ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ -ТЪРГОВИЩЕ
гр. Търговище, ул.”Петлешков №27,тел.факс:0601/639-71,т.0601/638-10
e-mail:csmptarg@elnics.com

З А П О В Е Д
№ РД-01-175
26.10.2026 г., гр. Търговище

На основание закона за киберсигурност, Наредбата за минималните изисквания за мрежова и информационна сигурност Директива/ЕС/ 2022/NIS2/Регламент/ЕС/2016/679, ЗЗЛД

Н А Р Е Ж Д А М:

1.Вътрешни правила за информационна сигурност при сключване, изменение и прекратяване на трудовите отношения.

Срок: постоянен
Отг.: ИУП и касиер-счетоводство

Контрол по заповедта нареждам да се осъществява от Главен счетоводител.

Настоящата заповед да се доведе до знанието на главен счетоводител, ИУП, касиер-счетоводство за сведение и изпълнение.

ДИРЕКТОР:
/Д-Р ЯНКА АНДРЕЕВА ИВАНОВА/

Т.5

Утвърдил:

Директор на ЦСМП – Търговище

ВЪТРЕШНИ ПРАВИЛА
за информационна сигурност при сключване, изменение и прекратяване на трудови правоотношения

ГЛАВА I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите правила уреждат изискванията за мрежова и информационна сигурност при назначаване на служители, промяна на длъжността или служебните им задължения и прекратяване на трудовите правоотношения в ЦСМП – Търговище.

(2) Правилата се прилагат за всички служители на центъра, включително медицински специалисти, диспечери в РКЦ, шофьори, административен, финансов и технически персонал, както и за лицата, на които е предоставен достъп до информационните активи на центъра по силата на договор.

Чл. 2. Основните цели на правилата са:

1. Предотвратяване на неправомерен достъп до информационните системи и служебната информация.
2. Защита на личните данни и информацията за здравословното състояние на пациентите.
3. Осигуряване на непрекъсваемост на спешната медицинска помощ и координацията на спешните екипи.
4. Ограничаване на риска от загуба, копиране, изменение или неправомерно разпространение на информация.
5. Осигуряване на проследимост на действията по предоставяне, промяна и прекратяване на достъпа.

Чл. 3. Правилата се прилагат във връзка със Закона за киберсигурност, Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Регламент (ЕС) 2016/679, Закона за защита на личните данни, Кодекса на труда и останалите приложими нормативни актове.

ГЛАВА II. ОТГОВОРНИ ЛИЦА

Чл. 4. Директорът на ЦСМП – Търговище:

1. Утвърждава настоящите правила и осигурява организацията за тяхното прилагане.
2. Определя лицата, които имат право да заявяват, одобряват и прекратяват достъпа до информационните системи.
3. Определя отговорностите на длъжностните лица при назначаване, преназначаване и прекратяване на трудовите правоотношения.
4. Осигурява предприемането на мерки при установени нарушения на информационната сигурност.

Чл. 5. Длъжностното лице, отговарящо за управлението на човешките ресурси или трудовите досиета:

1. Уведомява своевременно определените лица за предстоящо назначаване, изменение или прекратяване на трудово правоотношение.
2. Осигурява включването на задълженията за поверителност и относимите документи.
3. Организира подписването на декларации и документи за запознаване с вътрешните правила.
4. Документира изпълнението на необходимите действия при постъпване и напускане.

Чл. 6. Определеното длъжностно лице по мрежова и информационна сигурност, съвместно с техническия администратор, когато е приложимо:

1. Организира създаването, промяната, блокирането и прекратяването на потребителските профили.
2. Осигурява предоставянето на права само в необходимия за работата обхват.
3. Поддържа документация за предоставените и прекратените права за достъп.
4. Проверява наличието на активни профили на напуснали служители.
5. Докладва установените несоответствия и инциденти.

Прекият ръководител определя служебната необходимост от достъп съобразно длъжността и действителните работни задачи.

ГЛАВА III. ИНФОРМАЦИОННА СИГУРНОСТ ПРИ НАЗНАЧАВАНЕ

Чл. 7. Преди или при постъпване на работа се извършват следните действия:

1. Служителят се запознава с вътрешните правила за информационна сигурност и защита на личните данни.
2. Определя се необходимото ниво на достъп до помещения, документи, компютри, информационни системи и електронни регистри.
3. Предоставят се индивидуални потребителски профили, когато работата иззисква използване на информационни системи.

4. На служителя се предоставят само правата, необходими за изпълнение на конкретните му задължения.

5. Провежда се инструктаж за безопасна работа с информационните системи, служебната електронна поща, паролите и личните данни.

6. При необходимост се предоставят служебни ключове, карти, компютърна техника и други средства за достъп срещу документирано приемане.

Чл. 8. (1) Достъпът до информация се определя според длъжностните задължения и принципа „необходимост да се знае“.

(2) На служители, които не участват в обработването на медицинска информация, не се предоставя достъп до нея, освен когато такъв е необходим за изпълнение на законово или служебно задължение и е надлежно разрешен.

(3) Достъпът до системите на РКЦ, медицинската документация, административните архиви и финансовите системи се предоставя отделно според конкретните функции на служителя.

Чл. 9. (1) Всеки служител е длъжен да пази в тайна паролите си и да не предоставя личния си потребителски профил на други лица.

(2) Забранява се използването на общи потребителски профили, когато системата позволява индивидуална идентификация и приложимите правила изискват такава.

(3) При съмнение за компрометирана парола служителят незабавно уведомява отговорното техническо лице.

(4) Служителите преминават първоначален и периодичен инструктаж, като провеждането му се документира.

