Назва Закладу **Політика інформаційної безпеки**	
Назва: ПОЛІТИКА КОНТРОЛЮ ДОСТУПУ	**Для ЗОЗ 1 категорії**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Затверджено: ПІБ керівника ЗОЗ**

ПОЛІТИКА КОНТРОЛЮ ДОСТУПУ

1. Загальні положення

Мета цієї політики полягає в тому, щоб забезпечити контроль доступу до інформації та пристроїв, а також гарантувати наявність процедур для забезпечення надійного захисту інформації. Захист інформації з обмеженим доступом і зокрема захист персональних даних є пріоритетною ціллю.

2. Ролі щодо контролю доступу

Керівник закладу - визначає цю політику.

Відповідальний за інформаційну безпеку - координує цю політику.

Персонал - виконує цю політику, згідно посадових обов'язків.

3. Ідентифікація користувачів

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

- кожному користувачеві присвоюється унікальний обліковий запис;
- користувачі несуть відповідальність за використання та неправомірне використання свого індивідуального облікового запису користувача.

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

Обліковий запис блокується після максимум трьох (3) невдалих спроб входу в систему. Для відновлення доступу в цьому випадку потрібне залучення Адміністратора (відповідального фахівця ІТ-відділу).

Користувачі, яким необхідно отримати доступ до систем або мереж ЗОЗ, повинні заповнити відповідну Форму Доступу (Додаток 1). Ця форма повинна бути підписана безпосереднім керівником та погоджена керівником ЗОЗ або відповідальним за інформаційну безпеку.

4. Правила встановлення і поводження з паролями

Облікові записи користувачів і паролі потрібні для того, щоб отримати доступ до мереж і робочих станцій. До всіх паролів застосовується встановлена цим 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.

Вимоги до складу - Пароль повинен містити комбінацію символів латинського алфавіту верхнього та нижнього регістру, числових символів та спеціальних символів.

Частота зміни – Пароль повинен бути змінений кожні 30 днів. Скомпрометований пароль повинен бути змінений негайно.

Повторне використання - Попередні шість (6) паролів не можуть бути використані повторно.

Обмеження на обмін паролями - Паролі не повинні передаватися іншим працівникам, записуватися на папері або зберігатися на робочій станції і повинні зберігатися у таємниці.

Обмеження на відображення та зберігання паролів - Паролі маскуються на екрані робочої станції при введені, не друкуються і не включаються до електронних журналів чи звітів. Паролі зберігаються у зашифрованому виді.

5. Угода про конфіденційність

Користувачі інформаційних ресурсів Закладу при працевлаштуванні підписують угоду про конфіденційність (Додаток 2). Угода повинна містити наступне твердження:

Я розумію, що будь-яке несанкціоноване використання або розголошення конфіденційної інформації, може призвести до покарання, відповідно до чинного законодавства та політики інформаційної безпеки. Мої зобов'язання щодо нерозголошення конфіденційної інформації, залишаються чинними безстроково.

Тимчасово влаштовані працівники та підрядники, які не підписували угоди про конфіденційність, підписують такий документ при отримані доступу до інформаційних ресурсів ЗОЗ.

6. Контроль доступу

Інформаційні ресурси закладу захищаються за рахунок використання системи контролю доступу. Система контролю доступу включає внутрішні засоби захисту (паролі, шифрування, таблиці контролю доступу, налаштування інтерфейсів користувача тощо), так і зовнішні (пристрої захисту портів, брандмауери, автентифікацію на основі хоста тощо).

Правила доступу до ресурсів встановлюються власником ресурсу. Доступ надається тільки шляхом заповнення форми запиту на доступ (Додаток 1). Ця форма затверджується керівником чи відповідальним з ІБ.

При надані доступу використовується принцип мінімально необхідного доступу до ресурсу користувача для виконання ним функціональних завдань. Доступ користувача до відповідного ресурсу відбувається тільки після затвердження форми запиту на доступ керівником або головним лікарем та тільки до того ресурсу до якого був наданий запит на допуск.

