СРЕДНО УЧИЛИЩЕ „ПЕТКО РАЧОВ СЛАВЕЙКОВ” КРИЧИМ
4220 гр. Кричим, бул. „Тракия” № 24; тел. 03145/24-73;e-mail: info-1601403@edu.mon.bg

УТВЪРДИЛ
ДИРЕКТОР:

Заповед № РД-10-518/05.02.2026 г.

ИНСТРУКЦИЯ ЗА ОРГАНИЗАЦИОННИТЕ ПРОЦЕДУРИ ПО ИЗПОЛЗВАНЕ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ В СУ „П. Р. СЛАВЕЙКОВ“ гр. КРИЧИМ

2025/2026 учебна година

ГЛАВА I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) Чрез тази процедура се информират всички служители за техните права и задължения по отношение на използването на информационните системи в ***СУ „П. Р. Славейков“ гр. Кричим***,

(2) Процедурата определя правилата за ползване на информацията за вътрешна и външна комуникация, за предоставяне на услуги на граждани, за администриране,

(3) Процедурата е средство за извършване на проучвания и обмяна на информация.

(4) Достъпът до данните в локалната мрежа и ползването на програмните продукти е необходимост за служителите за да изпълняват своите задължения.

Чл.2. Информационните технологии в ***СУ „П. Р. Славейков“ гр. Кричим*** включват, локалните мрежи, интернет, електронната поща и всички програмни продукти, които ***СУ „П. Р. Славейков“ гр. Кричим*** ползва.

Чл.3. Чрез настоящата процедура се дават указания за етичната употреба от служителите на информационните технологии на и насърчава тяхната употреба с цел увеличаван ***СУ „П. Р. Славейков“ гр. Кричим*** е на продуктивността и ефективността на работата.

Чл.4. IT специалистите на са отговорни за цялостната дейност ***СУ „П. Р. Славейков“ гр. Кричим*** на информационните технологии и за подпомагането работата на служителите с тях.

Чл.5. Служителите на ***СУ „П. Р. Славейков“ гр. Кричим*** са задължени да спазват правилата, определени в тази процедура.

Чл.6. Всички компютърни програмни продукти и информация създадена и съхранена от служителите са собственост на ***СУ „П. Р. Славейков“ гр. Кричим*** .

Чл.7. Служителите нямат право да вземат програмните продукти с цел инсталацията им на домашните си компютри.

Чл.8. При напускане на ***СУ „П. Р. Славейков“ гр. Кричим*** служителите нямат право да копират или унищожават файлове с данни, които са създадени във връзка с тяхната работата.

ГЛАВА II. КОНТРОЛ ВЪРХУ РАБОТАТА С ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ на ***СУ „П. Р. Славейков“ гр. Кричим***

Чл. 9. Контролни функции на ръководството.

Ръководството на ***СУ „П. Р. Славейков“ гр. Кричим*** има право да контролира ползването на програмните продукти, електронната поща, Интернет и базите данни, създадени от служителите в училището.

(1) **Директорът** осъществява цялостен контрол върху прилагането на настоящата Инструкция и гарантира спазването на всички нормативни изисквания за мрежова и информационна сигурност, както и за защита на личните данни в информационните системи на институцията.

(2) Директорът определя със заповед **длъжностните лица**, които имат достъп и са отговорни за събирането, съхраняването и ползването на информацията в **Националната електронна информационна система за предучилищното и училищното образование (НЕИСПУО)**.

(2) Функции на Заместник-директора. **Заместник-директорът (по съответния ресор)** контролира ежедневното прилагане на ИТ процедурите и правилата за работа в електронна среда в рамките на неговия ресор.

Заместник-директорът отговаря за:

1. Контрол на **навременното и коректно въвеждане и обработка** на данни в **НЕИСПУО** от служителите в неговия ресор в съответствие с изискванията на Наредба № 8 и установените срокове.
2. Наблюдение върху спазването на правилата за **сигурност и поверителност** на информацията, включително ползването на служебни електронни пощи, пароли и достъпи.
3. Координиране на вътрешната комуникация, свързана с ИТ проблеми, и насочване на служителите към **Ръководителя на направление ИКТ** или **ИТ специалистите** при възникнали технически неизправности.
4. Участие в процеса на **анализ и оценка на риска** на критичните информационни системи, като предоставя информация за процесите в своя ресор.

(3). Функции на Ръководител направление ИКТ. **Ръководителят на направление ИКТ** (или определен ИТ специалист) осъществява технически и оперативен контрол върху функционирането на информационните системи и мрежи в училището.

Ръководителят на направление ИКТ отговаря за:

1. Поддръжка на **ИТ инфраструктурата** (сървъри, локална мрежа, хардуер) и осигуряване на нейната **непрекъсната и сигурна работа**.
2. Контрол върху прилагането на **политиките за мрежова и информационна сигурност** (антивирусни програми, защитни стени, актуализации) и предприемане на мерки за предотвратяване на киберзаплахи и неоторизиран достъп.
3. Управление на **потребителските акаунти и нивата на достъп** до информационните системи, включително **НЕИСПУО**, в съответствие със заповедите на директора.
4. Организиране на **архивирането (backup)** на критични данни и тестване на процедурите за възстановяване при срив.
5. Идентифициране на **най-важните ИТ компоненти**, анализ на заплахите за тяхната повреда или загуба, и предлагане на допълнителни контроли за подобряване на системата.

