Назва Закладу **Політика інформаційної безпеки**	
Назва: ПОЛІТИКА ВИКОРИСТАННЯ МЕРЕЖ І ПОСЛУГ МЕРЕЖІ	**Для ЗОЗ 2 категорії**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Затверджено: ПІБ керівника ЗОЗ**

ПОЛІТИКА ВИКОРИСТАННЯ МЕРЕЖ І ПОСЛУГ МЕРЕЖІ

1. Загальні положення

Мета цієї політики полягає в тому, щоб забезпечити контроль доступу до мережі та послуг мережі, гарантувати наявність процедур для забезпечення того, що користувачі отримують доступ до мережі та послуг мережі лише тоді, коли вони були спеціально авторизовані для такого використання. 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. Доступ до Інтернет

Заклади охорони здоров’я, які перебувають у державній власності, закуповують послуги (укладають договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій, які забезпечують Захищені вузли доступу до мережі Інтернет (ЗВІД) відповідно до Переліку операторів (провайдерів) телекомунікацій, що надають послуги з доступу до мережі Інтернет та мають чинні атестати відповідності систем захисту ЗВІД.

Усі пристрої, яким необхідний зв’язок з Інтернет, повинні бути у DMZ-зоні. Пристрої, що не використовують Інтернет-з’єднання, не повинні знаходитися в DMZ-зоні.

Доступ в Інтернет надається тільки тим співробітникам, хто його потребує для виконання службових обов’язків. Доступ до Інтернет це ресурс, за який ЗОЗ 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.

Персонал повинен розуміти, що індивідуальне використання Інтернету контролюється, і 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, то 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 брандмауерами. 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 ЗОЗ 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 ЗОЗ 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. Мережа може бути використана для продажів послуг ЗОЗ, однак 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.

4. 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 ЗОЗ, або обробляються на пристроях, що належать закладу, вважаються власністю Назва ЗОЗ, 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 ЗОЗ 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 ЗОЗ для отримання особистої вигоди суворо заборонено.
    4. Політична діяльність – Вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів ЗОЗ. Заклад заохочує своїх працівників голосувати та активно брати участь у виборчому процесі, але ці заходи не повинні виконуватися з використанням активів та ресурсів ЗОЗ.
    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 IT-ресурсів ЗОЗ 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.

Заклад зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів ЗОЗ. 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. Наприклад, для аудиту або аналізу витрат на зв'язок, можуть відстежуватися набрані номери зі службових телефонів, тривалість дзвінків, кількість дзвінків на/з конкретного телефону, час доби і т.д. Інші приклади, 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.

Заклад 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.

5. 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 тільки на вимогу керівника відділу з поданням Форми доступу (Додаток 1) та затверджуються керівником закладу чи відповідальним з ІБ.

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.

6. 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.

7. 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.

8. Договір на телекомунікаційні послуги

При укладанні договору на отримання телекомунікаційних послуг закладом необхідно враховувати наступні вимоги до постачальника таких послуг:

- відповідні розділи політики інформаційної безпеки надавача послуг були переглянуті та приведені у відповідність з вимогами політики інформаційної безпеки закладу;
- відповідні вимоги враховані та застосовуються;
- проведена оцінка ризиків пов’язаних з виконанням додаткових зобов'язань надавача послуг;
- включене право на аудит виконання договірних зобов’язань;
- домовленість стосовно повідомлення про інциденти інформаційної безпеки включені в угоду;

- наданий опис кожної послуги, яка буде доступна;
- доступ до ресурсів закладу надавачем послуг повинен бути лише на мінімально необхідному рівні, достатньому для виконання договірних зобов'язань;
- детальний список користувачів з боку надавача послуг, які будуть мати доступ до мережі закладу, повинен бути доступний для аудиту;
- дата і час, коли послуга повинна бути доступна, завчасно узгоджені;
- процедури щодо захисту інформаційних ресурсів узгоджені заздалегідь, а спосіб аудиту затверджений обома сторонами;
- спосіб моніторингу і припинення доступу користувачів визначений;
- обмеження на копіювання та розкриття інформації включені;
- обов'язки щодо встановлення та технічного обслуговування апаратного та програмного забезпечення зрозумілі та заздалегідь узгоджені;
- заходи щодо забезпечення повернення або знищення програмного забезпечення та інформації після закінчення дії договору визначені та прописані;
- заходи фізичного захисту, при необхідності, також включені в угоду;
- спосіб надання доступу та авторизація користувачів, повинен бути встановлений до того, як користувачам буде наданий доступ;
- створені механізми для забезпечення дотримання заходів безпеки сторонами угоди;
- детальний перелік заходів безпеки, які будуть вжиті сторонами угоди, повинен бути розглянутий та погоджений до укладення угоди.

9. Сегментація мережі

Мережа закладу сегментована наступним чином:

1. Внутрішня мережа.
2. Технологічна мережа (за наявності підключених до мережі керованих пристроїв).
3. Демілітаризована зона (за наявності пристроїв, які використовують Інтернет).
4. Зовнішня мережа віддалених або хмарних сервісів (за наявності таких сервісів).
5. Гостьова мережа (за умови надання гостьового доступу).

Сегменти мережі ізольовані один від одного за допомогою фізичного та логічного розмежування.

