ДОЗН ДМР
КОМУНАЛЬНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДНІПРОВСЬКИЙ ЦЕНТР ПЕРВИННОЇ МЕДИКО-САНІТАРНОЇ ДОПОМОГИ №3» ДНІПРОВСЬКОЇ МІСЬКОЇ РАДИ
(КНП «ДЦПМСД №3» ДМР)

Код ЄДРПОУ 37899762

НАКАЗ

30.01.2023 року № 66

Про затвердження політики
інформаційної безпеки
КНП «ДЦПМСД №3» ДМР

Відповідно до Законів України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні документи та електронний документообіг», Постанови КМУ від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», з метою забезпечення виконання Плану заходів щодо реалізації Концепції розвитку електронної охорони здоров'я, затвердженого розпорядженням Кабінету Міністрів України від 29 вересня 2021 року № 1175-р, з врахуванням листа Міністерства охорони здоров'я України від 19.12.2022 № 28/29950/2-22 та з метою підвищення рівня кібербезпеки у КНП "ДЦП МСД № 3" ДМР,

НАКАЗУЮ:

1. Затвердити Політику інформаційної безпеки (далі-Політика) КНП «ДЦПМСД № 3» ДМР на 2023 рік (додається).

2. Встановити, що Політика інформаційної безпеки КНП «ДЦПМСД № 3» ДМР затверджена пунктом 1 цього наказу.

3. Керівникам структурних підрозділів ознайомити усіх працівників та забезпечити неухильне дотримання затвердженої Політики.

4. Призначити уповноважену особу, відповідальну за інформаційну безпеку у КНП «ДЦП МСД №3» ДМР інженера-програміста Тарасенка Олександра Валентиновича.

5. Контроль за виконанням даного наказу покласти на заступника генерального директора з економічно-технічних питань Тарана Олександра Сергійовича.

Генеральний директор Ольга ШИЯТА

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМУНАЛЬНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА «ДНІПРОВСЬКИЙ ЦЕНТР ПЕРВИННОЇ МЕДИКО-САНІТАРНОЇ ДОПОМОГИ № 3» ДНІПРОВСЬКОЇ МІСЬКОЇ РАДИ

1. Загальні положення

1.1. Політика інформаційної безпеки КНП «ДЦПМСД №3» ДМР (далі — Політика) розроблена відповідно до задач, мети та принципів забезпечення захисту персональних даних та інформаційної безпеки у Центрі.

1.2. Адміністрація Центру впроваджує цю Політику інформаційної безпеки, яка містить цілі інформаційної безпеки або зазначає основні положення для визначення цілей інформаційної безпеки; містить зобов'язання відповідати застосованим вимогам, пов'язаним з інформаційною безпекою та зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою.

1.3. Об'єм, зміст та строки обробки персональних даних визначаються цілями обробки персональних даних.

1.4. Метою інформаційної безпеки Центру є збереження конфіденційності, цілісності, доступності інформації, захист інформаційних ресурсів Центру від зовнішніх та внутрішніх загроз, а також зведення до мінімуму кібератак, які можуть позначатися на репутації, фінансовому становищі та функціонуванні закладу.

1.5. Дія Політики поширюється на весь Центр в цілому. Всі працівники Центру, незалежно від рівнів доступу до інформації, мають дотримуватись вимог цієї Політики.

1.6. Метою цієї Політики є впровадження, ефективне функціонування, регулювання та підтримка системи управління інформаційною безпекою, яка забезпечує захист інформації Центру від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників закладу, третіх осіб, та створення позитивної репутації Центру при взаємодії з пацієнтами.

1.7. Центр застосовує процедури захисту інформації, а саме:

- обізнаність персоналу — надання кожним окремим працівником зобов'язання щодо збереження лікарської таємниці та іншої інформації з обмеженим доступом та обізнаність (усвідомлення) персоналу з відповідальністю за незаконне використання та розголошення інформації з обмеженим доступом;

- обов'язкове використання надійних паролів, антивірусного та ліцензійного програмного

- використання застережень про нерозголошення та захист конфіденційної інформації з обмеженим доступом та дотримання вимог цієї Політики у відносинах з третіми особами, що одержують доступ до інформаційних ресурсів ЗОЗ;

- резервне копіювання, архівування та інші заходи на розсуд адміністрації Центру.

1.8. Положення даної Політики ґрунтуються на вимогах Національних стандартів України з управління інформаційною безпекою та рекомендаціях кращих міжнародних практик в галузі захисту інформації.

2. Принципи та умови обробки персональних даних у Центрі.

2.1. Під час укладання Декларації про вибір лікаря, який надає первинну медичну допомогу, з пацієнтом, уповноважена особа надавача медичних послуг повинна вносити персональні дані пацієнта до електронної системи охорони здоров'я (ЕСОЗ) та відповідно до ЗУ «Про електронні довірчі послуги» підписувати її шляхом накладання кваліфікованого електронного підпису (КЕП).

2.2. КНП «ДЦПМСД №3» ДМР залишає за собою право перевіряти повноту та точність персональних даних, що надаються. У випадку виявлення помилкових або неповних персональних даних, КНП «ДЦПМСД №3» ДМР має право припиняти взаємовідносини із суб'єктом персональних даних.

2.3. КНП «ДЦПМСД №3» ДМР не передає персональні дані суб'єктів персональних даних третім особам без їх згоди, якщо інше не передбачено чинним законодавством, згідно Закону України «Про захист персональних даних».

2.4. Всі співробітники Центру, до того, як вони приступають до виконання своїх професійних обов'язків, повинні надати письмове зобов'язання щодо нерозголошення конфіденційної інформації та поширення персональних даних, яке залишається чинним протягом всього періоду роботи в закладі та після їх звільнення.

2.5. Наказом генерального директора призначається особа, відповідальна за організацію захисту персональних даних при їх обробці по Центру.

2.6. Кожен співробітник Центру забезпечує підтримку відповідного рівня інформаційної безпеки закладу. В своїй роботі всі підрозділи та працівники дотримуються вимог Політики інформаційної безпеки та несуть відповідальність за їх порушення згідно з чинним законодавством України. Всі працівники Центру зобов'язані негайно звітувати керівництву про інциденти інформаційної безпеки, а адміністрація приймає на себе зобов'язання негайно реагувати на такі інциденти шляхом усунення наслідків та причин їх виникнення.

2.7. Для зменшення ризиків виникнення інцидентів інформаційної безпеки адміністрація Центру зобов'язує керівників структурних підрозділів вести постійну роз'яснювальну роботу та здійснювати неухильний контроль за дотриманням підлеглими вимог з інформаційної безпеки

3. Правові засади та відповідальність

3.1. Дана Політика інформаційної безпеки регламентується наступними законодавчими актами та передбачає відповідальність відповідно до чинного законодавства.
- ст. 32 Конституцією України - право на нерозголошення конфіденційної інформації;
- ст. ст. 39-1,40, ч. 2 та 5 ст.39, ч.1 ст. 43 – право на медичну таємницю;
- ст. 6.8,16,22,24 Закону України «Про захист персональних даних»;
- ст. 189 -[39] Кодексу України про адміністративні правопорушення;
- ст. 145,182 Кримінального Кодексу України.

4. Перегляд політики

4.1. Політика підтримується в актуальному стані та переглядається за необхідністю, але не рідше ніж один раз на рік.

4.2. Причинами внесення змін до Політики є зміни в інформаційній інфраструктурі або впровадження в Центрі нових інформаційних технологій, а також зміни в законодавчих, регуляторних та інших нормах.