Чл. 10. Служителят подписва декларация за поверителност и запознаване със задълженията за информационна сигурност. Задължението за поверителност продължава да се прилага и след прекратяване на трудовото правоотношение, доколкото произтича от закона или валидно поетите задължения.

ГЛАВА IV. ПРОМЯНА НА ДЛЪЖНОСТТА И ПРАВАТА ЗА ДОСТЪП

Чл. 11. При преместване, промяна на длъжността, временно възлагане на други функции или промяна на служебните задължения се извършва преглед на предоставените права за достъп.

Чл. 12. При промяна на длъжността:

1. Прекратяват се ненужните за новата длъжност права.
2. Предоставят се нови права след съответното разрешение.
3. При необходимост се променят правата за достъп до помещения, архиви и технически средства.
4. Промените се документират с посочване на датата, основанието и отговорното лице.

Чл. 13. Временно предоставените расширени или административни права се ограничават до необходимия срок и се прекратяват след отпадане на основанието за предоставянето им.

ГЛАВА V. ИНФОРМАЦИОННА СИГУРНОСТ ПРИ ПРЕКРАТЯВАНЕ НА ТРУДОВОТО ПРАВООТНОШЕНИЕ

Чл. 14. При прекратяване на трудовото правоотношение се организира своевременно и координирано прекратяване на достъпа на служителя до информационните активи на центъра.

Чл. 15. При напускане се извършват следните действия:

1. Блокиране или закриване на потребителските профили в информационните системи и корпоративната мрежа съобразно определената дата и час на прекратяване на достъпа.
2. Прекратяване на достъпа до служебната електронна поща, отдалечените връзки, облачните услуги и външните системи, когато са предоставени от центъра.
3. Отнемане на административните права и преглед на достъпите до споделени ресурси.
4. Връщане на служебните ключове, карти, техника, носители на информация и други средства за достъп.
5. Предаване на служебните документи, текущите задачи и информацията, необходима за продължаване на работата.
6. Проверка за наличие на служебни данни на предоставени устройства и носители.
7. Документиране на извършените действия в обходен лист или друг утвърден контролен документ.

Чл. 16. (1) Достъпът на напускащия служител се прекратява най-късно към момента, в който той вече няма право да го използва, като се отчита правното основание и моментът на прекратяване на трудовото правоотношение.

(2) При отстраняване от работа, съмнение за неправомерен достъп или установен инцидент директорът може да разпореди незабавно ограничаване на достъпа в рамките на своите правомощия.

(3) Действията по прекратяване на достъпа се извършват така, че да не се прекъсва работата на РКЦ и другите критични функции на центъра.

Чл. 17. (1) При прекратяване на договорните отношения със служител, който е имал достъп до административни пароли или други споделени секретни данни, се извършва оценка на необходимостта от смяна на съответните пароли и ключове.

(2) Паролите на административните профили се сменят при условията и в сроковете, предвидени в приложимите правила за мрежова и информационна сигурност, включително при прекратяване на отношенията с лица, които са ги знаели.

(3) Не се съхраняват пароли в явен текст в документацията за прекратяване на достъпа.

Чл. 18. (1) Служебната информация, създадена или получена от служителя при изпълнение на трудовите му задължения, остава под контрола на центъра.

(2) Не се допуска служителят да изнася, копира или задържа служебни документи, медицински фишове, списъци, бази данни или други информационни активи без правно основание и разрешение.

(3) Не се допуска автоматично изтриване на служебната електронна поща, документи или файлове при напускане. Запазването, архивирането и предоставянето на достъп до тях се извършват от упълномощени лица при спазване на правилата за защита на личните данни и сроковете за съхранение.

Чл. 19. Задълженията за защита на личните данни, медицинската тайна, служебната информация и поверителната информация продължават да се спазват и след прекратяване на трудовото правоотношение съобразно приложимото законодателство.

ГЛАВА VI. НАРУШЕНИЯ И ОТГОВОРНОСТ

Чл. 20. Служителите са длъжни незабавно да докладват на прекия си ръководител или на определеното лице по информационна сигурност за:

1. Неоторозиран достъп до системи, помещения или документи.
2. Загуба на служебно устройство, носител, ключ или карта за достъп.
3. Разкриване или неправомерно изпращане на лични данни.
4. Съмнение за компрометирана парола или зловреден софтуер.
5. Неизпълнение на действията по прекратяване на достъпа на напуснал служител.

Чл. 21. При нарушение се извършва проверка, документират се установените факти и се предприемат подходящи мерки съобразно тежестта на нарушението и приложимото законодателство.

Чл. 22. Дисциплинарна отговорност се търси при наличие на законовите предпоставки и при спазване на реда и сроковете по Кодекса на труда. Настоящите правила не създават автоматично основание за дисциплинарно наказание.

ГЛАВА VII. КОНТРОЛ, ДОКУМЕНТИРАНЕ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 23. Всички действия по предоставяне, изменение и прекратяване на достъп се документират по начин, който позволява установяване на основанието, датата, обхвата и лицето, извършило действие.

Чл. 24. Правата за достъп се преглеждат периодично, най-малко в сроковете, предвидени в приложимите нормативни и вътрешни правила, както и при всяка промяна на длъжността или прекратяване на правоотношение.

Чл. 25. Контролът по изпълнението на настоящите правила се възлага на ..... съвместно с определените от директора отговорни лица.

Чл. 26. Правилата се преразглеждат най-малко веднъж годишно и при промени в нормативната уредба, информационната инфраструктура или организацията на работа.

Чл. 27. Настоящите правила влизат в сила от датата на утвърждаването им със заповед на директора на ЦСМП – Търговище.