript.
19. За защита от атаки от типа отказ от услуги (DoS):
20. Да се конфигурират типът и размерът на headers, които уеб сървърът ще приема;
21. Да се ограничат времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка, за да се минимизира въздействието и на slow HTTP атаки;
22. За защита от brute force атаки да се въведе ограничение от броя неуспешни опити за влизане в системата. Броят неуспешни и времето за изчакване след достигането му, когато системата отново ще позволи вход, са параметри, които ще има възможност да се конфигурират от

администраторите на системата през потребителски интерфейс. Стойностите по подразбиране на тези параметри да са 5 (пет) неуспешни опита и 3 (три) минути време за изчакване.

23. Комплексност на паролите за достъп на потребители на системата:
    - Дължина: поне 10 символа;
    - Да съдържат поне една голяма и една малка букви;
    - Да съдържат поне една цифра от 0 до 9;
    - Да съдържат поне един специален символ (например: ,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
24. За защита от SQL Injection атаки, да бъде използвана технология за достъп до базата данни с която да се гарантира, че всички заявки към базата данни се предават чрез SQL параметри и не се съставят чрез използване на низове или конкатенация на стрингове. Така подадените заявки следва да не са податливи на SQL injection атаки.
25. Стриктно да се валидират данните, въвеждани от потребителя. Input параметрите да бъдат конкретизирани и възможността за въвеждане ще бъде изолирана само до този предефиниран писък от възможности.
26. Да не се допуска използването на версии и framework, които са излезли от поддръжка или ще излязат от поддръжка в предвиденото време за експлоатация на системата.
27. Да се използват технологии и framework, които притежават вградени инструменти за защита от SQLi
28. Да не се позволява извеждане на списък на уеб директориите.
29. Бисквитките (cookies) да имат:
    - флаг за защита (security flag) – този флаг инструктира браузъра, че "бисквитката" може да бъде достъпна само чрез защитени SSL канали;
    - флаг HTTP only – инструктира браузъра, че "бисквитката" може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента.
30. В главната директория на уеб сайта (website) да бъде конфигуриран файл, който да дава указания на уеб роботите (ботове/паяци), колко често да обхождат сайта, както и кои части от него да обхождат и да индексират; ако този файл не съществува, уеб роботите обхождат целия сайт – всяка една негова страница, подстраница, статия, линк и т.н., което крие риск за конфиденциалността на информацията.
31. Системата следва да бъде внедрена в отделна и защитена среда. Тази среда ще бъде изолирана от другите информационни и комуникационни системи на УНСС. За защита на DNS ще се прилага DNSSEC (Domain Name Security Extensions).
32. Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за минималните изисквания за мрежова и информационна сигурност;
33. По подразбиране потребителите да нямат възможност да използват разширени обектни търсения (OQL,HQL). Наличието на такава, следва предварително да е съгласувана и одобрена от Мениджър ИС;
34. Защитата от SQL Injection атаки следва да стартира още при избора framework и backend, който ще бъде използват. Всеки разработчик следва да представи предварително подхода си за вида и версията на backend и framework още на етап техническо предложение. Използването на различни от декларираните без съгласуване с Мениджър ИС може да доведе до отказ от приемане на изпълнението, въпреки, че останалите параметри са изпълнение и спазени;

35. При проектирането и разработката на компонентите на Системата и при подготовката и разгръщането на средите трябва да се спазват последните актуални препоръки на OWASP (Open Web Application Security Project);
36. Трябва да бъде изграден модул за проследимост на действия и събития в Системата. За всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:
    - Уникален номер;
    - Точно време на възникване на събитието;
    - Вид (номенклатура от идентификатори за вид събитие);
    - Данни за информационна система, където е възникнало събитието;
    - Име или идентификатор на компонент в информационната система, регистрирал събитието;
    - Приоритет;
    - Описание на събитието;
    - Данни за събитието.
37. Астрономическото време за удостоверяване настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при технологична необходимост - милисекунда, изписани в съответствие със стандарта БДС ISO 8601:2006;
38. Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставимост, трябва да бъде удостоверявано с електронен времеви печат по смисъла на Глава III, Раздел 6 от Регламент ЕС 910/2014. Трябва да бъде реализирана функционалност за получаване на точно астрономическо време, отговарящо на горните условия, и от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161;
39. От екипа по разработка по възможност, трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата и които да потвърдят изпълнението на изискванията в настоящата точка, след което резултатите да бъдат предадени на УНСС за съхранение към общата документация по приемане на платформата.
40. При разработването и въвеждането в експлоатация на предложеното решение, следва да бъдат спазвани и всички изисквания на законовата нормативна уредба в това число:

- Закон за киберсигурност;
- Закон за електронното управление (ЗЕУ);
- Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги;
- Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМИС);
- Вътрешни правила за мрежова и информационна сигурност на УНСС.

