ДНІПРОВСЬКА МІСЬКА РАДА
ІНСПЕКЦІЯ З ПИТАНЬ ПРАЦІ ТА ЗАЙНЯТОСТІ НАСЕЛЕННЯ

пр. Дмитра Яворницького, 75, м. Дніпро, 49000, тел. 720 90 58, work@dniprorada.gov.ua

03.04.2023 № 4/2-261 На № _____ від _____

Генеральному директору
Комунального некомерційного
підприємства «Дніпровський
центр первинної медико-
санітарної допомоги №9»
Дніпровської міської ради
Галині ОДИНЦОВІЙ

Від трудового колективу:
Голові первинної профспілкової
організації Комунального
некомерційного підприємства
«Дніпровський центр первинної
медико-санітарної допомоги №9»
Дніпровської міської ради
Таісії ГРИЦЕНКО

Про повідомну реєстрацію
змін і доповнень
до колективного договору

Інспекція з питань праці та зайнятості населення Дніпровської міської ради повідомляє, що відповідно до п.3 постанови Кабінету Міністрів України від 13.02.2013 №115 «Про порядок повідомної реєстрації галузевих (міжгалузевих) і територіальних угод, колективних договорів» зміни і доповнення до колективного договору розглянуто на відповідність чинному законодавству України та зареєстровано за №242 від 03.04.2023 без зауважень.

Також повідомляємо, що відомості про повідомну реєстрацію змін і доповнень до колективного договору буде оприлюднено на офіційному сайті Дніпровської міської ради за посиланням: https://dniprorada.gov.ua/uk/page/inspekciya-z-pitan-praci-ta-zajnyatosti-naselennya-dniprovskoi-miskoi-radi (інформація на сайті оновлюється щомісяця).

Начальник інспекції Тетяна ЯНУШКЕВИЧ

Сисоєва Лідія 720 90 55

Від сторони Роботодавця

Комунальне некомерційне підприємство «Дніпровський центр первинної медико-санітарної допомоги № 9» Дніпровської міської ради

Генеральний директор

_____ Галина ОДІНЦОВА

«01» лютого 2023 року

Від сторони Працівників

Первинна профспілкова організація Комунального некомерційного підприємства «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради

Голова первинної профспілкової організації

_____ Таїса ГРИЦЕНКО

«02» лютого 2023 року

ЗМІНИ І ДОПОВНЕННЯ ДО КОЛЕКТИВНОГО ДОГОВОРУ

Між генеральним директором Комунального некомерційного підприємства «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради та первинною профспілковою організацією Комунального некомерційного підприємства «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради на 2022-2026 роки

Схвалено загальними зборами (конференцією) трудового колективу
«01» 02 2023 року
протокол № 1

м. Дніпро
2023

1. У зв'язку з укладанням договору з Національною службою здоров'я України №1569-Е123-Р000 про медичне обслуговування населення за програмою медичних гарантій виникла потреба у внесенні змін до колективного договору, а саме: додаток № 1 до колективного договору «Положення про оплату працівників», розділ ІІІ Складові заробітної плати, п.3.1. Фонд основної заробітної плати - посадові оклади (таблиця 1) доповнити посадою лікар-кардіолог та викласти в наступній редакції:

6	Лікар загальної практики-сімейний лікар, лікар-акушер-гінеколог, лікар-терапевт, лікар-нарколог, лікар-анестезіолог, лікар з фізичної реабілітаційної медицини, лікар з ультразвукової діагностики, лікар-невропатолог, лікар-невролог дитячий, лікар-ортопед-травматолог, лікар-ортопед-травматолог дитячий, ерготерапевт, фізичний терапевт, лікар-статистик, **лікар-кардіолог**	Професіона-ли			
6.1	вищої кваліфікаційної категорії		22 110	11	3,30
6.2	І кваліфікаційної категорії,		21 641	10	3,23
6.3	ІІ кваліфікаційної категорії,		21 105	9	3,15
6.4	без кваліфікаційної категорії		20 636	8	3,08

2. У зв'язку з виробничою необхідністю, яка виникла внаслідок встановлення камер відеоспостереження у місцях загального користування і на прилеглій території Комунального некомерційного підприємства «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради виникла потреба у внесенні змін та доповнень до колективного договору, а саме доповненні колективного договору додатком № 13 «Положення про відеоспостереження в Комунальному некомерційному підприємстві «Дніпровський центр первинної медико-санітарної допомоги № 9» Дніпровської міської ради. Додаток викласти в наступній редакції:

Додаток № 13
до колективного договору

ПОЛОЖЕННЯ
ПРО ВІДЕОСПОСТЕРЕЖЕННЯ
в Комунальному некомерційному підприємстві «Дніпровський центр первинної медико-санітарної допомоги № 9» Дніпровської міської ради

1. Загальні положення.

1.1. Положення про відеоспостереження в КНП «ДЦПМСД № 9» ДМР та його структурних підрозділах (далі – заклад) розроблене відповідно до Конституції України, Цивільного Кодексу України, Законів України «Про інформацію», «Про захист персональних даних» та визначає порядок використання відеоапаратури та організації системи відеоспостереження в закладі і його структурних підрозділах.

1.2. Відеоспостереження в закладі організовується з метою ефективного використання наявних ресурсів для оперативного вирішення питань виробничої діяльності та запобігання протиправних дій.

1.3 Це Положення є обов'язковим для працівників і відвідувачів закладу. Кожен працівник підлягає ознайомленню з Положенням. Витяг з Положення про ведення відеоспостереження підлягає розміщенню на видних місцях, доступних для відвідувачів закладу.

2. Основні поняття та скорочення.

У цьому Положенні застосовуються наступні основні поняття та скорочення:

2.1. Об’єкти - будівлі, споруди, приміщення, території, що підлягають оснащенню відеокамерами.

2.2. Несанкціоновані дії (далі - НСД) - навмисні дії, спрямовані на порушення правильності функціонування системи.

2.3.Протикримінальний захист працівників, відвідувачів, об'єктів і майна - діяльність, здійснювана з метою забезпечення безпеки в закладі.

2.4. Система відеоспостереження (далі - СВ) - сукупність відеокамер, телевізійних камер, каналів зв’язку, пристроїв для збереження, обробки, відтворення, перетворення відеоінформації, інших технічних засобів та кінцевих терміналів.

3. Мета і завдання відеоспостереження.

3.1. Метою відеоспостереження є відстеження приміщень закладу в режимі реального часу з метою аналізу стану об'єкта, виробничих ситуацій, ідентифікації порушників та інших завдань.

3.2. Система відеоспостереження повинна забезпечувати:

- пряме відеоспостереження приміщення та території закладу;
- запис відеоінформації в архів;
- безперервність збору інформації;
- програмування режимів роботи;
- відтворення раніше записаної інформації;
- оперативний доступ до відеозапису та відео архіву шляхом задання часу, дати та ідентифікатора телекамери.

4. Загальні вимоги і структура системи відеоспостереження.

4.1. Система відеоспостереження, технічні засоби повинні бути сертифіковані відповідно до чинного законодавства та забезпечувати захист від ураження електричним струмом. Вхідні до складу системи компоненти не повинні мати шкідливого впливу на здоров'я людини. Відеокамери, датчики, розміщуються у легкодоступних місцях з урахуванням їх функціональної надійності і можливості технічного обслуговування, ремонту, оперативної заміни.

Компоненти, що входять до системи відеоспостереження і матеріали, з яких вони виготовлені, не повинні здійснювати хімічний, біологічний, радіаційний, механічний, електромагнітний і термічний вплив на навколишнє середовище, а також виділяти в навколишнє середовище шкідливі, забруднюючі або отруйні речовини.

4.2. До системи відеоспостереження входять: відеокамери, відеореєстратори, відеомонітори, тощо.

4.3.Відеокамери встановлюються у місцях загального користування (коридори, холи, сходи, входи у приміщення і т.і.). Встановлювати відеокамери в місцях прийому пацієнтів, в туалетних кімнатах забороняється.

4.4 Працівникам і пацієнтам категорично забороняється втручатися у роботу системи відеоспостереження.

5. Режим відеоспостереження.

5.1. Відеоспостереження в закладі допускає встановлення зовнішніх та внутрішніх камер. Відеоспостереження в закладі ведеться постійно, цілодобово та щоденно. Відеокамери мають інфрачервону підсвітку, яка непомітна для людського ока і в нічний час висвітлює територію перед об'єктивом камери.

5.2. Про відеоспостереження співробітники і пацієнти сповіщаються написами і знаками встановленого типу «Ведеться відеоспостереження» та/або «Ведеться відео-, аудіо- спостереження» на видних місцях.

5.3. Орієнтовний термін часу, протягом якого зберігається запис на носіях, становить 15 днів. Після завершення цього терміну система автоматично знищує інформацію шляхом запису на неї нового відеоряду.

5.4. Доступ до записів системи відеоспостереження має виключно генеральний директор закладу та/або уповноважені ним особи.