Чл. 10. Задължения на служителите

(1) Всеки служител е длъжен да уведомява незабавно своя пряк ръководител (Заместник-директора) или **Ръководителя на направление ИКТ** при възникване на проблем, свързан с информационните системи или сигурността на данните.

(2) Служителите спазват стриктно правилата за работа с лични данни, конфиденциална информация и ползване на служебни технически ресурси.

ГЛАВА III. ЕЛЕКТРОННО СЪЗДАВАНЕ, ОБРАБОТВАНЕ И ДВИЖЕНИЕ НА ДОКУМЕНТИ (Е-РАБОТЕН ПРОЦЕС)

Чл. 11. Основна система за информация

(1) Събирането, обработването, използването и съхраняването на информацията в СУ „П. Р. Славейков“ гр. Кричим се извършва основно чрез **Националната електронна информационна система за предучилищното и училищното образование (НЕИСПУО)**.

(2) Информацията, събирана от институцията, се обработва чрез **НЕИСПУО** и други информационни продукти, интегрирани с нея и обслужващи определени дейности или процеси в образованието.

(3) Документите, издавани или водени от институцията, се създават, водят и съхраняват в **електронен и/или хартиен вид**.

Чл. 12. Процедура по създаване и подаване на документи

(1) Създаването на документи в системата на училищното образование се организира от министъра на образованието и науката.

(2) Документите се попълват на **български книжовен език** (с изключение на темата на уроци по чужд език и учебни предмети, преподавани на чужд език).

(3) **Въвеждането и подаването на данни и документи в НЕИСПУО** се извършва с **квалифициран електронен подпис (КЕП)**, съгласно изискванията на Регламент (ЕС) № 910/2014.

(4) Директорът определя със заповед **длъжностните лица**, които събират, съхраняват и ползват информацията в **НЕИСПУО**.

Чл. 13. Електронно движение и обработка

(1) Електронното движение на документите се осъществява чрез модулите и регистрите на **НЕИСПУО**.

(2) Длъжностните лица са отговорни за **навременното и коректно въвеждане и обработка** на данни в **НЕИСПУО** в установените срокове (напр. подаване и утвърждаване на Списък-образец, приключване на работата по Лично образователно дело).

Процедури за създаване, обработка и обжалване на вътрешни административни документи.

ГЛАВА IV. АДМИНИСТРАТИВЕН И ВЪТРЕШЕН ДОКУМЕНТООБОРОТ (НЕЕЛЕКТРОНЕН)

Чл. 14. Обхват на административните документи

(1) Тази глава регулира създаването и движението на **Заповеди, Писма, Инструкции, Служебни бележки, Протоколи, Удостоверения**, както и други вътрешни административни документи, които не се водят в електронните модули на НЕИСПУО. (2) Всички административни документи се създават, обработват и съхраняват съгласно изискванията на **Закона за администрацията** и **Правилника за дейността на училището**.

Чл. 15. Процедура по създаване и оформяне

(1) **Оформяне**: Всеки административен документ трябва да съдържа:

1. Наименование на училището и/или лого.
2. Вид на документа (напр. Заповед, Инструкция).
3. **Уникален регистрационен номер и дата** на издаване (чрез деловодната система).
4. Точно, ясно и недвусмислено **съдържание** и правно основание (при Заповеди).
5. Име, длъжност и подпис на **издателя** (напр. Директора) и на **изготвилия** документа.

(2) **Заповеди**: Заповедите се издават от **Директора** и влизат в сила от датата на подписването им, освен ако в тях не е посочен друг срок. Те са задължителни за всички служители или за лицата, до които се отнасят.

(3) **Служебни бележки и Протоколи**: Служебните бележки и протоколите се изготвят от съответния служител/комисия, имат вътрешен характер и служат за удостоверяване на факти или документиране на дейности.

Чл. 16. (Свеждане до знанието на заинтересованите лица)

(1) **Документите, пораждащи права или задължения** (Заповеди, Инструкции), се свеждат до знанието на служителите по един от следните начини:

1. **Срещу подпис** в приложен към документа **списък/разписка**.
2. Чрез публикуване на **вътрешен информационен носител** (напр. табло за обяви, вътрешен мрежов ресурс), като се удостоверява датата на публикуване.
3. Чрез **служебна електронна поща**, ако получателят потвърди получаването.

(2) Счита се, че служителят е **запознат** с документа от датата, на която е положил подпис или от датата на публикуване/потвърждение.

Чл. 17. (Срок на действие и съхранение)

(1) **Срок на действие**: Документите имат действие до изричната им **отмяна** с нов документ или до изтичане на **срока**, посочен в тях (ако е приложимо)

(2) **Архивиране**: Оригиналите на административните документи (включително списъците за запознаване) се съхраняват във **фирменото деловодство/архив** съгласно вътрешната **Номенклатура на делата** и законовите изисквания за архивиране. Срокът за съхранение се определя от вида на документа (напр. Заповедите за уволнение/назначаване се съхраняват 50 години).

