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

ПОЛИТИКА
ЗА
ДОПУСТИМО ИЗПОЛЗВАНЕ НА АКТИВИ

СЪГЛАСНО ISO/IEC 27001:2022

РЕГИСТРИРАНЕ НА ИЗМЕНЕНИЯТА	
Стр.	Същност на изменението

1. ЦЕЛ

- Политиката описва наложените минимални политики за сигурност при достъп на информационни системи на университета;
- Определя вътрешни правила, реда и отговорностите на служителите при използване на информационните активи на УНСС във връзка с внедрената Система за управление на информационната сигурност (СУИС) съгласно Стандарт ISO27001:2022.

2. ОБХВАТ

Политика за допустимо използване на активи засяга всички служители, доставчици и потребители от трети страни.,

Университета, освен че контролира употребата на активи, в последствие и търси отговорност от ползвателите на ресурси и информация за спазване на приетите правила.

3. ОПИСАНИЕ НА ДЕЙНОСТИТЕ

3.1.Използване на оборудването, собственост на УНСС

3.1.1. Служителите трябва да са запознати, че данните и документите, които са създадени, придобити и/или съхранявани чрез системите и оборудването на УНСС, са собственост на Университета.

3.1.2. Служителите са отговорни да упражняват самоконтрол при използването на компютърната техника, мрежата и мрежовите устройства, като не употребяват същите за лични нужди.

3.1.3. Всяка информация, която попада в някоя от категориите класифицирана информация, трябва да бъде защитена съгласно утвърдените правила и/или нормативната уредба.

3.1.4. С цел управление и гарантиране на сигурността и поддръжката на мрежата, Дирекция "Информационни технологии" (ДИТ) има право да наблюдава по всяко време цялото ИТ оборудване, както и мрежовия и интернет трафик.

3.1.5. ДИТ периодично одитира ИТ оборудването с цел да осигури съответствие с настоящите вътрешни правила.

3.2.Изнасяне на оборудване и информация извън територията на УНСС

3.2.1. Ръководството на УНСС допуска ползването на устройства извън работните помещения, ако това се налага за изпълняване на служебните задължения на служителите, като за защитата на оборудването се прилагат правилата, описани в ПС А 07 от СУИС.

3.2.2. Служителите са инструктирани да не съхраняват, съответно да не изнасят конфиденциална/значима информация на преносими устройства. При необходимост да се използват такива, се спазват правилата на ПС А 07 от СУИС.

3.2.3. Служителите на УНСС не използват служебни ресурси за лични цели. Не е позволено използването на лични електронни пощи за изпращане или получаване на служебна информация или данни. За работа с интернет и електронна поща се съблюдават правилата на процедурите и политиките от СУИС.

3.3.Електронна поща

Със служебна електронна поща разполагат всички служители в УНСС, за които длъжността им изисква наличието на такава.

Достъпът до електронни съобщения се предоставя на служителите на УНСС и се използва изключително за служебни цели.

Пощенски акаунт на напуснали потребители се запазва отворен за определен период от време. След изтичане на определения период, акаунтът се забранява (disable).

Достъпът до пощенските кутии е защитен с парола. От служителите се изисква да пазят своите пароли сигурни и защитени съобразно изискванията, описана в ПС А 08.

Всички електронни съобщения, които са част от официалната кореспонденция се запазват и се третират като записи.

3.3.1. **Забранено** е използването на електронна поща за:

- изпращане на поверителна/чувствителна информация (потребителски имена, пароли и др.), освен ако не е криптирана с криптографски механизми;
- създаване, изпращане, препращане или съхраняване на имейли с прикачени файлове или съобщения, които могат да бъдат незаконни или обидни, с едно или повече от следните съдържания: сексуално, расистко, клеветническо, нецензурно, уронващо, дискриминационно, заплашващо и т.н.;
- частни или благотворителни мероприятия, несвързани с дейността на УНСС;
- текстове, които могат да се тълкуват като официални изявления на УНСС, освен ако не са наистина такива;
- изпращане на съобщение от нечия друга електронна поща или от друго име (включително използването на фалшиви "From:" адреси);
- използването на служебната електронна поща за лични цели;
- всякакви други незаконни и/или неморални цели.