### А. 8.29. ТЕСТВАНЕ НА СИСТЕМИ ЗА СИГУРНОСТ

**Механизъм за контрол:** *Тестване на функционалността на системите за сигурност трябва да се провежда по време на разработването.*

1. УНСС е внедрил механизми за тестване на ново разработваните системи чрез използване на чек листи, с които да се провери дали системата генерира очакваните резултати. В завършен вид новоразработените системи се проверяват за наличие на уязвимости от Мениджър ИС. При констатиране на несъответствие с очакваните резултати или открита уязвимост, същата незабавно

се докладва на екипа, разработил системата. Специалисти на УНСС изготвят план за отстраняване, който се съгласува и одобрява от Мениджър ИС.

2. След реализирането му се извършва повторна проверка. При липса на пропуски в сигурността теста се счита за успешен и системата преминава във фаза готовност за въвеждане. При констатиране на несъответствия цикълът се повтаря до постигане на приемлив резултат

### А. 8.30. ИЗНЕСЕНА РАЗРАБОТКА

**Механизъм за контрол:** *УНСС трябва да ръководи, наблюдава и преглежда дейностите по изнесена разработка на системи.*

1. В УНСС не се управлява процес по изнесена разработка на софтуерни продукти и създаване на сорс код, в това число и извършване на тестване функционалността и зареждане на системите и продуктите с подходящи данни. По този механизъм за контрол към тази цел по контрола се прави изключение и не е приложим.

### А. 8.31. РАЗДЕЛЯНЕ НА РАЗРАБОТВАНЕ, ТЕСТВАНЕ И РАБОТНА СРЕДА

**Механизъм за контрол:** *Средите за разработка, тестване и производство трябва да бъдат разделени и защитени.*

1. Процесът и участващите в него служители, занимаващ се с разработване и изпитване, представлява заплаха за поверителността на информацията. Дейностите по разработване и тестване могат да причинят непреднамерени промени в софтуера или данните, ако споделят една и съща среда. Поради това е задължително да се разделят средите за разработка и тестване от продукционните. УНСС прилага следните мерки за защита:
    - компилатори, редактори и други инструменти за разработка или помощни програми, не предназначени за разработка, не се използват в същата среда с продукционната.
    - Не се провеждат тестове за сигурност или функционалност на продукционните системи, освен ако това не е крайно наложително, но само след одобрение от Мениджър ИС;
    - За тестовите системи са валидни изисквания за сигурност, контрол на достъпа, контрол на промените, управление на уязвимостите, управление на капацитета, patching, контрол на версиите и мерки за защита, идентични с продукционните;
    - Ако е приложимо се използват инструменти за мониторинг на сигурността идентични с тези на продукционните среди;
    - Тестовете среди се разделят логически или физически от продукционните, както по отношение на мрежовия достъп, така и по отношение на виртуализация, резервиране и възстановяване.

### А. 8.32. УПРАВЛЕНИЕ НА ИЗМЕНЕНИЯТА

**Механизъм за контрол:** *Измененията в УНСС, бизнес процеса, средствата за обработка на информацията и системите трябва да бъдат контролирани.*

1. Всички промени и изменения, свързани със системите за обработка на информацията, са документирани и управлявани. УНСС се стреми да не допуска нерегламентирани изменения, за да сведе до минимум проблемите в системи, свързани със сигурността на информацията. Установени са задължения и отговорности за управление на промените и са внедрени механизми за осигуряване на ефикасен контрол върху значими изменения на хардуерни и комуникационни системи,

операционни системни, софтуерни приложения, бизнес процеси, процедури и технологии. Управление на промените се изразява в следните стъпки:

- Всеки служител или клиент на УНСС може да инициира предложение за промяна, чрез заявка в свободен текст на актуалния канал за комуникация по въпросите на промените;
- Предложенията се преглеждат от Мениджър ИС и Мениджър ИТ/администратори на системата, обект на промяната/, след което се взима решение дали промяната да бъде одобрена, кога и как да бъде изпълнена.