Чл. 18. (Обжалване на вътрешни административни актове)

(1) Всеки служител има право да **обжалва** или да направи **възражение** срещу издаден от Директора вътрешен административен акт (Заповед), който пряко засяга негови права или законни интереси.

(2) Жалбата/Възражението се подава до **Директора** в **7-дневен** срок от датата на запознаване с акта, освен ако в специален закон не е предвиден друг срок. (3) **Директорът** разглежда жалбата/възражението и се произнася в законоустановените срокове, като може да:

1. **Отмени** акта изцяло или отчасти.
2. **Измени** акта.
3. **Остави** акта в сила.

(4) Редът за обжалване на актове, издадени по **Кодекса на труда (КТ)** (напр. дисциплинарни заповеди), се извършва по реда, предвиден в КТ.

Чл. 19. (Съответствие и сигурност)

(1) При обработване и съхраняване на информация (включително лични данни) и документи, служителите са задължени да спазват:

1. **Регламент (ЕС) 2016/679 (GDPR)** и Закона за защита на личните данни.
2. **Наредбата за обмена на документи в администрацията** (ПМС № 101/2008), която регулира съхраняването на документи в електронен формат.
3. **Наредбата за минималните изисквания за мрежова и информационна сигурност** (ПМС № 186/2019).

ГЛАВА IV. КОНФИДЕНЦИАЛНОСТ И ЗАЩИТА НА ИНФОРМАЦИЯТА

Чл. 10. Дефиниране на Конфиденциална информация

(1) За конфиденциална се счита всяка информация, свързана с:

1. **Лични данни** на ученици, родители и служители, обработвани в **НЕИСПУО** или други училищни информационни системи.
2. Данни и документи, свързани с **финансова, търговска или служебна тайна** на институцията.
3. **Резултатите от извършения контрол** върху работата с информационните технологии, както и доклади от **анализа и оценката на риска** на критичните информационни системи.
4. Всяка друга информация, за която със заповед на Директора е определено, че е с ограничен достъп.
5. (2) Конфиденциалната информация подлежи на най-висока степен на защита и не следва да бъде разгласявана извън рамките на служебната необходимост.

Чл. 11. Задължения за поверителност на служителите

(1) Всеки служител, който има достъп до конфиденциална информация чрез информационните системи, е длъжен да спазва **абсолютна конфиденциалност** по отношение на тази информация.

(2) Служителите са длъжни:

1. Да използват конфиденциалната информация **единствено за целите на изпълнение на служебните си задължения**.
2. Да **не разкриват, копират или предоставят** достъп до конфиденциална информация на неупълномощени лица.
3. Да пазят в **тайна своите потребителски имена и пароли** за достъп до информационните системи и да ги променят периодично.

4. Да докладват незабавно на **Директора** и/или **Ръководителя на направление ИКТ** при установяване на нарушение на сигурността или неоторизиран достъп до конфиденциална информация.

Чл. 12. Защита на достъпа и данни

(1) Достъпът до информационните системи, съдържащи конфиденциална информация (вкл. НЕИСПУО), се осъществява само с **индивидуални потребителски акаунти**, които са създадени и разрешени със заповед на Директора.

(2) Предаването на **Квалифициран електронен подпис (КЕП)** за работа с НЕИСПУО на друго лице е **строго забранено** и представлява грубо нарушение на служебните задължения.

(3) При напускане на служител или промяна на длъжност, **достъпът до информационните системи се прекратява незабавно** от Ръководителя на направление ИКТ по нареждане на Директора.

Чл. 13. Отговорност при нарушаване на конфиденциалността

(1) Нарушаването на задълженията за конфиденциалност представлява **дисциплинарно нарушение** по смисъла на Кодекса на труда.

(2) При разкриване на лични данни в нарушение на Регламент (ЕС) 2016/679 (GDPR), служителят носи **имуществена и административно-наказателна отговорност**, съгласно Закона за защита на личните данни.

(3) **Ръководството**. Директорът и Заместник-директорите гарантира, че резултатите от вътрешния контрол и оценките на риска **няма да се разгласяват** от тях, като се използват единствено за целите на подобряване на сигурността и вътрешните контроли.**ГЛАВА VI. ДОПУСТИМО ПОЛЗВАНЕ НА ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ ЗА ЛИЧНИ ЦЕЛИ**

Чл. 14. Принцип на ползване

(1) Всички **информационни системи**, **технически ресурси** (компютри, лаптопи, таблети, принтери) и **комуникационни канали** (Интернет, служебна електронна поща) на Седмо СУ „Кузман Шапкарев“ Благоевград са предназначени преди всичко за **изпълнение на служебните задължения** на служителите и за осигуряване на нормалния учебен и административен процес.

(2) Ползването на ИТ ресурсите за лични цели **не е право**, а **допустимо изключение**, което трябва да бъде инцидентно, дискретно и да не накърнява интересите на институцията.

Чл. 15. Условия за допустимо ползване

(1) Информационните системи и техническите ресурси могат да се ползват от служителите за лични цели, при условие че са спазени **едновременно** следните изисквания:

1. Ползването е **инцидентно, рядко** и е ограничено до **кратък период от време** (напр. кратка справка или проверка).
2. Ползването се извършва **извън работно време** на служителя (напр. по време на почивки, преди или след края на работния ден).