5.5.Запис із системи відеоспостереження може бути наданий правоохоронним органам, відповідним службам, державним органам та іншим особам відповідно до чинного законодавства України на підставі мотивованого письмового звернення до генерального директора.

6. Захист персональних даних при використанні систем відеоспостереження.

Правове регулювання обробки отриманих у ході відеоспостереження персональних даних встановлюється Законом України «Про захист персональних даних» від 01.06.2010 №2297-VI із змінами.

Юрисконсульт **Євгенія ГАЛЬЧЕНКО**

3. З метою забезпечення кібербезпеки КНП «ДЦПМСД №9» ДМР та враховуючи необхідність постійного підвищення рівня функціонування інформаційно-комунікаційної системи Центру виникла потреба у внесенні змін та доповнень до колективного договору, а саме доповненні колективного договору додатком № 14 «Положення про інформаційну безпеку в Комунальному некомерційному підприємстві «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради». Додаток викласти в наступній редакції:

Додаток № 14
до Колективного договору

ПОЛОЖЕННЯ ПРО
ІНФОРМАЦІЙНУ БЕЗПЕКУ
в Комунальному некомерційному підприємстві «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради

1. ВВЕДЕННЯ

1.1. Загальні положення

Це положення про інформаційну безпеку визначає основні засади забезпечення належного рівня інформаційної безпеки КНП «ДЦПМСД № 9» ДМР (далі – Підприємство), далі - Положення або *скорочено ПІБ*.

ПІБ служить центральним програмним документом з інформаційної безпеки, з яким повинні бути ознайомлені всі працівники КНП «ДЦПМСД № 9» ДМР, підрядники (постачальники послуг), і визначає дії, застереження, заборони, яких повинні дотримуватися всі користувачі інформаційних та цифрових активів Підприємства. Положення роздруковується та затверджується керівником КНП «ДЦПМСД № 9» ДМР та зберігається у відповідального за інформаційну безпеку Підприємства.

У разі відсутності відповідального за інформаційну безпеку із-за обмеженості людського ресурсу Підприємства, функцію відповідального за інформаційну безпеку виконує Генеральний директор КНП «ДЦПМСД № 9» ДМР.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів КНП «ДЦПМСД № 9» ДМР, який гарантує конфіденційність, доступність, цілісність інформації Підприємства та спостережність і контрольованість систем/підсистем, в яких ця інформація циркулює.

Належний рівень інформаційної безпеки досягається за рахунок вмілого застосування комплексу програмних/технічних засобів та організаційних заходів, спрямованих на забезпечення захищеності даних від зловмисного використання.

Вимоги та обмеження ПІБ, застосовуються до мережевої інфраструктури, баз даних, носіїв інформації, засобів шифрування, друкованих документів, мульті-медіа файлів, засобів бездротового зв'язку, телекомунікаційних систем, аудіо повідомлень та будь-яких інших засобів, що використовуються для передачі, обробки та зберігання інформації у всіх апаратних, програмних та інших інформаційних та цифрових системах Підприємства. Цього положення повинні дотримуватися всі штатні та тимчасові працівники в усіх місцях (на робочому місці, в будівлі Підприємства та його структурних підрозділах чи працюючи віддалено), а також підрядники - постачальники послуг, які працюють з Підприємством.

1.2. Глосарій

1.2.1. Загальні терміни та абревіатури, які використовуються в цьому документі.

Актив - матеріальні та нематеріальні об'єкти або інформація, що мають цінність для КНП «ДЦПМСД № 9» ДМР.

Брандмауер - спеціальне обладнання або програмне забезпечення, що працює на комп'ютері, яке дозволяє або відмовляє в проходженні трафіку через нього, на основі набору правил.

ВІБ - відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в закладі охорони здоров'я. Уразі неможливості призначити окремого відповідального за інформаційну безпеку, його функцію виконує головний лікар.

Вірус - шкідливе програмне забезпечення, здатне відтворювати сама себе і зазвичай здатне завдати великої шкоди файлам або іншим програмам на комп'ютері, який воно атакує.

ГД – Генеральний директор.

МД – Медичний директор.

ЗГД – заступник генерального директора.

Доступність інформації - властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб та процесів до інформації, а також відсутні простої в процесі її обробки, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна. У випадку втрати інформації існує можливість своєчасного її відновлення.

КНП «ДЦПМСД № 9» ДМР (Підприємство) - заклад охорони здоров'я.

Зовнішні носії інформації - компакт-диски, DVD-диски, дискети, флешки, USB, флеш- накопичувачі, касети та інші.

ІБ - Інформаційна безпека, це процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

ІС - Інформаційна система, організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

ІТ - Інформаційна технологія.

Генеральний директор - керівник закладу охорони здоров'я.

Конфіденційність інформації - властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Користувач - Будь-яка особа зі складу персоналу ЗОЗ, уповноважена на доступ до певного інформаційного ресурсу.

Користувачі з можливостями запиту (лише для читання) - особи, яким на основі прав доступу заборонено додавати, видаляти або змінювати записи в базі даних та інших доступних їм масивах інформації. Їх системний доступ обмежується лише зчитуванням інформації.

Користувачі з можливостями редагування/оновлення - особи, яким дозволено на основі прав доступу додавати, видаляти або змінювати записи в базах даних та інших масивах інформації Підприємства.

Локальна мережа - комп'ютерна мережа Підприємства.

ПІБ - Політика інформаційної безпеки, це центральний, програмний документ, який визначає основні засади забезпечення належного рівня інформаційної безпеки закладу охорони здоров'я.

Персонал - всі працівники КНП «ДЦПМСД № 9» ДМР, які використовують інформаційні ресурси закладу, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов'язків.

ПК - персональний комп'ютер.

Привілейовані користувачі - системні адміністратори та інші особи, які конкретно ідентифіковані та мають санкціонований керівництвом доступ до певних баз даних та масивів інформації.

РГІБ - робоча група з інформаційної безпеки, колективний керівний орган системи управління інформаційною безпекою Підприємства.

Спостережність системи - властивість, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки або забезпечення відповідальності за певні дії.

СУІБ - Система управління інформаційною безпекою, це комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням у ЗОЗ інформації та інформаційних технологій.

Третя сторона - фізична чи юридична особа, яка перебуває у будь-яких договірних відносинах з Підприємством та є стороною таких відносин.

Цілісність інформації - властивість, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами чи процесами.

Шифрування - процес перетворення інформації, використовуючи алгоритм, щоб зробити її нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати».

VLAN - Віртуальна локальна мережа - локальна мережа, яка використовується для сегментації мережевого трафіку з метою адміністрування та безпеки.

VPN - Віртуальна приватна мережа - забезпечує безпечну передачу даних та доступ через загальнодоступні мережі.

1.2.2. Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених чинним законодавством України.

1.3. Застосовані положення

Перелік нормативних та регулюючих законів, актів, стандартів на основі яких розроблено цей документ.

1. Закон України «Про основні засади забезпечення кібербезпеки України»;
2. Закон України «Про інформацію»;
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
4. Закон України «Про електронні документи та електронний документообіг»;
5. Постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;
6. ISO/IEC27000:2019 - Інформаційні технології - Методи і засоби забезпечення безпеки - Системи управління інформаційною безпекою - Загальні відомості і словник;
7. ISO/IEC 27001:2013 - Інформаційні технології - Методи захисту - Системи управління інформаційною безпекою - Вимоги;
8. ISO/IEC 27002:2013/COR 2:2015 - Інформаційні технології - Методи захисту - Звід рекомендованих правил для управління інформаційною безпекою;
9. ISO/IEC 27003:2017 - Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою - Керівництво;
10. ISO/IEC 27004:2016 - Інформаційні технології - Методи безпеки - Управління інформаційною безпекою - Моніторинг, вимір, аналіз і оцінка;
11. ISO/IEC 27005:2018 - Інформаційні технології - Методи безпеки - Управління ризиками інформаційної безпеки;
12. ISO/IEC 15408-1:2009 - Загальні критерії оцінки захищеності інформаційних технологій;
13. ISO/IEC TS 27008:2019 - Методи безпеки - Вказівки для оцінки засобів контролю інформаційної безпеки;
14. ISO 27032 - Інформаційні технології. Методи захисту;
15. ISO 27035 - Управління інцидентами.

1.4. Відповідальний за інформаційну безпеку

Відповідальний за інформаційну безпеку (ВІБ) Підприємства - призначена особа зі складу персоналу закладу, який/яка відповідає за дотримання належного рівня інформаційної безпеки Підприємства, контролює всю поточну діяльність, пов'язану з розробкою, впровадженням та підтримкою політики інформаційної безпеки закладу, зберігає актуальний затверджений примірник ПІБ у себе на робочому місці та при необхідності надає до нього доступ. Чинним ВІБ є:

Інженер-програміст Логунов Даниїл Михайлович (daniil.logunov@gmail.com)

1.5. Робоча група з інформаційної безпеки

Робоча група з інформаційної безпеки закладу, це колективний керівний орган з управління системою інформаційної безпеки .

