СУ „ОТЕЦ ПАИСИЙ“ с. МЕДКОВЕЦ

3400 с.Медковец, общ. Медковец, ул. Г. Димитров №25
e-mail: info-1205000@edu.mon.bg; тел: 0878608474

З А П О В Е Д № 37/30.09.2026 г.

На основание чл. 258, ал. 1 и чл. 259, ал. 1 от Закона за предучилищното и училищното образование (ЗПУО),

НАРЕЖДАМ:

УТВЪРЖДАВАМ политика за работа с информационни системи и активи за информационна сигурност на СУ “Отец Паисий“ през учебната 2026/2027 г.

Настоящата заповед, заедно с политиката за работа с инф.системи да се доведе до знанието на всички служители.

Контрол по изпълнение на заповедта възлагам на Горан Лозанов – зам.директор АСД.

Директор : .....
/Светла Неделчева/

СУ „ОТЕЦ ПАИСИЙ“ с. МЕДКОВЕЦ

3670 с.Медковец, общ. Медковец, ул. Г. Димитров №25
e-mail: info-1205000@edu.mon.bg; тел: 0878608474

УТВЪРДЕНИ: ……
Светла Неделчева
……

Заповед № …37…/30.09.2026 г.

ПОЛИТИКА ЗА РАБОТА С ИНФОРМАЦИОННИ СИСТЕМИ И АКТИВИ И ЗА ИНФОРМАЦИОННА СИГУРНОСТ

в СРЕДНО УЧИЛИЩЕ „ОТЕЦ ПАИСИЙ“

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящата политика цели да регламентира: правила и процедури за използване на информационните системи и активи на СУ „Отец Паисий“

1. от страна на служителите и на учениците;
2. запазване на конфиденциалността на информацията чрез осигуряване на мерки за защита от неправомерно придобиване, неправомерно модифициране, унищожаване или загубване;
3. развитие и поддържане на сигурни и надеждни информационни системи, осигуряващи цялост и достъпност на информацията;
4. мерки за реакция в случай на злоупотреба, загуба или неупълномощено придобиване на информация, както и при бедствия и аварии;
5. осигуряване на непрекъснатост на работните процеси;
6. информиране на педагогическия и непедагогическия персонал и на други лица, имащи достъп до информационните системи и активи на СУ „Отец Паисий“ за техните отговорности и задължения;

(2) Политиката обхваща:

1. информационните системи на образователната институция;

информационната сигурност;

5. утвърждава план за осигуряване непрекъснатостта на дейността и планове за обучение на служителите на институцията във връзка с използването на информационните системи и активи и информационната сигурност.

(2) Директорът на образователната институция проследява и осигурява актуалността на настоящата политика и свързаните с нея документи.

(3) Директорът на образователната институция отговаря за подходящото оповестяване на актуалната версия на настоящата политика и свързаните с нея документи. Той отговаря служителите на СУ „Отец Паисий“ да бъдат подходящо инструктирани и мотивирани за изпълнение изискванията на политиката.

Чл. 6. Специалистът по информационни технологии/системният администратор отговаря за:

1. управление и поддържане на информационните системи и активи на СУ „Отец Паисий“ и предоставяне на нужните нива на достъп;
2. архивиране на данни и информация;
3. осигуряване на защита от злонамерен софтуер;
4. мониторинг на уязвимости и инциденти;
5. изготвяне на нужната документация, свързана с администрирането на информационната система и активи.

Чл. 7. (1) Потребителите на информационните системи в СУ „Отец Паисий“, са задължени да следват правилата, инструкциите и заповедите, свързани с използването на информационни системи и активи и с информационната сигурност.

(2) Потребителите са длъжни да докладват за проблеми и инциденти с информационните системи и активи.

(3) Под потребители на информационни системи в настоящата политика се разбират всички лица, които имат достъп до системите по силата на своите служебни или договорни отношения, както и всички учащи, ползващи информационните системи на институцията.

(4) Педагогическите специалисти и непедагогическият персонал използват информационните системи и активи в СУ „Отец Паисий“ с цел увеличаване на продуктивността и ефективността на работата.

(5) Всички потребители се запознават с тези части от настоящата политика и свързаните с нея документи, които отговарят на техните роли и отговорности. Потребителите потвърждават, че са запознати и че разбират задълженията си по тези документи.