В закладі можуть використовуватись випливаючи на екрані робочих станцій електронні попередження про несанкціоноване використання ресурсу та про відповідальність порушника.

При використанні програмного забезпечення управління безпекою кінцевих пристроїв повинна підтримуватися онлайн авторизації при використані додатків. Кожне підключення підлягає процесу авторизації (введенню логіна та пароля).

7. Припинення права доступу

Якщо працівник змінює посаду його безпосередній керівник ініціює перегляд прав доступу та заповнює Форму запиту на доступ (Додаток 1). У Формі вказується дата набрання чинності зміни посади та назва посади, щоб ІТ-відділ міг змінити права доступ відповідно до принципу мінімально необхідного доступу до ресурсів. Протягом обмеженого періоду працівнику, який змінює посаду, можуть зберігатися попередні права доступу, а також додаватися нові права доступу, необхідні для виконання нових посадових обов'язків.

Перегляд прав доступу персоналу повинен проводитися не рідше ніж раз на рік. Відповідальний за інформаційну безпеку повинен сприяти перегляду прав доступу користувачів, щоб переконатися, що весь персонал має мінімально необхідні права доступ для ефективного виконання своїх робочих функцій. Виявлені в ході перегляду надлишкові права доступу повинні припинятися.

8. Припинення дії облікового запису користувача

При звільненні працівника, його безпосередній керівник повинен завчасно ініціювати процедуру припинення доступу, вказавши «Видалити доступ» у Формі запиту на доступ (Додаток 1) та дату останнього робочого дня працівника, щоб його обліковий запис користувача міг бути налаштований на закінчення терміну дії у день звільнення.

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

Не рідше одного разу на рік, відповідальний з інформаційної безпеки повинен ініціювати перегляд списку активних облікових записів користувачів для оцінки прав доступу відповідно до принципу надання мінімально необхідного доступу до IT-ресурсів для виконання функціональних завдань. Керівники відділів закладу повинні переглянути списки доступу стосовно своїх підлеглих та протягом п'яти (5) робочих днів надати уточнюючи дані щодо прав доступу. Якщо буде виявлені надлишкові права доступу вони повинні бути припинені. Про необхідність припинення надлишкових прав доступу або блокуванні активних акаунтів звільнених працівників керівники відділів закладу без зволікань повідомляють IT-відділ та надає оновлену Форму запиту на доступ (Додаток 1).

9. Заходи з безпеки екстреного доступу до електронної захищеної медичної інформації

Заклад забезпечує для медпрацівника гарантований терміновий засіб доступу до електронної захищеної медичної інформації у разі екстреної необхідності.

Рішення екстреного доступу використовується лише тоді, коли звичайні процеси виявляються недостатніми для своєчасного надання медичної допомоги і дозволяються в наступних ситуаціях, які можуть виникнути при наданні невідкладної медичної допомоги пацієнту:

- Медпрацівник забув свої ім’я користувача/пароль;
- Пароль медпрацівника заблокований;
- Медпрацівник не має облікового запису користувача;
- Збій центральної системи автентифікації;
- Несправність зчитувача смарт-карти або біометричних даних;
- Невідкладна медична ситуація змушує особу виконувати роль, у якій він/вона не має достатніх прав доступу до необхідної електронної захищеної медичної інформації.

Відповідальний з інформаційної безпеки розробляє, документує, впроваджує та перевіряє процедури екстреного доступу, які використовуються у випадку надзвичайної ситуації, яка вимагає екстреного доступу до електронної захищеної медичної інформації. Для кожної системи, яка містить електронну захищену медичну інформацію розроблена чітко визначена та зрозуміла процедура надання термінового доступу за допомогою альтернативних та/або ручних методів в екстрених випадках. Всі облікові записи для екстреного доступу та процедури розподілу доступу для них задокументовані та протестовані.

Доступ до таємних даних автентифікації, такі як логін та пароль, для використання надзвичайних облікових записів, створених заздалегідь, надаються на таких носіях, як друкована сторінка, картка з магнітною смугою, смарт-картка або жетон в залежності від способу автентифікації для конкретної системи.