Всі члени робочої групи з інформаційної безпеки (РГІБ), визначені в рамках цієї політики, призначаються Генеральним директором КНП «ДЦПМСД № 9» ДМР. Чинними членами РГІБ є:

- Одінцова Галина Миколаївна, генеральний директор;
- Ткаченко Юлія Сергіївна, медичний директор;
- Логунов Даниїл Михайлович, інженер-програміст;
- Гальченко Євгенія Леонідівна, юрисконсульт.

РГІБ вирішує нагальні питання інформаційної безпеки в міру їх виникнення, а також приймає та схвалює необхідні заходи безпеки, які повинні бути вжиті. Відповідальність РГІБ полягає в тому, щоб визначити ризики інформаційної безпеки та вчасно вжити необхідних заходів з мінімізації чи усунення.

РГІБ, за необхідністю, контролює ведення журналу подій інформаційної безпеки (Додаток 2). Ведення цього журналу здійснюється на постійній основі. До журналу вносяться дата події, дії, вжиті для вирішення події, а також рекомендації щодо подальших дій персоналу, якщо це доречно. Цей журнал розглядається РГІБ під час щоквартальних засідань.

Відповідальний за ІБ забезпечує ведення журналу подій інформаційної безпеки, а також напрацьовує на його основі та подає на розгляд РГІБ пропозиції з підвищення рівня ІБ, покращення захисту інформації та активів КНП «ДЦПМСД № 9» ДМР.

2. ОБОВ'ЯЗКИ ПЕРСОНАЛУ

2.1. Вимоги до персоналу

Першою лінією захисту в системі управління інформаційною безпекою є персонал або користувачі. Користувачі несуть відповідальність за безпеку всіх даних, які можуть надходити до них у будь-якому форматі.

Для ідентифікації персоналу запроваджуються ідентифікуючі беджі, які персонал повинен носити на собі та які легко переглядати іншім. Пацієнти та інші відвідувачі, які можуть перебувати в будівлі Підприємства, не повинні мати беджів та не можуть знаходитися у службових приміщеннях та приміщеннях з обмеженим доступом.

Обов'язком всього персоналу закладу є вжиття необхідних заходів для забезпечення фізичної безпеки активів Підприємства. Якщо будь хто з персоналу бачить невстановлену особу в службовому приміщені чи приміщені з обмеженим доступом, він/вона повинен вжити всіх можливих заходів для виведення такої особи із зазначеного приміщення та проінформувати про такий випадок ВІБ або охорону Підприємства при наявності служби охорони. Усі відвідувачі закладу повинні знаходитись тільки в тих приміщеннях, які дозволені для перебування відвідувачів.

Захист робочих станцій. Всі робочі станції (ПК), які знаходяться в закладі не повинні залишати Підприємство без відповідного дозволу керівника чи ВІБ. Всім новим користувачам надається перший інструктаж на робочому місці щодо правил використання та зберігання робочих станцій закладу. При використані робочих станцій за межами Підприємства користувач повинен вжити всіх можливих заходів із

забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення, що на ньому знаходяться.

На робочих станціях, серверному та іншому цифровому медичному обладнанні дозволено використання тільки ліцензійного програмного забезпечення та/або спеціального програмного забезпечення, яке надається авторизованим виробником разом з апаратним забезпеченням.

ПК без нагляду - робочі станції, які залишаються без нагляду повинні бути заблоковані користувачем при виході з робочої зони (робочого місця). Також на робочих станціях повинно застосовуватись налаштування автоматичного блокування екрана після тридцяти (30) хвилин бездіяльності. Персоналу заборонено відключати чи змінювати це налаштування без відповідного дозволу ВІБ.

Домашнє використання ПК. Дозволяється підключати до локальної мережі Підприємства тільки таке комп'ютерне обладнання та програмне забезпечення, яке дозволено використовувати. На ПК, що дистанційно підключається до локальної мережі Підприємства може бути встановлено лише програмне забезпечення, схвалене для використання. Персональні комп'ютери, що надаються для дистанційної роботи, повинні використовуватися виключно в службових цілях. Персонал і підрядники повинні бути ознайомлені і розуміти перелік заборонених видів діяльності, який викладений у п.2.2. нижче. Самовільне переналаштування або зміни конфігурації не допускаються на комп'ютерах, що використовуються для дистанційної роботи персоналом.

Збереження права власності - Усі програмні засоби та документація, що встановлюється на робочих станціях або надаються персоналу чи підрядниками для забезпечення діяльності ЗОЗ, є власністю закладу, якщо це не передбачено іншим договором. Виключенням можуть бути випадки використання на робочих станціях програмного забезпечення придбаного за власний кошт працівником закладу.

2.2.Заборонена діяльність

Персоналу забороняється здійснювати наступні дії. Перелік не є вичерпним. На інші заборонені види діяльності є посилання в інших місцях цього документа.

- Дії що призводять до збою інформаційної системи. Навмисні дії що призводять до збою інформаційної системи категорично заборонені. Користувачі можуть не усвідомлювати, що вони спричинили збій системи, але якщо буде виявлено, що збій стався в результаті дії користувача, повторні дії користувача, що призводять до збою інформаційної системи можуть розглядатися як навмисний вчинок.
- Спроба несанкціонованого доступу до інформаційного ресурсу або спроба обійти функцію безпеки. Це включає в себе запуск програм для злому паролів або програм для сканування локальної мережі з метою виявлення вразливостей, а також спроби обійти заборону на доступ до інформаційних ресурсів.
- Завантаження або спроба завантаження комп'ютерних вірусів, троянів, шпигунських програм або інших видів шкідливого програмного забезпечення в інформаційну систему. Винятком може бути перевірка стійкості системи уповноваженим персоналом або представниками третьої сторони, що авторизовано перевіряє СУІБ.
- Несанкціонований перегляд інформації. Умисний, несанкціонований доступ або перегляд інформації, до якої не надавалися права на доступ чи перегляд відповідно до правила «надання мінімально необхідного доступу» для виконання службових завдань. Цілеспрямована спроба перегляду або доступу до інформації, до

якої не було надано доступу за визначеною в ПІБ процедурою, суворо заборонено.

- Використання особистого або недозволеного програмного забезпечення на робочих станціях Підприємства заборонено. Все програмне забезпечення, встановлене на робочих станціях, має бути затверджене та дозволене до використання.
- Використання неліцензійного програмного забезпечення. Все програмне забезпечення, яке встановлене на робочих станціях повинно бути ліцензійним та/або дозволеним до використання.
- Використовувати дозволене програмне забезпечення не належним чином. Порушувати або намагатися порушити умови використання або ліцензійну угоду будь-якого програмного продукту, що дозволено до використання на робочих станціях, суворо заборонено.
- Використовувати інформаційні системи не належним чином. Брати участь у будь-якій діяльності з будь-якою метою, яка є незаконною або суперечить чинній політиці інформаційної безпеки, суворо заборонено.

2.3. Користування Інтернетом та електронною поштою

Електронні засоби комунікації та Інтернет є дієвими інструментами підвищення продуктивності, Ділове використання електронних комунікацій заохочується. Однак усі системи електронного зв'язку та всі повідомлення, що генеруються на обладнанні, що належить КНП «ДЦПМСД № 9» ДМР, або обробляються на пристроях, що належать закладу, вважаються власністю КНП «ДЦПМСД № 9» ДМР, а не власністю окремих користувачів. Отже, ця політика поширюється на весь персонал і підрядників (третю сторону) та охоплює всі електронні комунікації, включаючи, але не обмежуючись ними, телефони, електронну пошту, голосову пошту, обмін миттєвими повідомленнями, Інтернет, факс, персональні комп'ютери та сервери.

Надані персоналу інформаційні ресурси, такі як робочі станції або ноутбуки, комп'ютерні системи, мережі, електронна пошта, програмне забезпечення, а також доступ до Інтернет, призначені для використання в ділових цілях. Однак особисте використання допустимо до тих пір, поки це:

- не відволікає від виконання роботи або функціональних обов'язків,
- не зменшує продуктивність персоналу,
- не перешкоджає діяльності закладу,
- не порушує нічого з наступного:

1) Незаконна діяльність - використання інформаційних ресурсів КНП «ДЦПМСД № 9» ДМР для досягання незаконних цілей або для здійснення правопорушень, суворо заборонено.

2) Порушення авторських прав - це включає скачування, тиражування та використання піратського програмного забезпечення, музики, книг, відео та аудіо файлів, а також незаконне дублювання та/або розповсюдження інформації та іншої інтелектуальної власності, яка перебуває під авторським правом.

3) Комерційне використання - використання інформаційних ресурсів КНП «ДЦПМСД № 9» ДМР для отримання особистої вигоди суворо заборонено.