3. Ползването **не пречи на работата** на служителя, на други служители, нито на нормалното функциониране на информационните системи и мрежата.
4. Ползването **не води до допълнителни разходи** за училището (напр. закупуване на софтуер, консумативи, превишаване на абонаментни планове).
5. Ползването **не компрометира** мрежовата и информационната сигурност на училището.

Чл. 16. Недопустими действия при лично ползване

(1) Категорично **се забранява** използването на ИТ ресурсите на училището за лични цели, ако тези действия попадат в следните хипотези:

1. **Инсталиране, изтегляне или разпространяване** на нелицензиран софтуер, файлове или програми, които могат да въведат **вируси, зловреден код** или да нарушат целостта на училищната мрежа.
2. **Извършване на дейности**, които могат да доведат до **конфликт на интереси** или да накърнят авторитета и репутацията на институцията (напр. хазарт, политическа агитация, създаване на съдържание с неетично или незаконно естество).
3. Достъп до **порнографско, нелегално или екстремистко** съдържание.
4. Използване на служебната **електронна поща** за абонамент към лични или маркетингови услуги или за масово разпращане на верижни писма.
5. Използване на училищния интернет трафик за **теглене на големи по обем файлове** (филми, игри) или за продължително използване на платформи, изискващи голям мрежов капацитет.

Чл. 17. Мониторинг и контрол

(1) Директорът и **Ръководителят на направление ИКТ** имат право да осъществяват **технически мониторинг** на използването на информационните системи, мрежовия трафик и служебната електронна поща, за да гарантират спазването на тази Инструкция и за целите на **мрежовата и информационна сигурност**.

(2) Служителите са информирани и приемат, че **нямат очаквания за поверителност** по отношение на всяка информация, създадена, съхранявана, изпратена или получена чрез училищните ИТ ресурси.

(3) Установени нарушения на правилата за допустимо ползване могат да доведат до **дисциплинарна отговорност**, съгласно Кодекса на труда.

ГЛАВА VII. ЗАБРАНИ ЗА ПОЛЗВАНЕ НА ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ

Чл. 18. Общи забрани

(1) Този списък на забранените дейности е **неизчерпателен** и СУ „П. Р. Славейков“ гр. Кричим може да добавя допълнителни ограничения чрез заповеди на Директора.

(2) Категорично се забранява ползването на компютърните и информационните системи на СУ „П. Р. Славейков“ гр. Кричим за всяка дейност, която е **незаконна, неетична** или **противоречи** на мисията и вътрешния правилник на институцията.

Чл. 19. Забрани, свързани със сигурността и интегритета на системите

(1) **Заобикаляне на системите за сигурност**: Забранява се всякакъв опит за заобикаляне, деактивиране или компрометиране на въведените системи за сигурност, с цел разрушаване, намаляване на сигурността или неоторизиран достъп до:

1. Училищната **локална мрежа** (LAN).
2. **Сървъри и бази данни** (включително НЕИСПУО).
3. Защитни стени, антивирусни програми и филтри.

(2) **Неоторизиран софтуер и промени**: Забранява се **свалянето, инсталирането или стартирането** на компютърни програми, приложения, скриптове или настройки от Интернет или външни носители **без изричното писмено разрешение** на **Ръководителя на направление ИКТ** или оторизиран ИТ специалист.

(3) **Неправомерно копиране**: Забранява се **копирането** на **лицензираните компютърни програми** на училището, операционни системи или вътрешни програми, създадени за нуждите на институцията, **с цел лична употреба** или предоставяне на трети лица.

(4) **Зловредни действия**: Ползването на компютърните ресурси за извършване на **престъпление** или за подготовка на такова (включително кибертормоз, кражба на самоличност, фишинг, разпространение на зловреден софтуер).

Чл. 20. Забрани, свързани с електронната поща и комуникацията

(1) **Подправяне на самоличност (Spoofing)**: Забранява се подправянето на електронна поща с цел **скриване на самоличността** на подателя, **фалшифициране** на тази самоличност или изпращане на съобщения от името на друг служител или ръководител.

(2) **Служебна електронна поща**: Служебната електронна поща на училището **не може да се ползва** за:

1. **Комерсиални лични цели** или за подпомагане на бизнес, който не е свързан с дейността на СУ „П. Р. Славейков“ гр. Кричим.
2. Разпространение на **религиозни или политически** материали и агитация.
3. Изпращане на **масова непоискана кореспонденция** (спам).

(3) **Подпис на кореспонденцията**: Всички електронни писма, пращани от служителите по служебна кореспонденция, трябва да бъдат коректно и ясно подписани с **име, фамилия и длъжност** на подателя.

Чл. 21. Забрани, свързани с неслужебни дейности

(1) **Политическа дейност**: Забранява се ползването на компютърните системи и служебната мрежа за **политическа дейност**, която пряко или косвено би подпомогнала кампанията за избиране на даден кандидат или политическа партия.

(2) **Комерсиална употреба**: Забранява се използването на ресурсите за **подпомагане дейността на частна компания, нейните продукти, услуги или бизнес практика**, освен ако това не е изрично разрешено от Директора и е част от официална училищна инициатива.

