МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО
ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ – ШУМЕН
9700 гр. Шумен, ул."В. Априлов" № 63, тел. Директор 054/800327
тел. гл. счетоводител 800328, факс 800327, e-mail csmp@ro-in.net

ЗАПОВЕД

№ РД-01-611/04.08.2026 г.

Във връзка със Заповед № РД-04-35/29.07.2026 год. на Министъра на здравеопазването

УТВЪРЖДАВАМ:

Вътрешни правила за мрежовата и информационната сигурност на ЦСМП – Шумен.

Контрола по изпълнение на настоящата заповед да се осъществява от директор ЦСМП – Шумен и консултант-системен администратор на компютърни системи.

Препис от настоящата заповед да се сведе до знанието и изпълнението на всички служители от ЦСМП – Шумен, работещи с информационни компютърни системи срещу подпис.

Д-Р ЕНЧО ВАСИЛЕВ
Директор ЦСМП – Шумен

МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО

ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ – ШУМЕН

9700 гр.Шумен ул. „Васил Априлов“ № 63, тел. Директор 054/ 800 327

тел. Гл.счетоводител 800 328, факс 800 327, *e-mail csmp@ro-ni.net*

Утвърждавам:
Директор: /д-р Е. Василев /

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ НА ЦСМП - ШУМЕН

РАЗДЕЛ I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в ЦСМП - Шумен. В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от администрацията или с общо предназначение.

Чл. 2. Потребителите на информационни системи в ЦСМП - Шумен са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредба за общите изисквания за мрежова и информационна сигурност.

РАЗДЕЛ II
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.4. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

(1) разделяне на потребителски от администраторски функции;

(2) установяване на нива и достъп до информация;

(3)регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

(4) осъществяването на контрол от Директора на ЦСМП – Шумен и консултант-системен администратор на компютърни системи.

Чл. 5. Всеки служител има точно определени права на достъп и използва КЕП или уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили;

Чл. 6. Системният администратор на определен програмен продукт или онлайн платформа, предоставят достъп на служителите, като се задават определени права до конкретни информационни ресурси, според заемната длъжност и функция. Не се предоставя достъп на неоторизирани лица.

Чл. 7. Лицата, които обработват лични данни, използват КЕП или уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

Чл. 8. Всички пароли за достъп се променят периодично;

Чл. 9. Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл. 10. На служителите на ЦСМП - Шумен, които използват електронни бази данни и техни производни (текстове, кореспонденция и аудио записи) се забранява:

(1) да ги изнасят под каквато и да е форма извън служебните помещения без разрешение на Директора на ЦСМП - Шумен;

(2) да ги използват извън рамките на служебните си задължения;

(3) да ги предоставят на външни лица без да има регистрирано такова искане в деловодството.

Чл. 11. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

РАЗДЕЛ III
УПРАВЛЕНИЕ НА ИНЦИДЕНТИ И ДОКЛАДВАНЕ

Чл. 12. При установяване на значим инцидент, застрашаващ сигурността на мрежите или непрекъснатостта на спешната медицинска помощ, ЦСМП – Шумен спазва следните срокове за уведомяване на Националния CERT (ЕРИКС):

1. Ранно предупреждение: в срок до 24 часа от узнаването за инцидента.
2. Уведомление за инцидент: в срок до 72 часа, включващо първоначална оценка на мащаба и въздействието.
3. Месечен доклад: в срок до един месец след подаване на уведомлението, описващ причините и предприетите коригиращи мерки.

РАЗДЕЛ IV
РАБОТНО МЯСТО

Чл.13. Работното място се състои от работно помещение, работна маса и стол, компютърна и периферна техника, комуникационни средства.

Чл.14. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл.15. Сървъри на локални компютърни мрежи се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за мрежова и информационна сигурност.

Чл.16. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него данни на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл.17. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява посредством КЕП или въвеждането на персонално потребителско име и парола;

Чл.18. Забранява се работата на външни лица с компютърните конфигурации на ЦСМП - Шумен, освен в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствието на служител от ЦСМП - Шумен.

Чл.19. След края на работния ден всеки служител задължително изключва компютъра;

Чл.20. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява консултант-системен администратор на компютърни системи, който му оказва съответна техническа помощ;

Чл.21. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват достъпа на трети лица до служебна информация;

Чл.22. Инсталиране и разместване на компютърни конфигурации и части от тях се извършва само след съгласуване с консултант-системен администратор на компютърни системи;

Чл.23. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на ЦСМП – Шумен, без знанието на Директора на ЦСМП или на консултант-системния администратор на компютърни системи.

Чл.24. Служителите имат право да обменят компютърна информация посредством външни носители, имейли и комуникационни канали само във връзка с изпълнение на служебните си задължения;

Чл.25. Достъпът до помещенията, където са разположени сървърите и комуникационните шкафове се ограничава само до консултант-системен администратор на компютърните системи, отговорници на филиали, както и специализиран по поддръжката им персонал, след легитимация, посредством служебни карти.

РАЗДЕЛ V
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл.26. Консултант-системния администратор компютърни системи извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронните пощи на ЦСМП – Шумен.

Чл.27. Ползването на компютърната мрежа и електронните пощи от служителите става чрез получените потребителско име и парола.