4) Політична діяльність - Вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів КНП «ДЦПМСД № 9» ДМР. Заклад заохочує своїх працівників голосувати та активно брати участь у виборчому процесі, але ці заходи не повинні виконуватися з використанням активів та ресурсів КНП «ДЦПМСД № 9» ДМР.

5) Переслідування та дискримінація - забороняється використання комп'ютерів,

електронної пошти, голосової пошти, обміну миттєвими повідомленнями, текстових повідомлень та Інтернету способами, які є образливими для інших або шкідливими та аморальними. Наприклад, показ або передача зображень, повідомлень і відео сексуального характеру суворо заборонені. Інші приклади неправильного використання включають, але не обмежуються ними, етнічні образи, расові коментарі, або все, що може бути розтлумачено як переслідування, дискримінація, зневажливе ставлення, вираз погроз або прояв неповаги до інших.

6) Небажана електронна пошта - усі повідомлення зроблені з використанням ІТ-ресурсів КНП «ДЦПМСД № 9» ДМР повинні бути адресними та доцільними. Розповсюдження «небажаної» пошти, наприклад, листів щастя, реклами або несанкціонованих клопотань, забороняється. Якщо користувачі отримали будь-яке з перерахованого вище повідомлень, необхідно їх видалити та нікому не пересилати.

Підприємство зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів КНП «ДЦПМСД № 9» ДМР. Це робиться з метою належного обслуговування та захисту інформаційно- телекомунікаційного обладнання, мереж та ефективного використання наявних ресурсів. Моніторинг може здійснюватися постійно або час від часу. Для цього можуть застосовуватися різні методи моніторингу: можуть відстежуватися набрані номери зі службових телефонів, тривалість дзвінків, кількість дзвінків на/з конкретного телефону, час доби і т.д.; коли електронні комунікації можуть контролюватися, включають, але не обмежуються, дослідженнями та тестуваннями спрямованими на оптимізацію ІТ-ресурсів, усунення технічних проблем та виявлення закономірностей зловживань або незаконної діяльності.

Підприємство залишає за собою право на власний розсуд переглядати файли або електронні повідомлення будь-якого працівника в обсязі, необхідному для забезпечення ефективного використання всіх службових електронних носіїв і засобів комунікації відповідно до всіх чинних законів і нормативних актів, а також цієї Політики інформаційної безпеки.

2.4. Доступ до Інтернет

Доступ в Інтернет надається тільки тим співробітникам, хто його потребує для виконання службових обов'язків. Доступ до Інтернет це ресурс, за який КНП «ДЦПМСД № 9» ДМР витрачає кошти тому його використання потребує виконання наступних вимог. Персонал, що має доступ до Інтернету, не повинен використовувати цей доступ для розваг, прослуховування музики чи радіо, прослуховування онлайн аудіо книг та перегляду фільмів та інших медійних файлів тощо. Забороняється використовувати доступ до Інтернет для особистої комерційної діяльності чи вирішення своїх побутових питань. Треба розуміти, що використання цього ресурсу не цільовим шляхом збільшую витрати закладу, а також створює додаткові загрози інформаційної безпеки.

Якщо виявиться, що співробітник витрачає надмірну кількість часу, витрачає великі обсяги трафіку для особистого чи нецільового користування, або відвідує ресурси, які небезпечні з точки зору забезпечення інформаційної безпеки, до нього/неї будуть вжиті дисциплінарні заходи.

Ресурси які заборонено відвідувати, такі як ігрові інтернет-сайти, торенти, файлообмінники, порносайти, чати та онлайн програми для обміну музикою, тощо, автоматично блокуються. Перелік заборонених ресурсів постійно контролюється і

оновлюється в міру необхідності. Будь-який співробітник, який цілеспрямовано, неодноразово буде намагатися відвідати заборонені ресурси в Інтернет, буде притягнутий до дисциплінарної відповідальності і може бути звільнений.

В закладі здійснюються спеціальні запобіжні заходи для блокування зовнішнього доступу через Інтернет до інформаційних ресурсів закладу, не призначених для публічного доступу, а також для захисту конфіденційної інформації Підприємства при її передачі через Інтернет.

Відповідальний за інформаційну безпеку контролює виконання заходів із безпечного використання Інтернету, а саме:

- контролює щоб доступ до Інтернет з робочих місць здійснювався через встановлені точки доступу до Інтернет;
- контролює, щоб тільки публічна та відкрита інформація про КНП «ДЦПМСД № 9» ДМР була доступна в Інтернете;
- контролює, щоб користувачі не мали прав встановлювати або завантажувати будь-яке програмне забезпечення (додатки, медіа файли, заставки тощо) з Інтернет. Якщо у користувачів є потреба в додатковому програмному забезпеченні, користувач повинен отримати дозвіл;
- використання Інтернету повинно узгоджуватися з комерційною діяльністю закладу. Використання мережі на робочому місці для отримання особистого прибутку заборонено;
- конфіденційні або персональні дані, включаючи номери кредитних карток, номери телефонів, паролі для входу в систему та інші дані, які можуть бути використані для доступу до конфіденційної або персональної інформації повинні передаватися через Інтернет у зашифрованому виді.
- використання програмного забезпечення для шифрування та ключів шифрування повинно контролюватися відповідальним за ІБ. Самостійне використання шифрувального програмного забезпечення та ключів шифрування, без погодження з відповідальним за ІБ, заборонено, і може призвести до дисциплінарного покарання.

2.5. Повідомлення про несправності

Користувач повинні інформувати відповідального ІТ працівника про випадки, коли програмне забезпечення робочої станції не функціонує належним чином. Несправне програмне забезпечення становить ризик для інформаційної безпеки. Якщо користувач, або керівник користувача, підозрює зараження робочої станції вірусом, слід негайно вжити наступних заходів:

- припинити використання комп'ютера;
- не запускати на виконання ніяких команд, включаючи команду збереження даних;
- не закривати жодного з вікон або програм комп'ютера;
- не вимикати комп'ютер або периферійний пристрій на самому екрані;
- по можливості фізично відключити комп'ютер від мереж живлення та локальної мережі;
- повідомити про ураження робочої станції відповідального ІТ та відповідального за ІБ, вказавши ознаки незвичайної поведінки комп'ютера (блокування екрану, виникнення несподіваного доступ до системного диска, незвичайна реакція на команди тощо) і час, коли це було вперше помічено;
- повідомити про будь-які зміни у використанні апаратного чи програмного забезпечення, які передували несправності;
- не намагатися самостійно видалити підозрілий файл!

Відповідальний з ІБ повинен вжити заходи для усуненням несправності, а також повідомити керівнику закладу про результати цих дій з рекомендаціями щодо подальших кроків для запобігання подібних випадків у майбутньому.

2.6. Повідомлення про інциденти безпеки

Весь персонал, який є користувачами інформаційних ресурсів закладу або підрядники, які мають доступ до цифрових активів КНП «ДЦПМСД № 9» ДМР зобов'язані повідомляти відповідального з ІБ про виявлені інциденти інформаційної безпеки. Користувач - це будь-яка особа, уповноважена на доступ до інформаційного ресурсу закладу. Користувачі несуть відповідальність за повсякденну практичну безпеку ресурсу, яким вони користуються. Користувачі повинні повідомляти про всі інциденти безпеки або порушення політики безпеки негайно своєму безпосередньому керівнику або відповідальному з інформаційної безпеки. При неможливості негайного повідомлення про інцидент безпеки вищевказаним особам, користувач повинен без зволікань проінформувати про інцидент будь-якого члена Робочої групи з інформаційної безпеки закладу, які вказані вище в цьому документі.

Реагування на повідомлення про інциденти інформаційної безпеки повинно бути якомога швидким. Кожен член Робочої групи з інформаційної безпеки повинен негайно вжити заходи відповідно до Плану реагування на інцидент інформаційної безпеки. Кожен інцидент повинен бути проаналізованим, щоб визначити, чи потрібно внесення необхідних змін в існуючу систему управління інформаційною безпекою КНП «ДЦПМСД № 9» ДМР. Усі виявлені інциденти реєструються в журналі інцидентів інформаційної безпеки. Обов'язком відповідального за ІБ є організація та проведення навчання, щодо будь-яких змін у плані реагування на інциденти, які були зроблені в результаті розслідування інциденту.

Внутрішні порушення інформаційної безпеки повинні оперативно розслідуватися. У разі підозри на порушення законодавства, відповідальний з ІБ повинен звернутися до правоохоронних органів.

2.7. Передача конфіденційної інформації

Передача конфіденційної інформації може здійснюватися за допомогою засобів електронного зв'язку, на цифрових носіях чи у паперовому виді. Конфіденційна інформація передається від однієї особи іншій під час ведення службових справ. Особа, яка отримала конфіденційну інформацію повинна забезпечити її зберігання відповідно до умов, встановлених особою, що надала таку інформацію та Положенням «Про конфіденційну інформацію та медичну таємницю» (додаток №12 до колективного договору). Будь-яке цілеспрямоване оприлюднення конфіденційних даних, до яких працівник має доступ, є порушенням, за яке передбачена відповідальність.