(3) **Недопустимо съдържание**: Забранява се **свалянето** от Интернет и съхранението на **аудио и видео файлове, MP3 файлове, филми или игри**, които не са пряко свързани с учебния процес или служебните задължения.

ГЛАВА VIII. РАЗКРИВАНЕ НА ИНФОРМАЦИЯ И ОТГОВОРНОСТ

Чл. 22. Неоторизирано разкриване

(1) **Неоторизираното разкриване** на служебна информация, която е получена или обработвана в информационните системи на СУ „П. Р. Славейков“ гр. Кричим, представлява сериозно нарушение на задълженията за **конфиденциалност** и може да доведе до:

1. **Негативни финансови и правни последици** за институцията.
2. **Накърняване на имиджа и репутацията** на училището пред обществеността и други институции.
3. Нарушаване на **правата и свободите** на физическите лица (ученици, родители, служители) в контекста на защитата на личните данни (GDPR).

Чл. 23. Обхват на забраната за разкриване

(1) **Забранява се** разкриването или предоставянето на информация, получена чрез служебен достъп до ИТ системите, на лица, които нямат **служебна необходимост** от нея или **не са упълномощени** да я получат, включително, но не само:

1. **Лични данни** на ученици, родители или служители (адреси, ЕГН, здравна информация, данни от ЛОД).
2. **Вътрешни административни актове**, които не са предназначени за публичност.
3. **Технически данни** за мрежата, пароли, системни настройки или резултати от одити по сигурността.

(2) Разкриването на информация може да бъде извършено само след **изрично писмено разрешение** на Директора или когато то е **нормативно установено** (напр. предоставяне на информация на контролни органи).

Чл. 24. Отговорност при злоупотреба с информация

(1) Служител, който **копира, използва или разкрива** информация от локалната мрежа или информационните системи на училището **за лична изгода** или с цел **причиняване на вреда** на училището или на трети лица, носи:

1. **Дисциплинарна отговорност** по реда на Кодекса на труда, като нарушението може да бъде основание за налагане на най-тежкото наказание.
2. **Имуществена отговорност** за причинени преки и непосредствени вреди, съгласно българското законодателство.
3. **Административно-наказателна или наказателна отговорност** в зависимост от характера на нарушението (напр. при неправомерно разкриване на лични данни).

ГЛАВА IX. АНТИВИРУСНА ЗАЩИТА И ПРЕВЕНЦИЯ

Чл. 25. Заплаха от компютърни вируси

(1) Компютърните вируси, зловредният софтуер (malware), рансъмуерът (ransomware) и другите киберзаплахи представляват **голяма и постоянна заплаха** за всички потребители на ИТ услуги в СУ „П. Р. Славейков“ гр. Кричим и за целостта на училищната информация.

(2) **Компютърният вирус** е програма, която се задейства на даден компютър и се разпространява към други дискове, програми и мрежови ресурси, които са в контакт със заразеното устройство.

(3) Вирусът може да причини **блокиране на компютъра**, да **промени или унищожи бази данни**, да направи някои данни **невъзможни за ползване** или да компрометира цялата мрежа.

Чл. 26. Правила за превенция и защита

(1) **Обучение и информираност**: Служителите трябва да имат необходимите **знания** как вирусите се разпространяват (чрез прикачени файлове, компрометирани уебсайтове, външни носители) и каква вреда могат да нанесат.

(2) **Задължения на Ръководителя на направление ИКТ**:

1. Да осигури **централизирана, актуална и лицензирана антивирусна защита** на всички служебни компютри и сървъри.
2. Да следи за **редовното обновяване (пачове)** на операционните системи и критичния софтуер.
3. Да прилага **политики за мрежова сигурност** (напр. филтриране на опасни прикачени файлове в електронната поща).

(3) **Задължения на служителите**:

4. Да **не деактивират** или променят настройките на инсталираната антивирусна програма.
5. Да **не отварят** прикачени файлове или хипервръзки от **непознати или подозрителни податели** в електронната поща (особено тези, които изискват въвеждане на парола).
6. Да сканират за вируси всички **външни носители** (USB флаш памети, външни дискове) преди тяхното използване в училищни компютри.
7. При съмнение за инфекция или нетипично поведение на компютъра, служителят трябва **незабавно да уведоми Ръководителя на направление ИКТ** и да спре работата си с машината.

ГЛАВА X. ОРГАНИЗАЦИЯ НА ЗАЩИТАТА ОТ ВИРУСИ

Чл. 27. Отговорност за антивирусната защита

(1) **ИТ специалистите** (или Ръководителят на направление ИКТ) на СУ „П. Р. Славейков“ гр. Кричим носят **пълната техническа отговорност** за:

1. **Избор, инсталиране и конфигуриране** на централизираната антивирусна програма на училищно ниво.
2. Осигуряване на **редовна и автоматична актуализация** (ъпдейт) на дефиниционните файлове на антивирусния софтуер на всеки индивидуален компютър.
3. Поддръжка на **лицензите** за антивирусния софтуер, за да се гарантира непрекъснатата му работа.
4. (2) Служителите имат **задължението да следят** дали техният антивирусен софтуер се **осъвременява** и при съмнение за технически проблем с актуализацията (напр. липса на актуализация повече от седмица), **незабавно да информират** ИТ специалиста.