Чл.28. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл.29. Компютрите, свързани в мрежата на ЦСМП - Шумен използват интернет само от доставчик, с когото ЦСМП - Шумен има сключен договор за доставка на интернет;

Чл.30. Забранява се свързването на компютри едновременно в мрежата на ЦСМП - Шумен и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на ЦСМП - Шумен и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и Наредба за общите изисквания за мрежова и информационна сигурност

Чл.31. Забранява се отварянето без контрол от страна на консултант-системния администратор на компютърни системи:

1. получени по електронна поща или на преносими носители изпълними файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;
2. получени по електронна поща съобщения, които съдържат неразбираеми знаци.
3. съобщения, за които има съмнение, че са фишинг опити, целящи събиране на лични данни, пароли или финансова информация чрез препращане към фалшиви уеб страници.

Чл.32. (1)Използването на двуфакторна автентикация е задължителна за служебната електронна поща:

csmp@ro-ni.net
csmp-shumen@mh.government.bg

(2) Двуфакторната автентикация при опит за вписване в служебните пощи, се осъществява посредством приложение достъпно само на консултант-системния администратор на компютърни системи, който удостоверява входа.

РАЗДЕЛ VI
ОБУЧЕНИЕ, КИБЕРХИГИЕНА И ОТГОВОРНОСТ НА РЪКОВОДСТВОТО

Чл. 33. Задължително обучение на ръководството

(1) Директорът на ЦСМП – Шумен преминава периодично специализирано обучение, насочено към разпознаване на рисковете в областта на мрежовата и информационната сигурност и методите за управление на тези рискове.

(2) Обучението по ал. 1 се провежда най-малко веднъж на две години или при настъпване на съществени промени в нормативната уредба по киберсигурност.

Чл. 34. Инструктаж и подготовка на служителите:

(1) Всички служители на ЦСМП – Шумен преминават първоначален инструктаж по мрежова и информационна сигурност при постъпване на работа и последващи периодични обучения (най-малко веднъж годишно).

(2) Обученията обхващат следните задължителни теми:

1.Разпознаване на опити за социално инженерство и фишинг атаки;

2.Правила за сигурност при работа с електронна поща и интернет;

3.Сигурно управление на пароли и използване на многофакторна автентикация (MFA);

4.Процедури за незабавно докладване при съмнение за киберинцидент.

Чл. 35. Правила за киберхигиена:

(1) Служителите са длъжни да спазват висока киберхигиена, включваща изключване на работните станции при напускане на работното място и използване на служебните ресурси само за целите на дейността на ЦСМП.

(2) Забранява се използването на служебните електронни адреси за регистрации в лични платформи, социални мрежи или други услуги, които не са пряко свързани с медицинската или административната дейност.

Чл. 36. С цел документиране на всяко проведено обучение или инструктаж се съставя протокол с присъствен списък, който се съхранява като доказателство за изпълнение на мерките за сигурност по Директива NIS2.

РАЗДЕЛ VII
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл.37. С цел антивирусна защита се прилагат следните мерки:

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) Консултант-системния администратор на компютърни системи извършва следните дейности:

1.активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

2.настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично.

3.проверява за правилно настроен софтуер за автоматично обновяване на операционната система и инсталирания софтуер;

(3) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира консултант-системния администратор на компютърни системи.

РАЗДЕЛ VIII
ОСИГУРЯВАНЕ НА НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл.38. Всички сървъри и устройства за съхранение на данни са свързани към устройство за непрекъсваемост на ел. снабдяването.

Чл. 39. Специфика при централизирани системи

(1) Поддръжката, архивирането и защитата на централизираните медицински информационни системи и бази данни се осъществяват от външни изпълнители, определени с договори от Министерство на здравеопазването (МЗ).

(2) ЦСМП – Шумен, в качеството си на ползвател, няма административен достъп до сървърната инфраструктура за извършване на самостоятелни архиви (backups).

(3) При установяване на системни грешки, невъзможност за достъп до данни или съмнение за компрометиране на информацията, консултанта по компютърни системи незабавно уведомява:

1. Поддържащата фирма (чрез официалния им канал за поддръжка/Helpdesk);
2. Директора на ЦСМП – Шумен.

(4) Всички сигнали за инциденти и отговорите от поддържащата фирма се описват, като доклад, изготвен от консултант-системния администратор на компютърни системи и се завеждат в Автоматизираната информационна система (АИС) „ Eventis R7 “, който служи за доказателство за положена грижа от страна на Центъра.

Чл. 40. При избор на нови външни доставчици на ИТ продукти или услуги (извън утвърдените от МЗ), ЦСМП – Шумен извършва предварителна оценка на техните мерки за сигурност и включва в договорите клаузи за задължително уведомяване при възникнал киберинцидент в техните системи.

РАЗДЕЛ IX
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Служителите на ЦСМП - Шумен са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от Директора на ЦСМП – Шумен и консултант-системен администратор на компютърни системи.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като може да се приемат и прилагат допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тези вътрешни правила са разработени в съответствие със Закона за киберсигурност, Наредбата за минималните изисквания за мрежова и информационна сигурност и Директива (ЕС) 2022/2555 (NIS2) и са утвърдени със заповед № РД-01-61/04.08.2026 год. на Директора на ЦСМП – Шумен.

Изготвил:
Неждет Мехмедов
Консултант, системен администратор на компютърни системи