2.8. Передача даних та програмного забезпечення

Власне програмне забезпечення, яке не дозволене до використання в закладі не може використовуватися на робочих станціях чи комп'ютерах або в локальній мережі КНП «ДЦПМСД № 9» ДМР. Якщо існує потреба в конкретному програмному забезпеченні, потрібно надати запит на дозвіл своєму безпосередньому керівнику. Користувачі не повинні використовувати програмне забезпечення, що встановлене на робочих станціях, або на особистих комп'ютерах чи комп'ютерному обладнанні при дистанційній роботі без відповідного дозволу.

Дані, що є власністю закладу включаючи інформацію про пацієнтів, інформацію про ІТ-системи, фінансову інформацію або дані про людські ресурси, не

повинні розміщуватися на будь-якому комп'ютері, який не є власністю Підприємства, без письмової згоди відповідного керівника. Підприємство повинне захищати всі дані та програмне забезпечення, які йому належать, тому повинен контролювати системи, в яких такі дані містяться. У випадку, якщо відповідний керівник отримає від персоналу запит на переміщення даних з робочої станції на особистий ПК, керівник повинен визначитися чи є в цьому службова потреба та уразі прийняття рішення на дозвіл переміщення, повідомити відповідального з інформаційної безпеки про таку передачу даних.

2.9. Шифрування електронної пошти та даних

Для забезпечення конфіденціальної та захисту конфіденційної інформації при передачі в мережі Інтернет дозволяється використання відповідного програмного забезпечення (наприклад програми WinZip), яке дозволяє персоналу обмінюватися електронною поштою з віддаленими користувачами, які теж мають відповідне програмне забезпечення для шифрування/дешифрування.

3. УПРАВЛІННЯ ДОСТУПОМ

3.1. Ідентифікація користувачів

Кожний користувач повинен мати унікальний ідентифікатор (обліковий запис, логін) та пароль для входу. Система контролю доступу повинна ідентифікувати кожного користувача і запобігати доступу та використанню інформаційних ресурсів закладу неавторизованим користувачем. Вимоги безпеки для ідентифікації користувача включають:

- кожному користувачеві присвоюється унікальний ідентифікатор;
- користувачі несуть відповідальність за використання та неправомірне використання свого індивідуального ідентифікатору.

Усі ідентифікатори входу користувачів перевіряються щонайменше раз на рік і всі неактивні ідентифікатори блокуються. Відділ кадрів Підприємства сповіщає відповідального за ІБ або відповідного фахівця ІТ-відділу про звільнення працівника або припинення співробітництва з персоналом підрядника. При отримані такого сповіщення неактивні ідентифікатори блокуються.

Ідентифікатор входу блокується після максимум трьох (3) невдалих спроб входу в систему. Для відновлення доступу в цьому випадку потрібне призначення нового тимчасового паролю Адміністратором.

Користувачі, які бажають отримати доступ до систем або мереж Підприємства, повинні сповістити відповідального за ІБ.

3.2. Встановлення паролів

Ідентифікатори користувачів і паролі потрібні для того, щоб отримати доступ до мереж і робочих станцій. До всіх паролів застосовується встановлена цім документом Парольна політика, для забезпечення стійкості паролів. Це означає, що всі паролі повинні відповідати вимогам, які призначені для того, щоб пароль було важко підібрати чи зламати. Користувачі зобов'язані створювати та користуватися паролями, щоб отримати доступ до відповідних мереж, ІТ-ресурсів чи робочої станції. При призначені паролю користувачеві буде автоматично запропоновано вручну призначити пароль, відповідно до таких вимог:

Довжина пароля - Пароль повинен складатися з мінімуму восьми (8) символів.

своєчасну здачу працівником, що звільняється відповідних пристрої доступу, які йому/їй надавалися. Обліковий запис та доступ працівника блокується по завершені останнього робочого дня.

4. ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ

4.1. З'єднання та підключення

Доступ до інформаційних ресурсів закладу через модеми, інші комунікаційні пристрої або відповідне програмне забезпечення підлягає авторизації та автентифікації системою контролю доступу. Зовнішній виклик чи комутація на внутрішній номер (кінцевий пристрій) без проходження через систему контролю доступу заборонений.

Системи, що дозволяють проходження зовнішнього виклику на кінцевий пристрій, в тому числі сервер повинні гарантувати додаткову безпеку на рівні операційної системи та додатків. Такі системи повинні також мати можливість контролювати рівень активності, щоб гарантувати, що використання кінцевих пристроїв відбувається належним чином та з виконанням заходів безпеки.

Права доступу до з'єднання через комутатори надаються відповідальним за ІБ тільки на вимогу керівника відділу.

Підключення до зовнішніх мереж відбувається через інтернет-провайдера. Якщо користувач має конкретну потребу зв'язатися із зовнішнім комп'ютером або мережею через прямий канал зв'язку він повинен отримати дозвіл від керівника закладу або відповідального з ІБ. При прийняті позитивного рішення відповідальний з інформаційної безпеки повинен вжити необхідних заходів із забезпечення належного рівня безпеки нового каналу зв'язку.

4.2. Телекомунікаційне обладнання

До телекомунікаційного обладнання та засобів відноситься наступне:

- телефонні лінії та обладнання
- факсимільні лінії та обладнання
- телефоні навушники та гарнітура
- телефони типу програмного забезпечення, встановлені на робочих станціях
- службові мобільні телефони
- програмне забезпечення для маршрутизації викликів
- обладнання для адміністрування телефонної системи
- мережеві лінії
- міжміські лінії
- місцеві телефонні лінії.

Цей перелік не є вичерпним.

4.3. Постійні з'єднання

Забезпечення безпеки телекомунікаційних з'єднань є дуже важливим завданням. Інформаційна безпека закладу може бути поставлена під загрозу, якщо не забезпечити безпечне користування засобами зв'язку. Необхідно забезпечити аналіз ризиків при підключені до зовнішніх мереж та регулярно аналізувати ризики постійно діючих каналів з'єднання. Аналіз ризиків повинен враховувати тип необхідного доступу, цінність інформації що передається, заходи безпеки, що застосовуються третьою стороною, а також наслідки для системи управління безпекою закладу. Відповідальний за інформаційну безпеку повинен бути залучені до процесів проектування та затвердження каналів підключення до зовнішніх мереж, а також

укладення договорів з третьою стороною на отримання послуг з телекомунікаційного забезпечення закладу.

4.4. Договір на телекомунікаційні послуги

При укладанні договору на отримання телекомунікаційних послуг закладом необхідно враховувати відповідні розділи політики інформаційної безпеки надавача послуг.

4.5. Брандмауер

Налаштування брандмауера повинно контролюватися відповідальним з ІБ. Якщо брандмауер знаходиться та налаштовується стороною, яка надає ІТ-послуги закладу то ця сторона повинна надати повну інформацію про актуальні налаштування брандмауера відповідальному за інформаційну безпеку та активно співпрацювати з ним/нею у питаннях подальшого його використання та змін налаштувань.

5. АНТИВІРУСНИЙ ЗАХИСТ

5.1. Встановлення та оновлення антивірусного ПЗ

Антивірусне програмне забезпечення встановлюється на всіх робочих станціях, кінцевому обладнанні і серверах закладу та періодично оновлюється.

5.2. Перевірка нового ПЗ

На внутрішніх комп'ютерах і мережах закладу використовується лише дозволене до використання програмне забезпечення. Встановлення нового програмного забезпечення здійснюється відповідальним за ІБ.

Усе файли і програми, які були передані в електронному вигляді на комп'ютери або мережу закладу з іншого місця, повинні бути перевірені на віруси відразу після отримання.

5.3. Збереження прав власності

Усі програмні продукти та документація, що надаються працівникам або підрядникам є власністю закладу, якщо на них не поширюється дія іншого договору. Програмні засоби, застосунки або документація які розробляються за замовленням закладу є також його власністю. Розробники таких програмних продуктів та документації повинні підписати заяву, в якій визнається право власності закладу на відповідний програмний продукт та документацію. Програмне забезпечення, придбане працівником за власний рахунок, залишається власністю працівника, який придбав це програмне забезпечення.

6. КРИПТОГРАФІЧНИЙ ЗАХИСТ

6.1. Визначення

Криптографічний захист інформації за допомогою шифрування даних є найефективнішим способом забезпечення безпеки даних КНП «ДЦПМСД № 9» ДМР. В закладі використовуються наступні засоби криптографічного захисту: інфраструктура відкритих ключів з електронним цифровим підписом; програма - архіватор типу WinZip; передача файлів за допомогою протоколу FTP; захищений веб-інтерфейс SSL.

Криптографічний захист інформації, що передається обробляється та зберігається в медичних інформаційних системах забезпечується провайдером такої системи.