3.3.2. Допълнителни изисквания

- Преди изпращане, текстът на имейла трябва да се прегледа внимателно, особено официалната комуникация с външни лица.
- Имейлите се сканират автоматично за зловреден софтуер.
- Бъдете бдителни, когато отваряте имейл с прикачен файл, независимо дали е от познат изпращач или не. Особено съмнителни са имейли, подканващи за смяна на парола, попълване на определена информация или инсталиране на файл. Такива имейли трябва да докладвани своевременно на Мениджър ИС.
- Бъдете разумни за броя и размера на имейлите, които изпращате и запазвате. Периодично почиствайте вашата пощенска кутия от стари имейли, които вече не са необходими или ги съхранявайте във вид на файлове в подходящи папки. Важни имейли трябва да се архивират в съответствие с процедурата за архивиране.
- Внимавайте, когато избирате получателя от поле "To", относно запаметени преди това имейли. Възможно е в бързината да изпратите имейл до друго лице.
- Внимавайте, когато отговаряте на имейл, чрез "Reply all". Чрез избор на "Reply all" ще върнете отговор на всички получатели на входящото писмо.
- Внимавайте, когато получите съобщение за спечелена сума от лотария, джакпот или за наследство от далечен роднина.

3.4.Системи за документооборот

3.4.1. Оборотът на документи в УНСС се управлява чрез автоматизирана информационна система за документооборот (АИС) и вътрешен сайт.

3.4.2. До системи за документооборот имат достъп служителите, чиято длъжност изисква употребата им.

3.5.Позволено използване на интернет

Интернет се предоставя единствено за целите на подпомагане на дейности, необходими за изпълняване на функциите на работните места. Всички потребители трябва да спазват вътрешните правила по отношение на използването на ресурсите и да упражняват добра преценка при използването на интернет. Въпроси могат да бъдат адресирани до Мениджър ИС и Мениджър ИТ.

Приемливото използване на Интернет за изпълнение на ежедневните задачи включва:

- Комуникация между служители и външни лица и т.н.;
- ИТ техническа поддръжка;
- Преглед на уеб сайтове на възможни доставчици относно информация за продукти и услуги;
- Проверка на информация във връзка с изпълнение на служебни задължения;
- Проверка на актуалното законодателство и изисквания.

Всички служители трябва да са наясно, че интернет трафикът се следи и логовете се преразглеждат периодично.

Съхранение или предаване на лична информация се прави на свой собствен риск. УНСС не носи отговорност за загуба на информация.

3.6.Забранено използване на интернет

Използването на интернет е забранено за:

- лични цели без одобрение от Мениджър ИС;
- придобиване, съхраняване и разпространение на незаконни данни, порнографско съдържание, съдържание накърняващо раса, пол или вероизповедание;
- провеждане на странични мероприятия, участието в каквато и форма на събиране на информация за настройки на оборудване, извършване на дейности с цел измама, или съзнателно разпространение на фалшиви или иначе клеветнически материали;
- достъп до информация, която не е необходима за изпълнение на служебните задължения;
- всяко поведение, което представлява или насърчава престъпление, довело до гражданска или наказателна отговорност или по друг начин нарушава нормативната уредба;
- използване, предаване, дублиране, сваляне или доброволно получаване на материали, които нарушават авторските права, търговски марки, търговски тайни, или патентни права на всяко лице или организация, извън тези, свързани с изпълнение на ежедневните задължения;
- предаване на всяка информация от ниво конфиденциална/вътрешна, без съответните контролни механизми;
- всякакви форми на игри, хазарт и т.н.;
- неоторизирано сваляне на всякакви софтуерни програми или файлове, извън тези, свързани с изпълнение на ежедневните задължения и изрично указани в "Списък на одобрения софтуер".

3.7.Достъп до оборудване

До оборудване от типа на принтери, факс, мултифункционални устройства, имат достъп всички служители на УНСС, чиято дейност изисква това, като контрол върху употребата се осъществява от Мениджър ИС и Дирекция "Информационни технологии".

3.8.Елементи от мрежовата и информационната сигурност

3.8.1. Съхраняване и опазване в тайна на паролите за достъп до различните елементи на ИС – управлява се по реда на ПС А 08 от СУИС.

3.8.2. При пренос на информация между отдалечени мрежи на организацията или мобилни устройства се използва криптиране на информацията по реда на ПС А 08.