Чл. 28. Процедура за действие при вирусна атака

(1) Служителите трябва да приемат всяко **съобщение или индикация за вирус** или зловреден софтуер изключително сериозно и да следват установената процедура за реакция:

1. **Незабавно информиране**: Служителят трябва **незабавно да информира** своя пряк ръководител (Заместник-директора) и **ИТ специалиста**.
2. **Спиране на действията**: Служителят **не трябва да предприема никакви самостоятелни действия** за отстраняване на вируса, а да остави компютъра във вида, в който е установен проблемът.
3. **Изолиране**: При възможност и по указание на ИТ специалиста, компютърът може да бъде **физически изолиран** от мрежата, за да се предотврати разпространението на заразата.
4. (2) Преднамереното **разпространяване на данни, за които служителят знае, че са заразени**, е **грубо нарушение** на служебните задължения и се санкционира по дисциплинарен ред.

Чл. 29. Правила за работа с файлове и софтуер

(1) **Сваляне на файлове**: На служителите е **разрешено да свалят файлове** от външни източници на училищната мрежа **само във връзка с тяхната служебна работа** и при спазване на правилата за сканиране, посочени в тази инструкция.

(2) **Инсталиране на софтуер**: **Не е разрешено** на служителите да инсталират каквито и да е **програмни продукти** (включително игри, помощни приложения или драйвери) **без предварителното писмено разрешение** на ИТ специалистите, тъй като това създава опасност от заразяване с вируси или нарушаване на стабилността на системата.

Чл. 30. Защита на електронната поща

(1) **Входящата електронна поща** трябва да се третира с **особено внимание** поради потенциалната възможност да бъде основен вектор за разпространение на вируси и фишинг атаки.

(2) **Работа с прикачени файлове**: Отварянето на приложения (прикачени файлове) да се прави **САМО** след като антивирусната програма е **автоматично ги е сканирала** и е установила тяхната безопасност.

(3) **Непознати податели**: Електронни писма, получени от **неизвестни податели**, трябва да се **изтриват незабавно** и в никакъв случай да не се отварят прикачени файлове или хипервръзки, съдържащи се в тях.

(4) **Подозрителни файлове**: Всяко получаване на файл с разширение, което е нетипично или подозрително (**напр. .exe, .bat, .scr, .zip, .7z, .rar**, ако не се очаква), трябва да бъде докладвано на ИТ специалиста.

ГЛАВА XI. АРХИВИРАНЕ НА ИНФОРМАЦИЯТА (BACKUP)

Чл. 31. (Необходимост от архивиране) (1) Сривовете в компютърното оборудване, вирусните атаки, рансъмуерът и случайното изтриване на файлове могат да причинят **необратима загуба на критични данни**. Поради това е **жизненоважно** информацията във всяка компютърна система на училището да бъде редовно архивирана. (2) **Целта** на архивирането и възстановяването е да се **възстанови работата възможно най-бързо** и пълноценно в случай на прекъсване по технически или злонамерени причини, като по този начин се **минимизират възможните проблеми и загуби** за учебния и административния процес.

Чл. 32. (Отговорност за архивиране) (1) **Централизирано архивиране**: **ИТ специалистите** (или Ръководителят на направление ИКТ) отговарят за централизираното архивиране на **критични системи** (напр. сървъри, НЕИСПУО, деловодна система) и за **тестване на процедурата за възстановяване**. (2) **Локално архивиране**: Всяко звено (канцелария, счетоводство, методически обединения) в СУ „П. Р. Славейков“ гр. Кричим , съгласувайки с ИТ специалистите, трябва да има **адекватна система за локално архивиране** на данните от своята работа на технически носители (външни дискове, вътрешни мрежови хранилища).

Чл. 33. Честота и носители

(1) **Честота на архивирането**: Честотата на архивирането се определя от Директора в **писмена процедура** или заповед и тя зависи от **броя на транзакциите** и тяхната **значимост** за системата (напр. ежедневна за счетоводство, седмична за общи административни документи).

(2) **Минимално изискване**: Задължително в СУ „П. Р. Славейков“ гр. Кричим , пълен **архив** на всички критични данни се прави **поне веднъж месечно**.

(3) **Носители**: Архивното копие трябва да се съхранява на **отделен носител**, който не е постоянно свързан към основната мрежа (off-line backup), за да се защити от разпространение на рансъмуер.

Чл. 34. Съхранение на архивите

(1) **Продължителността на съхранение** на архивите се определя в **Наредбата за деловодната дейност** или в Заповед на Директора, като се съобразява с минималните

срокове, установени в **Наредба № 8** (за документи, свързани с ЛОД) и други нормативни актове.

(2) **Физическо съхранение**: Архивни копия трябва да се съхраняват на **защитено място**, което е различно от мястото, където се намира основното оборудване, за да се предпазят от пожар, наводнение или физическа кражба.

(3) **Проверка**: ИТ специалистът трябва **периодично да проверява** целостта на архивните копия и да тества процедурите за възстановяване, за да гарантира, че данните могат да бъдат възстановени при необходимост.