6.2. Ключі шифрування

Ключ шифрування визначає особливе перетворення простого тексту у зашифрований, або навпаки під час дешифрування (розшифрування). У разі виникнення інциденту, пов'язаного з криптографічним захистом інформації, його

вирішенням повинен займатися відповідальний з інформаційної безпеки закладу. Заклад може використовувати декілька методів безпечної передачі даних за допомогою криптографічного захисту.

6.3. Використання інфраструктури відкритих ключів

Користувач, який має потребу у безпечній передачі інформації електронною поштою конкретному ідентифікованому зовнішньому користувачеві, може скористатися інфраструктурою відкритих ключів та електронним цифровим підписом (ЕЦП/КЕП). Порядок використання ЕЦП/КЕП у закладі повинно бути погоджено з керівником чи відповідальним за інформаційну безпеку.

6.4. Використання WinZip

Це програмне забезпечення дозволяє персоналу закладу обмінюватися електронною поштою з віддаленими користувачами, які мають відповідне програмне забезпечення для шифрування та дешифрування.

6.5. Протокол передачі файлів FTP

Користувач може передати файли зі своєї робочої станції на захищені sFTP-сайти за допомогою відповідних заходів безпеки. FTP (англ. File Transfer Protocol) або sFTP (Secure File Transfer Protocol) це стандартний мережевий протокол прикладного рівня призначений для пересилання файлів між клієнтом та сервером в комп'ютерній мережі. Клієнт та сервер створюють окремі канали для передачі даних та обміну командами. Можлива автентифікація клієнтів із використанням логіну та паролю користувача. Порядок FTP-передачі файлів повинен бути погоджений з керівником та відповідальним за інформаційну безпеку..

6.6. Веб-інтерфейс рівня захищених сокетів (SSL)

Для передачі конфіденційної інформації через веб-інтерфейсі використовується веб-інтерфейс захисту SSL. SSL (англ. Secure Sockets Layer) — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і веб-сервером. Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP/IP. Користувач через веб-інтерфейс захисту SSL передає/отримує конфіденційну інформації через веб-сторінку в Інтернеті при наданні/отриманні послуг онлайн. Порядок використання веб- інтерфейсу захисту SSL погоджується з керівником закладу та відповідальним з інформаційної безпеки.

7. ФІЗИЧНА БЕЗПЕКА

Забезпечення фізичної безпеки персоналу полягає у створені безпечних умов на робочому місці та одночасним забезпеченням безпечного зберігання активів закладу. Будівля (комплекс будівель) закладу є дещо унікальним місцем з точки зору прав власності на будівлю або умов договору оренди, території навколо, шляхів під'їзду/виїзду, зовнішнього огородження, входів у приміщення, вимог до пожежної безпеки, систем електроживлення, забезпечення безпечного використання цифрових активів та контролю серверної кімнати. Підприємство постійно покращує та модернізує систему забезпечення фізичної безпеки для підвищення захисту своїх активів та медичної інформації.

- Вхід до будівлі в неробочий час зачинений та контролюється охоронною сигналізацією. Спроба входу без введення коду безпеки для зняття з охоронної сигналізації призводить до негайного повідомлення до охоронної служби.
- Тільки конкретним працівникам закладу видається код безпеки для входу. Розголошення коду безпеки не працівникам категорично заборонено.
- Код безпеки змінюється на періодичній основі, змінений код відповідні працівники отримують через сповіщення на робочу електрону пошту. Код безпеки

обов'язково змінюються при звільненні працівника, який мав доступ до нього.

- Вхідні двері в зону прийому пацієнтів та відвідувачів завжди замикаються у неробочий час і відмикаються у робочі години закладу.
- Будь-яка невизнана особа, яка перебуває в службових приміщеннях закладу повинна негайно виводитись зі службової зони персоналом, що її побачив, та супроводжуватись до зони рецепції.
- До приміщення де знаходиться серверне обладнання мають доступ тільки визначене коло посадових осіб.

8. БЕЗПЕКА ДАНИХ

8.1. Захист апаратного забезпечення

Захист від вірусів: Антивірусне програмне забезпечення встановлене на комп'ютерах закладу і налаштоване на періодичне оновлення.

Шафа або сейф: Працівники мають зберігати пристрої в шафі, що замикається або сейфі.

Блокування екранів: Працівник, перш ніж відійти від робочої станції, має заблокувати екран. Дані на екрані можуть містити конфіденційну інформацію.

8.2. Безпека даних

Резервне копіювання даних: Для резервного копіювання використовується тільки встановлена відповідальним за ІБ процедура. Створювати самостійно інші процедури резервного копіювання даних заборонено.

Електронна пошта: Не дозволено передавати будь-яку конфіденційну інформацію та персональні дані електронною поштою, якщо вона не зашифрована.

Друковані звіти або робочі документи: Працівникам заборонено виносити та використовувати в особистих цілях інформацію з обмеженим доступом та таку що містить лікарську таємницю на будь-яких носіях та в паперовому вигляді. Працівникам заборонено залишати без нагляду електронні ключі.

Надсилання даних за межі закладу: Працівникам Підприємства заборонена передача даних за межі Підприємства без згоди безпосереднього керівника.

8.3. Утилізація паперових та зовнішніх носіїв

Паперові документи: Всі паперові документи, які містять конфіденційну інформацію, перед утилізацією потрібно подрібнити. Заборонено викидання не подрібнених паперових документів.

Зовнішні носії: Всі зовнішні носії надані закладом для забезпечення роботи повинні бути повернуті до закладу для утилізації.

9. ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ

Метою впровадження політики чистого столу та чистого екрану на Підприємстві є:

- запобігання витоку/втраті конфіденційних даних закладу;
- дотримання правил кібергігієни та розвитку кіберкультури, щодо безпечного та належного поводження з конфіденційною інформацією та її носіями;
- створення та підтримання позитивного іміджу закладу серед пацієнтів.

Відповідальність

Вимоги цієї політики поширюються на весь персонал закладу. Усі працівники закладу мають бути ознайомлені із її вимогами. До будь-якого працівника закладу, визнаного винним у порушенні цієї політики, може бути застосована дисциплінарна практика.

Вимоги

Увесь персонал закладу повинен дотримуватись наступних правил:

• зберігати власні паролі в таємниці, не розголошувати та нікому не повідомляти їх;

• закривати активні сеанси після завершення роботи, якщо їх не можна захистити відповідним блокуючим механізмом, наприклад блокуванням екрану;

• робочі станції, комп'ютери та засоби зв'язку повинні бути залишені у стані виконаного виходу із системи/вимкнені коли вони перебувають без нагляду;

• цифрове медичне обладнання, що не використовується повинно бути вимкнене або переведене у безпечний режим;

• документи, які містять конфіденційну інформацію, повинні забиратися виконавцем з принтерів негайно;

• наприкінці робочого дня/зміни увесь персонал повинен упорядкувати своє робоче місце;

• чорнові варіанти конфіденційних документів підлягають утилізації шляхом подрібнення.

• після закінчення робочого дня та у разі тривалої відсутності на робочому місці необхідно замикати на замок усі шафи та сейфи де зберігається конфіденційна інформація та робочі документи.

Збереження/знищення медичної інформації

Медична інформація, є конфіденційною інформацією закладу та потребує дотримання процедур безпечного збереження та утилізації.

Збереження записів - документи, що стосуються використання та розкриття інформації, форми авторизації, договори та угоди, повідомлення про інформаційну практику, відповіді пацієнту, який хоче змінити або виправити свою інформацію, заява пацієнта про незгоду та запис скарг зберігаються протягом періоду у 5 років.

Знищення - Вся паперова медична документація, потребує знищення після закінчення терміну зберігання. Знищення медичної документації відбувається встановленим порядком шляхом спалювання.

10. УТИЛІЗАЦІЯ ЗОВНІШНІХ НОСІЇВ ТА КОМП'ЮТЕРІВ

10.1. Утилізація зовнішніх носіїв

Всі зовнішні носії, які використовувались персоналом містять конфіденційну та/або медичну інформацію. Відповідно застаріли або зіпсовані зовнішні носії, подальша експлуатація яких вже неможлива, повинні бути утилізовані методом, який гарантує, що не буде втрати даних і що конфіденційність і безпека цих даних не будуть порушені.

Відповідальний з ІБ забезпечує знищення зовнішніх носіїв, що підлягають утилізації.

10.2. Утилізація комп'ютерного обладнання

Комп'ютерне обладнання, в тому числі медичне, яке підлягає утилізації, проходить відповідну процедуру, яка складається з видалення усіх даних, затирання усіх міток та конфігурацій та повернення до заводських налаштувань. Відповідальний з інформаційної безпеки забезпечує утилізацію комп'ютерного обладнання відповідно до встановленої процедури.

10.3. Використання надлишкового обладнання

Старе комп'ютерне обладнання може бути використане:

- для запасних частин,
- для аварійної заміни,
- для тестування нового програмного забезпечення,
- для створення та зберігання резервних копій для іншого виробничого обладнання,
- для використання персоналом за межами закладу, в тому числі для забезпечення

дистанційної роботи.

