Ⓓ 150 ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ - ХАСКОВО
адрес: гр.Хасков[illegible]ие" №49;тел.:038/664136, e-mail: csmphaskovo@mh.government.bg

Регламент (ЕС) 2016/679

Утвърдил:

Директор на ЦСМП-Хасково

Дата: 18.03.2026 год.

ВЪТРЕШНИ ПРАВИЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В ЦСМП ХАСКОВО

Раздел I: Общи положения и цели

- **Правно основание:** Настоящите правила се издават на основание Закона за киберсигурност и НМИМИС / НАРЕДБА за минималните изисквания за мрежова и информационна сигурност/

В настоящите вътрешни правила понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми.

- **Обхват:** Правилата са задължителни за всички служители в администрацията, диспечерския център (Районна координационна централа - РКЦ) и филиалите за спешна медицинска помощ (ФСМП). Потребителите на информационни системи в ЦСМП Хасково са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Системата за сигурност на информацията в ЦСМП Хасково има за цел да защитава служителите, партньорите и пациентите на ЦСМП Хасково от незаконни или вредни действия на физически лица, пряко или косвено, съзнателно или несъзнателно при обработката на информацията и лични данни, които са на тяхно разположение, а също така и при употребата на определено оборудване за изпълнение на служебните им задължения.

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 Наредбата за минималните изисквания за мрежова и информационна сигурност (приета с ПМС № 186/26.07.2019 г.).

- **Цел:** Осигуряване на непрекъсваемост на спешната медицинска помощ чрез защита на конфиденциалността, интегритета и достъпността на медицинските и комуникационните системи.

Раздел II: Управление на сигурността и отговорности

- **Директор на ЦСМП:** Носи пряка отговорност за утвърждаването на правилата и осигуряването на бюджет за киберсигурност и изпълнява контролни функции, следи за спазването на правилата и координира реакцията при инциденти.
- **Потребители (медицински и административен персонал):** Длъжни са лично да спазват мерките за киберхигиена и да докладват за съмнителни активности.

Раздел III: Правила за киберхигиена на работното място

- **Управление на пароли:** Служителите, според естеството им на работа, имат достъп до различни системи. Служител с оторизиран достъп, използва за вход поименен квалифициран електронен подпис (КЕП) или уникален потребителски профил, така че да може да бъде идентифициран. Всички пароли за достъп до информационни системи се променят периодично.
- **Забрана за споделяне:** Абсолютно се забранява споделянето на потребителски имена и пароли между дежурните екипи/смени. Всеки служител влиза с индивидуален профил. Не е разрешено използването на групови профили. Служителите не могат да отстъпват паролите си за достъп до компютъра си на други служители, външни лица, роднини и приятели.
- **Контрол на външни носители:** Забранява се включването на лични USB флаш памети, външни дискове или телефони към компютърната мрежа на ЦСМП. Техниката да се използва изключително и само за служебни цели. Не се позволява инсталирането на какъвто и да е нов и реконфигурирането от потребителите на вече инсталиран софтуер и хардуер, както и самостоятелни опити за поправка или подобрения на горепосочените. При съмнение за възникнал проблем незабавно се уведомява директора и/или упълномощен служител, който уведомява фирмата за поддръжка, с която Центъра има сключен договор, отговарящо за мрежовата и информационна сигурност.

Не се допускат външни лица до комуникационните шкафове и техниката за интернет връзка, с изключение на техници от оторизирани фирми, и то само придружени от представител на звеното, в което се намират. Не се допуска достъпа на външни лица до компютърната техника в служебните помещения на Центъра, с изключение на поддържащата фирма.

- **Политика за "чист екран":** При напускане на работното място (дори за кратка почивка) служителят е длъжен да заключи компютъра (клавишна комбинация Win + L).
- Защитата на автоматизираните информационни системи и/или мрежи в ЦСМП Хасково включва: Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на ЦСМП Хасково. Прилагането на тази мярка е

с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае";

Раздел IV: Защита на личните и медицинските данни

- **Ограничен достъп:** Достъп до медицинските досиета и данните за повикванията имат само оторизирани лица съгласно техните преки служебни задължения (принцип на "необходимост да знае").
- **Криптиране:** Всички електронни масиви, съдържащи ЕГН, здравен статус и адреси на пациенти, трябва да бъдат криптирани в състояние на съхранение и обмен.
- **Физическа сигурност:** Сървърните помещения и комуникационните шкафове в РКЦ и филиалите трябва да бъдат заключени с контролиран физически достъп.
- При работа с телекомуникационната система, се прилагат адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола), като по този начин гарантира, че само упълномощени служители получават достъп до решаване на възложените задачи.
- Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.
- Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