ГЛАВА XII. ДОСТЪП И УПРАВЛЕНИЕ НА ПАРОЛИТЕ

Чл. 35. Предоставяне на достъп

(1) Учителите и служителите от СУ „П. Р. Славейков“ гр. Кричим получават достъп до **локалната мрежа** и до **всички информационни системи и програми**, които са им необходими **единствено за изпълнение на служебните им задължения**.

(2) Достъпът до дадена програма, база данни (вкл. НЕИСПУО) или мрежови ресурс се дава на **конкретен служител** по силата на заповед на Директора и **не може да се прехвърля** на друго лице.

(3) **Ръководителят на направление ИКТ** отговаря за създаването, предоставянето и премахването на потребителските акаунти, както и за определяне на **нивата на достъп** (права за четене, писане, редактиране) според длъжностната характеристика на служителя.

Чл. 36. Поверителност на паролите

(1) Учителите и служителите от СУ „П. Р. Славейков“ гр. Кричим трябва да пазят своите **лични пароли в абсолютна тайна**.

(2) **Строго се забранява**:

1. **Споделянето** на пароли с колеги, ученици, родители или други познати.
2. **Записването на пароли на хартия** (бележки, стикери) и оставянето им на работното място (около компютъра, под клавиатурата или в незаключени чекмеджета).
3. Използването на пароли, които са **лесни за отгатване** от колегите или трети лица (напр. собствено име, име на дете, рождена дата, думата "парола").

Чл. 37. (Изисквания към сигурността на паролите)

(1) Когато даден продукт или информационна система изисква парола, служителите трябва да спазват следните задължителни правила:

1. **Първоначална промяна**: Служителите трябва да **променят първоначалната парола** (обикновено генерирана от системата) и да създадат своя **индивидуална** при първото влизане в съответната информационна система.
2. **Дължина и сложност**: Паролите трябва да са **поне от 8 знака** (актуално изискване за сигурност), като е силно препоръчително да включват комбинация от: **големи букви, малки букви, цифри и специални символи**.

3. **Забрана за повторение**: При периодична промяна на паролата **не трябва да се използват стари**, вече използвани пароли (системите трябва да не позволяват повторното използване на последните 5-10 пароли).
4. **Срок на валидност**: Ако е необходимо, паролите трябва да се сменят на определена честота (**препоръчително на всеки 90 дни**, но най-малко веднъж на 6 месеца) за критични системи като НЕИСПУО.

Чл. 38. Контрол на достъпа

(1) Системите трябва да бъдат настроени така, че да **не позволяват** един и същи потребител да се включи в **няколко компютъра едновременно** с една и съща парола, за да се гарантира проследимост и сигурност.

(2) При **3 или повече неуспешни опита** за влизане в дадена програма, системата трябва **автоматично да блокира** достъпа на потребителя за определен период от време (напр. 30 минути) или до намеса на ИТ специалист.

Чл. 39. Процедура при забравена парола

(1) Ако учителят или служителят **забравят своята парола**, те трябва незабавно да уведомят:

1. **Оторизирания Заместник-директор** (за административен контрол).
2. Да се свържат с **ИТ специалиста** (или Ръководителя на направление ИКТ) на СУ „П. Р. Славейков“ гр. Кричим за техническо съдействие.
3. (2) **ИТ специалистът** е единственото лице, което има право да **нулира или генерира временна парола**, като тази процедура трябва да се документира. Служителят е длъжен да смени временната парола веднага след първото влизане.

ГЛАВА XIII. ИНТЕРНЕТ

Чл. 40. (Насърчаване на служебното ползване) (1) Ръководството на СУ „П. Р. Славейков“ гр. Кричим насърчава ползването на Интернет от служителите за **служебни цели**, като:

1. Обмяна на информация и комуникация с колеги и външни партньори.
2. Извършване на **проучвания и събиране на данни** във връзка с учебната, възпитателната и административната дейност.
3. Достъп до **Националната електронна информационна система за предучилищното и училищното образование (НЕИСПУО)** и други официални държавни и образователни портали.

Чл. 41. (Отговорност за уместна употреба)

(1) **Заместник-директорите** и други оторизирани длъжностни лица отговарят за контрола върху **уместната и етична употреба** на интернет ресурсите от служителите в техния ресор.

(2) Служителите са задължени да ползват Интернет ресурсите по начин, който **не създава риск** за сигурността на училищната мрежа и **не нарушава** вътрешните правила, особено по отношение на Глава VII. Забрани за ползване на информационните технологии.

Чл. 42. Ограничения при ползване на Интернет

(1) **Сваляне на файлове**: Категорично се **забранява свалянето** от Интернет на **аудио, видео файлове** (с изключение на тези, необходими за пряко изпълнение на учебния процес и при спазване на авторските права) или други големи по обем мултимедийни файлове.

(2) **Инсталиране на софтуер**: **Не е разрешено** свалянето и инсталирането на **програмни продукти** (приложения, игри, помощни програми) от Интернет **без предварителното одобрение** на **ИТ специалистите** на СУ „П. Р. Славейков“ гр. Кричим.