11. УПРАВЛІННЯ ЗМІНАМИ

Для того, щоб відстежувати та управляти змінами в мережах, IT-системах та на робочих станціях, включаючи встановлення та налаштування нового програмного забезпечення та виправлення вразливостей програмного забезпечення в інформаційних системах, які містять конфіденційну та медичну інформацію, запроваджена процедура управління змінами, яка полягає в наступному:

Процедура

1. Відповідальний працівник, який впроваджує зміну, забезпечує створення всіх необхідних резервних копій програмного забезпечення та даних.
2. Працівник, який впроваджує зміну, також повинен бути ознайомлений з процесом повернення до попередніх налаштувань у тому випадку, якщо зміна викликає збоїв в мережі чи системах і потребує видалення.

Оновлення дозволеного програмного забезпечення проводиться відповідно до рекомендацій розробників цього ПЗ. Персонал повинен здійснювати оновлення програмного забезпечення невідкладно, по мірі отримання/можливості доступу до оновленої версії ПЗ.

12. МОНІТОРІНГ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Моніторинг стану інформаційної безпеки - це відповідні технологічні та процесуальні дії, які спрямовані на відстеження і фіксацію комп'ютерної та мережевої діяльності з метою визначення, чи сталося порушення інформаційної безпеки. Моніторинг передбачає відстеження та фіксацію зареєстрованих комп'ютерних подій, які стосуються стану операційних систем, програмного забезпечення або діяльності користувачів.

На Підприємстві проводиться моніторинг діяльності користувачів з метою запобігання технологічних збоїв та виявлення потенційних ризиків та вразливостей системи інформаційної безпеки. Відповідно до виявлених збоїв, ризиків та вразливостей в закладі розробляються та запроваджуються відповідні адміністративні, фізичні та технічні заходи забезпечення інформаційної безпеки відповідно до вимог чинного законодавства у сфері кіберзахисту.

13. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

На Підприємстві раз на рік, проводиться аудит стану інформаційної безпеки, який включає, але не обмежується такими заходами як, перевірка облікових записів користувачів та прав доступ до IT- систем та мереж, доступ до файлів, перегляд та аналіз інцидентів безпеки, перегляд журналів моніторингу тощо. Аудит може проводитись як відповідним персоналом закладу так і зовнішніми аудиторами. Мета проведення аудиту - мінімізація порушень безпеки та забезпечення інформаційної безпеки закладу на належному рівні. У разі неможливості проведення аудиту стану інформаційної безпеки власними силами та засобами, Підприємство може звернуся до авторизованих зовнішніх аудиторів.

Аудит стану ІБ проводиться щорічно але може проводитися позапланова, якщо є підстави підозрювати порушення, які можуть призвести до тяжких наслідків.

Висновки Аудиту повинні бути відображені у звіті інформаційної безпеки Підприємства. Особи що проводили аудит передають звіт та перелік рекомендованих заходів відповідальному з інформаційної безпеки для ознайомлення та вживання відповідних заходів. Відповідальний з ІБ при отримані звіту повинен невідкладно

вжити всіх належних заходів з приведення стану ІБ до відповідного рівня та усунення виявлених недоліків.

14. ЦІЛІСНІСТЬ ДАНИХ ПАЦІЄНТІВ

Підприємство впроваджує та підтримує відповідні організаційні та технологічні заходи для підтвердження того, що медичні дані пацієнтів інша конфіденційна інформація стосовно пацієнтів не були змінені або знищені несанкціонованим чином. Метою таких дій є забезпечення цілісності даних пацієнтів.

Підприємство підтримує впровадження автоматизованих систем та програмного забезпечення, в тому числі з використанням штучного інтелекту, для автоматичної перевірки наявності людських помилок при обробці даних пацієнтів.

Підприємство застосовує відповідні мережеві та хост-систем виявлення вторгнень. Відповідальний за ІБ організовує встановлення, контролює обслуговування та оновлення таких систем.

Збереження цілісності даних пацієнтів, що знаходяться в медичних інформаційних системах забезпечується провайдерами таких систем.

Для запобігання збою ІТ-систем, які можуть призвести до порушення цілісності даних, Підприємство забезпечує перевірку своїх інформаційні системи на точність і функціональність, перш ніж почне їх використовувати.

Підприємство встановлює та регулярно оновлює антивірусне програмне забезпечення на всіх робочих станціях та серверах, щоб своєчасно виявити та запобігти зміні або знищенню даних шкідливим програмним забезпеченням.

15. ПЛАНИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА АВАРІЙНОГО ВІДНОВЛЕННЯ

На Підприємстві впроваджені заходи та процедури реагування на надзвичайні події, які можуть завдати шкоди ІТ-системам та мережам, а також інформації. Для цього розроблений План аварійного відновлення та План резервного копіювання. Підприємство періодично переглядає цій план з метою аналізу його ефективності та оцінки ризиків для внесення відповідних корегувань.

15.1. План резервного копіювання

Відповідальний з ІБ забезпечує розробку та впровадження плану резервного копіювання даних для створення та підтримки точних копій операційних систем, програмного забезпечення, баз даних, іншої інформації та даних закладу.

15.2. План аварійного відновлення

Відповідальний за ІБ розробляє План аварійного відновлення з метою своєчасного відновлення та/або запобігання будь-яких втрат даних, систем, необхідних для надання медичної допомоги пацієнтам та забезпечення неперервності критично важливих процесів функціонування закладу.

*План аварійного відновлення повинен містити п*орядок створення та оновлення копій документів щодо результатів інвентаризації інформаційних активів, конфігурації мереж, порядок відновлення втрачених даних, порядок використання аварійних систем протягом часу коли основні інформаційні системи недоступні та необхідні заходи для відновлення функціонування закладу.

16. ОБІЗНАНІСТЬ ТА НАВЧАННЯ З ПИТАНЬ БЕЗПЕКИ

Для підвищення обізнаності стосовно питань інформаційної безпеки весь персонал закладу, включаючи керівництво, повинен регулярно проходити відповідні навчання. Навчання з ІБ для всього персоналу проводиться раз на рік, або позапланово при необхідності.

Відповідальний за інформаційну безпеку організовує та проводить навчання з інформаційної безпеки. Він/вона здійснює первинний інструктаж для нових працівників, щорічний інструктажі для всього персоналу, а також планові заняття стосовно Політики інформаційної безпеки та актуальних загроз.

Відповідальний з ІБ, при необхідності, може організовувати позапланові навчання при змінах у апаратному або програмному забезпечені, збільшені загроз, внесені змін у політику інформаційної безпеки, за результатами аудиту, тощо.

17. УПРАВЛІННЯ РИЗИКАМИ

17.1. Для забезпечення інформаційної безпеки Підприємство проводить точну та ретельну оцінку потенційних ризиків та вразливостей стосовно конфіденційності, цілісності та доступності даних, що зберігаються, обробляються та передаються інформаційними системами та мережами закладу.

Підприємство проводить повторну оцінку ризиків безпеки та оцінку ефективності заходів безпеки, якщо це необхідно при змінах у штатній структурі, створені нових процесів чи розвитку технологій.

При оцінці загроз конфіденційності, цілісності та доступності даних, які створених, отримані, зберігаються, передаються чи обробляються закладом звертається увага на таке:

- загрози пошкодження даних навколишнім середовищем, наприклад, землетрусом, повінню, штормом, тощо.
- загрози надзвичайних ситуацій - пошкодження пожежею, аварією електромережі, припиненням отримання комунальних послуг, тощо.
- людські загрози, а саме:

* ненавмисні дії, наприклад, помилки при введені даних, використання несправного програмного забезпечення, нездатність оновити програмне забезпечення, відсутність належних фінансових та людських ресурсів для підтримки необхідних засобів контролю безпеки

* неналежна діяльність, наприклад, неналежна поведінка, зловживання привілеями чи правами, марнотратство, переслідування особистої користі

* зловмисні дії, наприклад шахрайство, крадіжки, вандалізм, диверсії,

* зовнішні атаки, наприклад, хакерські атаки, сканування, геополітичні ризики.

Відповідальний за ІБ здійснює оцінку ефективності заходу стосовно усунення чи мінімізації ризику та при необхідності забезпечує здійснення повторної оцінки.

18. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ

При порушенні чинного законодавства та політики інформаційної безпеки настає відповідальність за порушення.

До конфіденційної інформації закладу відноситься:

- захищена медична інформація - індивідуальна інформація про стан здоров'я пацієнтів, яка знаходиться в будь-якій формі будь то електронна, паперова або усна;
- електронна захищена медична інформація - індивідуальна інформація про стан здоров'я пацієнтів, яка знаходиться в електронному форматі;
- інформація про медичний персонал - будь-яка інформація, пов'язана з наймам та/або працевлаштуванням будь-якої фізичної особи, яка є або була працевлаштована в закладі.
- дані про заробітну плату персоналу;
- фінансові/бухгалтерські записи - будь-які записи, пов'язані з бухгалтерською або фінансовою звітністю закладу;
- інша конфіденційна інформація - будь-яка інша інформація, яка має

конфіденційний характер або вважається конфіденційною відповідно до чинних угод та договорів.