(6) Правата и задълженията на потребителите и служителите на СУ „Отец Паисий“ по отношение на информационните системи и активи и информационната сигурност в образователната институция, се определят в съответствие с настоящата политика, в правила, заповеди или в длъжностните им характеристики.

за онлайн обучение софтуери.

(2) Изключения от разпоредбата на ал. 1 са допустими при изрично разрешение на директора на институцията и за целите на работния или образователния процес.

Чл. 14. При напускане на институцията, работниците/служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работа.

Чл. 15. (1) Забранява се ползването на информационните системи и активи на образователната институция в следните случаи:

1. Заобикаляне на системите за сигурност с цел разрушаване или намаляване сигурността на учебната локална мрежа или бази данни.
2. Ползване на информационните системи за извършване на престъпление.
3. За подпомагане дейността на частни лица, в това число търговски дружества, техните продукти, услуги или бизнес практика.
4. Електронната поща на институцията не може да се ползва за комерсиални лични цели, религиозни цели или да се подпомага бизнес, който не е свързан с дейността на образователната институция.
5. За политическа дейност, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат.
6. Подправяне на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. Всички електронни писма, пращани от персонала трябва да са лично подписани.
7. Свалянето от интернет на аудио и видео файлове.
8. Сваляне и инсталиране на компютърни програми от интернет без разрешение на компютърните специалисти.
9. Копиране на лицензираните компютърни програми на институцията с цел лична употреба.

(2) Този списък на забранените дейности във връзка с информационните технологии не е изчерпателен и към него може да се добавят допълнителни забрани със заповед на директора.

Чл. 16. (1) Неоторизираното разкриване на служебна информация може да доведе до негативни последици за образователната институция и накърняване на нейния имидж и репутация.

(2) Работник/служител, който е копирал и използвал информация от локалната мрежа на институцията за лична изгода или за да причини вреда на институцията, носи съответната дисциплинарна и имуществена отговорност по Кодекса на труда.

Чл. 17. (1) Ръководството насърчава ползването на интернет от работниците/служителите за обмяна на информация, извършване на проучвания и събиране на данни във връзка с дейността им.

(2) Заместник-директорите и други оторизирани длъжностни лица отговарят за

включват ясни клаузи, гарантиращи, че правата за интелектуалната собственост остават за институцията.

(3) Образователната институция инсталира и използва само лицензирани продукти, като адекватно преценява и осигурява срока, броя потребители и др. Ръководството на образователната институция и специалистът по информационни технологии осъществяват проверки за целта.

РАЗДЕЛ СЕДМИ
ФИЗИЧЕСКА СИГУРНОСТ

Чл. 22. Информационните системи и оборудването на СУ „Отец Паисий“, в това число копирни машини, факсове и мрежови принтери, се защитават физически от заплахи за сигурността и влияние на рискове от околната среда с цел предотвратяване на загуби, щети или излагане на риск на активи и затрудняване или прекратяване на дейността на институцията.

Чл. 23. Помещенията, в които е разположено оборудване, свързано с информационните системи на образователната институция, се обособяват като защитени физически зони с ограничен и контролиран достъп.

За целта директорът на СУ „Отец Паисий“ издава заповед със съответните мерки и отговорни лица. Подобни мерки могат да включват секретни ключалки, дневник за достъп, видео наблюдение и др.

Мерките за физическа защита не трябва да възпрепятстват и затрудняват служебния и учебния процес.

Чл. 24. Изнасянето извън сградите на институцията на информационни активи, принадлежащи на институцията, се извършва с разрешение от директора или оправомощено лице.

Чл. 25. Служебна информация не се оставя без надзор или контрол, което означава видима на екран.

Чл. 26. Физическият достъп на външни лица, в това число и на учениците, до информационните системи и активи на институцията се извършва от и/или в присъствие на служители на образователната институция.

Чл. 27. Сървърното помещение на институцията е оборудвано с подходящи и съвременни системи за климатизация, за пожароизвестяване и пожарогасене, за контрол на влажността, както и с непрекъсваеми захранващи устройства.