Носій з таємними даними автентифікації зберігається в запечатаному конверті у сейфі старшої медсестри. Отримання носія вимагає надання ідентифікації за допомогою посвідчення особи, яка отримує носій, та реєстрації факту отримання носія в журналі реєстрації з метою гарантування принципу 4-х очей та неспростовності події.

Всі факти використання носія, перевіряються відповідальним з інформаційної безпеки. Під час перевірки, робиться огляд виконаної діяльності, включаючи отримані дані або дані, до яких був доступ. Отримані фактичні дані та контрольні журнали звіряються, щоб пересвідчитися в їх відповідності. Якщо це необхідно, відповідальний з інформаційної безпеки робить відповідні записи з розкриття інформації. Для запобігання повторному використанню, коли пароль відомий, екстрені облікові записи невідворотно блокуються. Відповідальний з інформаційної безпеки визначає ефективність процедури екстреного доступі, і за необхідності корегує її.

Неприйнятне використання екстреного доступу фіксується як інцидент інформаційної безпеки, відносно якого вживаються відповідні заходи реагування на інциденти.

Відповідальний з інформаційної безпеки щорічно проводить перевірку і навчання персоналу, щоб переконатися, що процедура екстреного доступу залишається актуальною.

9. Заходи безпеки з обмеження доступу до персональних даних

В закладі встановлено процес класифікації персональних даних. Персональні дані збираються лише на основі особистої згоди, або якщо це визначено чинним законодавством, і лише з метою та в обсязі, як це зазначено у згоді чи визначено законодавством. Персональні дані обробляються та зберігаються не довше, ніж це необхідно для досягнення цілей, для яких вони були зібрані. Персональні дані можуть передаватися третім особам лише за наявності дозволу чи відповідно до вимог законодавства. Зібрані персональні дані захищаються від несанкціонованого доступу відповідно до вимог чинного законодавства та кращих галузевих практик.

Встановлені та виконуються наступні процедури:

- отримання згоди фізичних осіб на збір персональних даних;
- надання доступу до персональних даних;
- обробки та зберігання персональних даних;
- безпечної передачі персональних даних третім особам;
- деперсоналізації персональних даних;
- безпечного видалення персональних даних;
- обробки запитів та претензій від осіб щодо обробки їхніх персональних даних, експорту даних;
- повідомлення про інциденти несанкціонованого доступу чи цілісності персональних даних.

Доступ до персональних даних надається обмеженій групі осіб. Доступ до персональних даних надається на підставі службових обов'язків в частині медичного обслуговування пацієнтів. Експорт масиву персональних даних здійснюється у виняткових випадках через формальне затвердження з боку керівництва.

Кількість працівників, яким надається доступ до персональних даних обмежена до мінімально необхідної з урахуванням необхідності забезпечити надання доступу для осіб, які будуть заміняти колег у разі відсутності для забезпечення неперервності процесів закладу.

Передача персональних даних включно з персональними медичними даними третій стороні заборонена, окрім випадків, коли це дозволено згодою пацієнта чи передбачено законодавством. Для всіх процесів, що включають доступ третьої сторони до персональних даних визначено ролі та обов'язки володільця та розпорядника даних.

Одразу після досягнення мети обробки персональних даних, вони деперсоналізуються чи безпечно видаляються, включно з персональними медичними даними. В іншому випадку, отримується нова згода пацієнта на обробку його персональних даних. Видалення персональних даних здійснюється безпечно і невідворотно, відповідно до кращих галузевих практик.

10. Заходи безпеки з обмеження фізичного доступу

Заходи безпеки з обмеження фізичного доступу визначені в розділі "ФІЗИЧНА БЕЗПЕКА" Політики інформаційної безпеки Закладу.

11. Відповідальність

Вимоги цієї політики поширюються на весь персонал закладу. Усі працівники закладу мають бути ознайомлені із її вимогами. Відповідальність за порушення визначена у відповідному розділі затвердженої Політики інформаційної безпеки Назва ЗОЗ.