19. ПЕРЕВІРКА КАНДИДАТІВ

Підприємство проводить довідкові перевірки кандидатів перед працевлаштуванням. Від кандидата завчасно отримується згода на проведення такої перевірки (Додаток 3) . Кандидат, який відмовляється від такої перевірки, перестає бути кандидатом та його вивчення кадровим відділом припиняється.

Відділ кадрів збирає інформацію про репутацію кандидата, особисті характеристики або спосіб життя. Ця інформація може бути зібрана в Інтернеті, включаючи сайти соціальних мереж, через публічні чи освітні записи або через співбесіди з попередніми роботодавцями, партнерами, особами, що можуть надати рекомендаційні листи або будь кім іншим.

Тип інформації, яка буде зібрана закладом під час перевірки біографічних даних, може включати, але не обмежуватися наступною інформацією:

- довідка про непритягувана до кримінальної відповідальності;
- диплом про освіту (включаючи середній бал);
- історію працевлаштування, здібності та причини припинення трудових відносин;
- сертифікати, дипломи про закінчення закладів навчання, курсів, тощо;
- кредитна історія;
- реєстр рішень цивільних судів;
- записи у відкритих реєстрах стосовно володіння рухомим та нерухомим майном;
- професійні або особисті довідки;
- резюме кандидата.

Ця інформація також може бути додатково переглянута під час здійснення працівником порушення або його/її перепризначення на посаду з розширенням прав доступу. Повідомлення про судимість не обов'язково дискваліфікує кандидата на працевлаштування. При прийняті рішення враховується характер і серйозність правопорушення, дата правопорушення, обставини та можливі ризики для закладу при працевлаштуванні такого кандидата.

Підприємство має право відкликати пропозицію про працевлаштування, або звільнити працівника при виявлені свідомого надання неправдивої інформації стосовно себе.

Звіти про перевірку біографічних даних зберігається, як конфіденційна інформація відділом кадрів.

20. РЕАГУВАННЯ НА ІНЦИДЕНТ

20.1. Повідомлення про порушення

Будь-який працівник, якому стало відомо про порушення політик інформаційної безпеки або про інцидент ІБ негайно повідомляє про це свого безпосереднього керівника та відповідального за ІБ.

Повідомлення повинно відбуватися негайно після виявлення можливого порушення або до закінчення зміни, якщо інші обов'язки заважають зробити це негайно.

Безпосередній керівник або відповідальний за ІБ перевіряє обставини можливого порушення та невідкладно вживає можливі заходи реагування на порушення, а також доповідає про порушення керівнику закладу.

Реагування на інцидент

Відповідальний за інформаційну безпеку при отримані повідомлення про порушення або інцидент самостійно або із залученням відповідних працівників Підприємства вживає заходів по збиранню та збереженню доказів та припиняє несанкціоновану дію. Відключає або локалізує ІТ-систему, яка може бути уражена. По можливості відновлює записи, дані, що могли постраждати. По можливості усуває вразливості та слабкі місця, які призвели до інциденту. За рішенням керівника повідомляє правоохоронним органам (кіберполіцію) про інцидент безпеки та його ознаки. Заклад повинен повідомляти Міністерство охорони здоров'я України про значні інциденти інформаційної безпеки. Порядок повідомлення про такі інциденти встановлюється МОЗ.

Розслідування та мінімізація ризиків

1. При інциденті інформаційної безпеки, що може причинити значні негативні наслідки відповідальний за ІБ долучає до розслідування членів Робочої групи з інформаційної безпеки. До РГІБ також долучається керівник відділу/підрозділу де трапився інцидент.
2. Група розглядає обставини, причини та наслідки інциденту та оцінює ризики інформаційної безпеки, які пов'язані з інцидентом. При цьому розглядаються наступні фактори, але не обмежуються ними:

- Характер цифрового активу, який постраждав в наслідок інциденту та його важливість для функціонування закладу;
- Необхідні заходи та засоби для відновлення функціонування;
- Договірні зобов'язання, які можуть бути не виконані, порушені;
- Ризики крадіжки особистих даних або втрати інформації в наслідок її псування, затирання чи шифрування, можливості щодо відновлення якомога актуальнішої версії резервного копіювання;
- Ризик заподіяння фізичної шкоди, якщо втрата даних ставить під загрозу життя людини;
- Ризик заподіяння шкоди репутації закладу;
- Обсяги (масив) втраченої, вкраденої чи зіпсованої інформації та кількість постраждалих осіб.

Повідомлення постраждалих

1. Відповідно до чинного законодавства заклад повідомляє постраждалим особам про виток їх персональних даних та медичної інформації.
2. Постраждалі особи повинні бути повідомлені не пізніше двох місяців після відбуття інциденту. Повідомлення повинні містити наступну інформацію:

- що сталося;
- яка сама персональна та медична інформація стосовно постраждалої особи вкрадена (скомпрометована) чи зіпсована;
- рекомендації, що постраждалій особі бажано зробити;
- інформація про дії закладу для запобігання подібних інцидентів у майбутньому;
- контактна інформація.

Повідомлення надсилається на електронну пошту постраждалої особи або інший електронний акаунт.

3. Якщо заклад повідомив про інцидент правоохоронні органи то інформування постраждалих осіб відбувається тільки після дозволу правоохоронців, щоб не перешкоджати кримінальному розслідуванню.

4. Непряме сповіщення, таке як публікація інформації на веб-сайті або сторінці закладу у соціальних мережах, може відбутися коли кількість постраждалих значна, перевищує 500 осіб.

5. Використання декількох методів оповіщення в певних випадках може виявитися найбільш ефективним підходом.

Профілактика

1. Після вжиття негайних заходів для зменшення ризиків, пов'язаних з порушенням, відповідальний за ІБ проводить розслідування причин порушення.

- При необхідності може проводитися аудит безпеки фізичних, організаційних і технологічних заходів.
- Це також може включати перегляд політики інформаційної безпеки.

2. Для проведення розслідування причин інциденту відповідальний за ІБ залучає відповідних працівників закладу та при необхідності зовнішніх експертів.

3. Результати розслідування доповідаються керівнику закладу разом з рекомендаціями, щодо запобігання подібних інцидентів у майбутньому.

4. За результатами складається план заходів з усунення недоліків, виявлених в ході розслідування інциденту, якщо це доречно.

Відповідальність

Керівник закладу несе повну відповідальність за захист даних та підтримку належного рівня інформаційної безпеки закладу. Керівництво та всі працівники закладу, які порушують політику інформаційної безпеки та/або чинне законодавство несуть дисциплінарну, адміністративну чи кримінальну відповідальність.

Інженер-програміст **Даниїл ЛОГУНОВ**

Юрисконсульт **Євгенія ГАЛЬЧЕНКО**

Додаток № 1
до Положення про
інформаційну безпеку

ЗГОДА ПРО НЕРОЗЛОШЕННЯ

Я розумію і погоджуюся зберігати, захищати та не розголошувати конфіденційну інформацію КНП "ДЦПМСД № 9" ДМР.

Крім того, я розумію, що будь-яке несанкціоноване використання або розголошення інформації закладу, може призвести до дисциплінарної, адміністративної чи кримінальної відповідальності відповідно до політики інформаційної безпеки КНП "ДЦПМСД № 9" ДМР та чинного законодавства.

Дата ПІБ, підпис

Додаток №2
до Положення про
інформаційну безпеку

ЖУРНАЛ РЕЄСТРАЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

№ з/п	Назва події	Дата. Час.	Ознаки	Вжиті заходи	Коментар

Додаток № 3
до Положення про
інформаційну безпеку

ЗГОДА НА ПЕРЕВІРКУ КАНДИДАТА

Я, _____, даю свою згоду КНП "ДЦПМСД №9" ДМР на перевірку моєї біографічної і особистої інформації. Я розумію, що за результатами цієї перевірки мені можуть не запропонувати працевлаштування в КНП "ДЦПМСД № 9" ДМР.

Дата _____ Підпис заявника _____

Підписи Сторін

Від сторони Роботодавця	**Від сторони Працівників**
Комунальне некомерційне підприємство «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради	**Первинна профспілкова організація Комунального некомерційного підприємства «Дніпровський центр первинної медико-санітарної допомоги №9» Дніпровської міської ради**
Генеральний директор	**Голова первинної профспілкової організації**
_____ **Галина ОДІНЦОВА**	_____ **Таїса ГРИЦЕНКО**
«01» лютого 2023 року	«01» лютого 2023 року

Пронумеровано, прошнуровано,
та скріплено печаткою
28 (двадцять вісім) арк.
Генеральний директор
КНП «ДЦПМСД № 9» ДМР
_____ Галина ОДІНЦОВА