3.8.3. Защита на информацията, съхранявана на преносимите устройства – всеки служител е длъжен редовно да изтрива ненужната информация, а важната да бъде преместена в предназначената за това директория. На преносимия компютър е допустимо да се съхранява информация, върху която се работи в момента по текущи задачи, при спазване на политиките и процедурите от СУИС.

3.8.4. Безопасност при използване на електронна поща и интернет – управлява се по реда на настоящите вътрешни правила.

3.8.5. Устройствата и системите се конфигурират в съответствие с препоръките за сигурност на съответния им доставчик или производител, като се приложат политиките и процедурите от СУИС.

3.8.6. Мениджър ИС следи за новооткрити уязвимости в сигурността на използвания в системите на УНСС софтуер и фърмуер и за техни актуализации (нови версии, ъпдейти и пачове), които отстраняват тези уязвимости, или мерки за смекчаването им, публикувани от производителите или доставчиците.

3.8.7. Реда за инсталиране на ъпдейти на сървъри и компютри е посочен в ПС А 08 от СУИС.

3.9.Неприемлива употреба

Строго забранено е следното неприемливо използване на информационни активи и системи:

- Неоторизирано използване, унищожаване, модифициране и разпространение на информация или информационни системи.
- Използване или опит за използване на чужда самоличност в електронна комуникация.
- Използване на информационни системи, включително електронна поща с цел тормоз и изпращане на неприлични, заплашителни или клеветнически съобщения.
- Използване на информационни системи, за търговски дейности, религиозни или политически каузи или за лична изгода.
- Изпращане на нежелани и неоторизирани масови имейли (спам).
- Умишлено разпространяване на зловреден софтуер или заразени файлове.
- Използване на думи или фрази, които могат да се тълкуват като унизителни въз основа на раса, цвят на кожата, пол, възраст, увреждане, национален произход или друга категория.
- Всеки опит за променяне, деактивиране, неспазване или заобикаляне на контроли, политики и процедури за сигурност.
- Саботаж, унищожаване, злоупотреба или неоторизирани системни поправки на информационни системи.
- Промяна на софтуерни или хардуерни конфигурации или намеса в администрирането на информационните ресурси.
- Използване на персонални компютърни системи или тестови устройства във или в мрежи без писменото разрешение на ръководството.
- Използване на инструменти, които компрометират сигурността.
- Кражба на ресурси, включително чувствителна информация.
- Свързване на лични комуникационни устройства (рутери, суитчове) към мрежата на УНСС.
- Неправомерен достъп до мрежово оборудване на УНСС (защитни стени, рутери, комутатори и т.н.).
- Неоторизиран достъп до университетско комуникационно оборудване.
- Съхраняване на университетски данни на неоторизирани устройства.
- Показване, публикуване, отпечатване или изпращане на материали, които противоречат на етичният кодекс на УНСС.
- Нарушаване на правата на интелектуална собственост, плагиатство и неразрешено използване или възпроизвеждане в нарушение на патенти, търговски марки, авторски права, софтуер и други лицензионни споразумения.

Ръководството на организацията непрекъснато ще контролира ефективността и ефикасността на заложените цели по информационна сигурност чрез периодичен преглед и съизмерима оценка, посредством редовно извършване на вътрешни одити и прегледи от ръководството. Тази Политика ще бъде преразглеждана при настъпване на промени в обхвата на системата за управление на информационната сигурност и периодичните Прегледи от ръководството на организацията.

Ръководството се ангажира да не допуска отклонения от намерението за постигане на целите по информационна сигурност, като поддържа и непрекъснато усъвършенства своята система за управление на информационната сигурност, осигурявайки необходимите ресурси за това.

Изпълнението на Политиката по информационна сигурност е задължително за всички служители на компанията.

Ръководството декларира, че тази Политика е одобрена, публикувана и комуникирана до всички нива в екипа и съответните външни страни, по подходящ за целта начин и форма.

4. ТЕРМИНИ И СЪКРАЩЕНИЯ

- **Термини**

Няма.

- **Съкращения**

УНСС – Университет за национално и световно стопанство;
СУИС – Система за управление на информационната сигурност;
НМИМИС – Наредба за минималните изисквания за мрежова и информационна сигурност;
ДИТ – Дирекция "Информационни технологии";
АИС – Автоматизирана информационна система;
ИС – Информационна система

Дата: 19.10.2023 г.

Утвърдил: ……
Проф. д-р Димитър Димитров - Ректор