2. Промени се инициират в случай на, но не се ограничават до:
   - Имплементиране и/или преконфигуриране на хардуерно оборудване, значимо за дейността на УНСС;
   - Внедряване и/или надстройване на операционни системи, значими за дейността на УНСС;
   - Внедряване и/или надстройване на бизнес приложения, значими за дейността на УНСС;
   - Изменения в утвърдени процедури на УНСС.
   - Промени се възлагат от Мениджър ИТ на Специалист/и с нужната квалификация и опит, съгласно техните задължения, отговорности и ниво за допуск до информацията на УНСС;
   - Промените могат да бъдат възложени от определен от УНСС служител или лично от него, на трета страна, с която УНСС има сключено споразумение за съответните дейности;
   - Контрола по изпълнението се поема от Мениджър ИТ;
   - Всички утвърдени промени се отразяват в организирана за целта база данни. Контрола на достъп до базата е регламентиран и проследим;
   - Направените промени се описват в съответния раздел в дистрибюшън група - change@unwe.bg;
   - Контрол се упражнява от Мениджър ИС, като включва минимум:
   - Планирано действие;
   - Очакван резултат;
   - Получен резултат;
   - Одобрение на действието;
   - Приемане или отказ на новото състояние;
   - Варианти за връщане на предходно стабилно състояние на информационните системи.

3. По преценка на Мениджър ИТ новото състояние може да бъде документирано в кореспондиращите документи, схеми, диаграми, процедури, системи и т.н.
   - След успешно реализиране на промени, изпълнилия промяната е задължен да уведоми по надлежния начин заинтересованите лица, които включват задължително Мениджър ИС.
   - Изменения в експлоатационните системи се възлагат, само когато има действителна причина за това, например: внедряване на нова функционалност или повишен риск за информационната система.

### А. 8.33. ЗАЩИТА НА ТЕСТОВИ ДАННИ

**Механизъм за контрол:** *Информацията използване на тестове, трябва да бъде подбрана, защитена и управлявана по подходящ начин..*

1. Информацията за тестовете в УНСС се подбира така, че да гарантира надеждността на резултатите от тестовете и поверителността на използваните данни.

2. Забранено е чувствителна информация (включително лични данни) да се използва в средите за разработка и тестване.
3. По време на тестовете се прилагат идентични механизми за контрол на достъпа с тези заложени в крайния вариант на разработваното приложение/система;
4. Използват се различни данни за аутентификация, с които еднозначно да се различи логването в тестова и продукционната система;
5. След приключването на тестовете и приемане на система, данните за заличават необратимо;

### А. 8.34. МЕХАНИЗМИ ЗА КОНТРОЛ ЗА ОДИТ НА ИНФОРМАЦИОННИ СИСТЕМИ

**Механизъм за контрол:** *Изискванията на одита и действията, включващи проверки върху работни системи, трябва да бъдат внимателно планирани и съгласувани, за да се минимизира рискът от разрушаване на бизнес процесите.*

1. При реализирането на този процес Мениджър ИС включва проверки върху работни системи, като внимателно планира и съгласува същите, за да се минимизира рискът от разрушаване на бизнес процесите на УНСС. Процесът на прилагане на проверката включва и се осигурява следните условия:
   - изискванията на одита трябва да бъдат съгласувани с Ръководството на УНСС;
   - обхватът на проверките трябва да бъде уговорен и контролиран;
   - проверките трябва да бъдат ограничени до достъп само за четене на софтуера и данните;
   - достъп, различен от този само за четене, може да бъде позволен само за изолирани копия на системни файлове, които трябва да бъдат заличени след приключване на одита или да имат подходяща защита, ако има задължение за поддържане на такива файлове съгласно изискванията на документацията на одита;
   - ресурсите за извършване на проверките трябва да бъдат изрично определени и налични;
   - изискванията за специална или допълнителна обработка трябва да бъдат определени и съгласувани;
   - всички изисквания и отговорности трябва са документирани в заповед;
   - лицата, които извършват одита, трябва да бъдат независими от проверяваните дейности, ако е възможно.

## 6. СПРАВОЧНИ ДОКУМЕНТИ

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

## 7. ПРИЛОЖЕНИЯ

**……**

Дата: 19.10.2023 г.

Утвърдил: ……

Проф. д-р Димитър Димитров, Ректор