(3) **Контрол на трафика**: Интернет трафикът може да бъде **филтриран и наблюдаван** от ИТ специалистите с цел:

1. Предотвратяване на достъп до **незаконно или неподходящо** съдържание (порнография, екстремизъм, хазарт).
2. Ограничаване на използването на **мрежовия капацитет** за лични цели, които забавят служебната работа.

ГЛАВА XIV. ЕЛЕКТРОННА ПОЩА

Чл. 43. (Предназначение и ограничения) (1) Служебната електронна поща (e-mail) на СУ „П. Р. Славейков“ гр. Кричим е предназначена **само за служебна кореспонденция** и **не може да се ползва** за:

1. **Комерсиални цели** или за подпомагане на **частен бизнес** и дейности, които не са свързани с мисията на училището.
2. **Религиозни или политически цели** или за подпомагане на кампании за избиране на даден кандидат.
3. Разпращане на **масова непоискана кореспонденция** (спам, верижни писма).

Чл. 44. (Изисквания към подателя и съдържанието) (1) **Забрана за фалшифициране**: **Забранява се подправянето** на електронна поща с цел скриване на самоличността на подателя или фалшифициране на тази самоличност. (2) **Личен подпис**: Всички електронни писма, пращани от служителите, трябва да бъдат **лично и коректно подписани** (име, длъжност, институция). (3) **Адрес на получателя**: Служителите трябва да **проверяват внимателно точния адрес** на получателите на официални писма, **особено тези с прикачени файлове**, съдържащи важна или конфиденциална информация, за да не бъде изпратена по погрешка на непознати лица.

Чл. 45. (Управление на пощата и сървърите) (1) **Изтриване на неформални съобщения**: **Неформалните съобщения**, които не са от официален характер, трябва да се **трият регулярно** от пощата, за да не се товарят сървърите на СУ „П. Р. Славейков“ гр. Кричим . (2) **Съхранение на важна кореспонденция**: Всички **важни съобщения**, които имат отношение към дейността на училището и документооборота, трябва да се **пазят** в електронната поща в специални папки, а при необходимост и на хартиен носител, съгласно правилата за архивиране (Глава XI). (3) **Проверка на пощата**: Служителите са задължени да **проверяват служебната си електронна поща** ежедневно, за да не пропускат важни служебни съобщения и указания.

Радвам се, че приключваме с детайлизирането на **Инструкцията за организационните процедури при използването на информационните системи**!

Ето и разработените последни глави, включващи **Лице за контакт** и **Допълнителни/Заключителни разпоредби**, които финализират документа.

ГЛАВА XV. ЛИЦЕ ЗА КОНТАКТ И ТЕХНИЧЕСКА ПОДДРЪЖКА

Чл. 46. (Лице за контакт) (1) **ИТ специалистите** (или **Ръководителят на направление ИКТ**) на СУ „П. Р. Славейков“ гр. Кричим са определените **лица за контакт** по всички технически въпроси, свързани с работата на компютърните системи, мрежата и информационните продукти. (2) Служителите са задължени да **насочват всички технически проблеми и запитвания** към ИТ специалистите, включително:

1. Сривове в хардуера или софтуера.
2. Проблеми с мрежовия достъп или интернет връзката.
3. Съмнения за **вирусна инфекция** или инциденти със сигурността.
4. Проблеми с достъпа и паролите (след уведомяване на Заместник-директора).
5. Необходимост от инсталиране на служебен софтуер или сваляне на файлове. (3) ИТ специалистите отговарят за **навременното отстраняване на техническите проблеми** и за осигуряването на **техническа поддръжка** на служителите.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. Оценка на риска на информационните системи

(1) При извършване на **самооценката на вътрешните контроли** на СУ „П. Р. Славейков“ гр. Кричим, задължително се включва **анализ и оценка на риска** на критичните информационни системи (напр. НЕИСПУО, счетоводна система, локална мрежа).

(2) **Целта** на оценката на риска е да се:

1. **Идентифицират** най-важните компоненти (оборудване, програми, бази данни) и техните зависимости.
2. Определят **заплахите** за тяхната повреда или загуба и **последиците** от това за дейността на училището.
3. Анализират **наличните контроли** за предотвратяване на потенциалните проблеми.
4. Предложат **допълнителни контроли**, които са необходими за подобряване на системата.

§ 2. Участници в оценката на риска (1) В процеса на оценка на риска участват задължително **ИТ специалистите** и **Ръководството** (Директор и Заместник-директори), тъй като те притежават както техническото познание, така и знанието за критичните бизнес процеси. (2) Оценката на риска обхваща:

1. **Извършеното** и **моментното състояние** на информационната сигурност.
2. **Мерките за подобряване** на слабите места във вътрешните контроли и необходимите ресурси.
3. **Остатъчният риск** за СУ „П. Р. Славейков“ гр. Кричим, който контролите не могат да елиминират напълно.

§ 3. Изисквания при разработване на нов софтуер (1) При създаването на **програмен продукт** специално за нуждите на СУ „П. Р. Славейков“ гр. Кричим, е необходимо още при **задаването на неговите параметри на доставчика** да се заложат **основните контролни функции и изисквания за сигурност** (напр. управление на пароли, нива на достъп, одит пътеки), които този продукт трябва да притежава по дизайн.