- При необходимост от ремонт на компютърната техника се предоставя на фирмата отговаряща за поддръжка и ремонт на хардуера на ЦСМП Хасково или на оторизирана организация от МЗ, касаеща компютърните системи 112.
- На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице от МЗ (за медицинска част- телекомуникационна система 112, а за регистър ЧР, Финансово-счетоводна дейност и Контрагенти – ПП ТЕРЕС и КОНТО). Забранено е самоволното инсталиране на всякакъв друг вид софтуер. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица.

Раздел V: Резервно копиране (Backup) и непрекъсваемост

- **Автоматичен архив:** Системата за запис на повикванията и медицинският софтуер се архивират автоматично всеки ден.

➢ **Изолирано съхранение:** Поне едно резервно копие се съхранява в изолирана среда извън основната мрежа (извън обсега на евентуален криптовирус/ransomware).

~ Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на ЦСМП Хасково.

~ Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

~ Отговорност за архивиране има лицето, обработващо личните данни.

~ Срокът на архивиране следва да е съобразен с действащото законодателство/веднъж годишно/.

➢ **Тестване:** На всеки 6 месеца се извършва тестово възстановяване на данни, за да се гарантира годността на архивите.

Раздел VI: Реакция при инциденти и верига на доставки

➢ **Докладване в организацията:** При съмнение за вирус, фишинг атака или технически срив, служителят незабавно уведомява Директора на ЦСМП и преустановява работа с устройството. Директорът на Центъра или Техническия секретар се свързва с фирмата, с което ЦСМП Хасково има сключен договор за поддръжка на компютърните системи и периферни устройства, като обяснява за настъпилата ситуация и осигурява достъп до помещението, където е проблема.

➢ **Докладване към държавата (CERT.bg):** Значимите инциденти, застрашаващи работата на ЦСМП Хасково, като част от единната система 112, се докладват към Министерство на здравеопазването и Националния CERT съгласно процедурата в НМИМИС.

➢ **Договори с трети страни:** Всички външни ИТ фирми, поддържащи софтуер, хардуер или GPS на линейките, подписват задължителна клауза за конфиденциалност и спазване на минималните стандарти за сигурност на ЦСМП.

Раздел VII: Оперативни контролни дейности

➢ Главният счетоводител и старшата мед. сестра контролират правомерното и коректно използване на предоставената компютърна и периферна техника, като при необходимост изясняват причините за не използване на техниката и програмите или използването им не по предназначение, като докладват на директора.

➢ Служители, които не поддържат актуални данните, с които работят, въведат умишлено или неволно неверни данни и създадат условия за разпространение на невярна електронна информация, както и тези, които извършат нарушение на настоящите вътрешни правила се наказват за

нарушаване на трудовата дисциплина, в съответствие с Кодекса на труда и се задължават да възстановят данните в актуален вид.

Раздел VIII: Заключителни разпоредби

- Всички служители в ЦСМП Хасково са длъжни да познават и спазват разпоредбите на тези правила.
- Контрол по спазване на правилата се осъществява от Директора на ЦСМП Хасково
- Инструктаж: Всеки новопостъпил служител преминава задължителен първоначален инструктаж по тези правила.
- Санкции: Неспазването на правилата съставлява нарушение на трудовата дисциплина и е основание за налагане на наказания по Кодекса на труда, независимо от административнонаказателната отговорност по Закона за киберсигурност.
- Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като ЦСМП Хасково може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията, получени в указателни писма от МЕУ или МЗ.

Регламент (ЕС)

2016/679

Изготвил:
Антония Тонева
Гл.счетоводител на ЦСМП Хасково

150 ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ - ХАСКОВО

адрес: гр.Хасково 6300, бул."Съединение" №49; тел.: 038/ 664136, 0884/ 638886

e-mail: csmp-haskovo@mh.government.bg

З А П О В Е Д

№РД-01-26

гр. Хасково,19.03.2026 г.

На основание Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност

О П Р Е Д Е Л Я М :

Петя Маринова – технически сътрудник да отговаря за мрежовата и информационна сигурност в ЦСМП Хасково.

Настоящата заповед да се сведе до знанието на длъжностните лица за сведение и изпълнение.

Регламент (ЕС) 2016/679

Директор :

(Д-р Петя-Димитрова)