РАЗДЕЛ ОСМИ
КОНТРОЛ НА ДОСТЪПА, УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ЗАЩИТА ОТ ЗЛОНАМЕРЕН СОФТУЕР

поддържане на системите за защита от злонамерен код. За целта се използват като минимум:

1. системи за защита;
2. софтуер за откриване на вируси, сканиращ както входящия трафик към външни (интернет) страници и платформи на институцията, така и към потребителските персонални компютри, използвани в институцията.

Чл. 34. (1) Специалистът по информационни технологии на образователната институция носи пълната отговорност за избирането и инсталирането на антивирусната програма, както и за нейната актуализация на всеки индивидуален компютър. Служителите също трябва да следят дали тяхната антивирусна програма се осъвременява периодично с най-новата версия.

(2) Потребителите на информационните системи на институцията трябва да приемат всяко съобщение за злонамерен софтуер или друго злонамерено събитие изключително сериозно и да следват вътрешните процедури за реакция в такъв случай.

(3) Преднамереното разпространяване на данни, за които потребителят знае, че са заразени с вирус, е нарушение на служебните задължения, което се санкционира по дисциплинарен ред.

(4) В случай на злонамерена атака потребителят трябва незабавно да информира специалиста по информационни технологии, без да предприема никакви действия самостоятелно.

(5) Входящата електронна поща трябва да се третира с особено внимание поради потенциалната възможност да е заразена със злонамерен софтуер. Отварянето на приложения да се прави само след предварителното им сканиране с антивирусна програма.

(6) Ползването на външни носители (USB, външна памет и др.) на информация е допустимо само след предварителното им сканиране с антивирусна програма.

Чл. 35. (1) СУ „Отец Паисий“ събира и анализира данни за вида и броя на инцидентите, свързани със сигурността на информацията. Въз основа на анализа се прави преценка на разходите за защита. Също така въз основа на анализа се идентифицират повтарящи се инциденти или инциденти с голямо влияние и на тази база се оптимизират мерките за защита.

(2) Информацията от извършваните по предходната алинея анализи се взема предвид в процеса по управление на риска в организацията.

Чл. 36. При работа от разстояние и необходимост от достъп до информационните системи на образователната институция дистанционно – извън вътрешната мрежа:

1. се използва двуфакторна автентикация на достъп;
2. се използват само канали с висока степен на защита като Virtual Private Network (VPN);
3. не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

4. име на служителя, извършил архивирането.

(3) Архивните копия се проверяват периодично за пълнота на архивираната информация и възможност за възпроизвеждането ù. Копията се проверяват поне веднъж годишно, а носители с информация от ключово значение за дейността на образователната институция – поне веднъж на 6 месеца.

Чл. 40. (1) При срив в информационните системи, специалистът по информационни технологии предприема нужните действия за възстановяване на нормалното функциониране на системите.

(2) При загуба или повреждане на информация специалистът по информационни технологии я възстановява, като използва последното актуално архивно копие.

РАЗДЕЛ ЕДИНАДЕСЕТИ
РАЗРАБОТВАНЕ И ВНЕДРЯВАНЕ НА ИНФОРМАЦИОННИ СИСТЕМИ

Чл. 41. С цел предотвратяване на увреждане или загуба на информация или грешки в информационните системи на образователната институция, при разработени и внедряване на нови или при усъвършенстване на съществуващи информационни системи, се планират подходящи мерки, които се залагат в договорите с разработчиците.

Чл. 42. (1) За всяка информационна система се поддържат отделни една от друга среда за тестване и продукционна среда, в която системата функционира.

(2) Дейности по разработване не се извършват в тестовата и продукционна среда на системата.

(3) Не се допуска пряк достъп на разработчиците до продукционната среда.

РАЗДЕЛ ДВАНАДЕСЕТИ
ОЦЕНКА НА РИСКА

Чл. 43. (1) Като част от дейността по управление на риска, образователната институция идентифицира и оценява рисковете, свързани с използването на информационните системи и информационната сигурност.

(2) При оценката на риска се идентифицират рискове за всяка система и актив, описани в списъка по чл. 12, ал. 4 на настоящата политика.

(3) Въз основа от резултатите от оценката на риска се прецизират и предприемат конкретните мерки във връзка с областите на прилагане и защита на информационните технологии и информацията, описани в настоящата политика.

ДОПЪЛНИТЕЛНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