10. Визначення захисту периметру мереж

Сегменти мережі відділені від інших мереж захисним периметром. Захисний периметр побудовано з використанням міжмережевого екрана (брандмауера). Доступ з Інтернет надається лише до тих IT-сервісів закладу, які мають бути загальнодоступними. Доступ до мережевих портів та протоколів обмежується тільки тими, які необхідні для загальнодоступних сервісів. Підключення до засобів оброблення інформації сторонніх мережевих пристроїв технічно заблоковано адміністративними політиками безпеки операційної системи хоста. Використання бездротових подовжувачів та підсилювачів

сигналу заборонено. Сигнал точок бездротового доступу не розповсюджується за фізичний периметр організації і не доступний поза приміщеннями організації.

11. Брандмауер

Всі комп'ютери закладу захищені від безпосереднього доступу з Інтернет та загроз із внутрішньої мережі за допомогою зовнішніх та вбудованих брандмауерів. Політика брандмауерів за замовчанням, встановлена як "заборонено все, що явно не дозволено". Налаштування брандмауерів контролюється відповідальним з ІБ. Якщо брандмауер знаходиться та/або налаштовується стороною, яка надає ІТ-послуги закладу, то ця сторона надає повну інформацію про актуальні налаштування брандмауера відповідальному за інформаційну безпеку та активно співпрацювати з ним/нею у питаннях подальшого його використання та змін налаштувань.

Всі зміни списку контролю доступу (ACL) відстежуються в спеціалізованій системі обліку. Правила є конкретними і визначають мережеві протоколи та порти, де це можливо. Правила надають тільки мінімально необхідний доступ і не дають надлишкові права доступу. Мережеві протоколи та порти, які зокрема використовуються для адміністративного доступу, такі як SSH (TCP/UDP 22) або RDP (TCP 3389), не дозволені для недовірених мереж. Вхідний ICMP трафік з недовірених мереж обмежений лише необхідними типами та кодами ICMP повідомлень. ACL обмежує трафік для версії IP протоколу IPv6. ACL блокує зовнішній вхідний трафік, якщо замість зовнішньої IP-адреси відправника вказано IP-адресу, яка належить діапазону IP адрес внутрішньої мережі закладу. Нові правила задокументовані у системі управління фаєрволом або в іншій системі для централізованого зберігання таких записів. Опис правила містить таку інформацію:

- ім'я особи, яка додала правило;
- дата додавання правила;
- призначення правила;
- ІТ-компоненти та користувачі, на яких вплине зміна;
- обґрунтування правила.

Кожне нове правило (новий запис у ACL) перевірено перед впровадженням, щоб переконатися, що воно працює належним чином. Кожна фактична зміна ACL автоматично реєструється в системі реєстрації подій.

12. Заходи щодо обмеження доступу до внутрішньої мережі

Доступ до внутрішньої мережі мають тільки авторизовані мережеві пристрої та засоби оброблення інформації. Санкціонування доступу до внутрішньої мережі відбувається відповідно до "Політики контролю доступу". Для контролю доступу кінцевих пристроїв до мережі використовується протокол контролю доступу 802.1x або технологія управління доступом до мережі (NAC) для автоматичної оцінки відповідності кінцевих пристроїв встановленим вимогам безпеки та блокування

доступу до мережевих ресурсів, якщо такі вимоги не виконуються. Пристрої, що не відповідають встановленим вимогам, розміщуються в карантинній зоні, де будуть задіяні виправлення перед наданням доступу до мережі. При віддаленому доступі до внутрішньої мережі запроваджено багатофакторну автентифікацію.

13.Заходи щодо обмеження доступу до бездротових мереж

Бездротовий доступ до інформаційних ресурсів з обмеженим доступом надається лише у виняткових випадках за службової необхідності та на основі письмового дозволу керівництва відповідно до "Політики контролю доступу". Заборонено використання бездротових протоколів і конфігурацій, що мають серйозні вразливості безпеки. Використовуються лише точки бездротового доступу, які автоматично припиняють з’єднання після встановленого періоду. Період активності сесії бездротового доступу встановлюється відповідно до ділових потреб, але не більше 24 годин. Для доступу до бездротових мереж використовується протокол WPA-802.1X. Сигнал точок бездротового доступу не розповсюджується за фізичний периметр організації і не доступний поза приміщеннями організації.

14. Заходи щодо обмеження доступу до гостьової мережі

Гостьова мережа відділена від внутрішніх IT-сервісів. Гостьовий доступ в Інтернет фільтрується та проксується. Доступ до неправомірного веб-контенту заборонено. Фільтрування контенту налаштоване відповідно до прийнятного використання гостьового доступу до мережі. Для гостьових з'єднань встановлено обмеження пропускної здатності. Доступ до гостьової мережі контролюється та спостерігається IT-відділом. При наданні послуг доступу, споживачам надається можливість ознайомитись і явним чином прийняти Умови обслуговування перед отриманням доступу до Інтернет. Умови обслуговування розроблено за допомогою професійного юриста для того, щоб забезпечити, що ці умови також будуть захищати заклад від потенційних юридичних дій кінцевих користувачів як результату певних втрат або шкоди, понесених внаслідок шкідливого вмісту або нечітких політик і практик надання послуг.

15.Обмеження доступу до мережевих пристроїв

Адміністративний доступ до мережевих пристроїв захищений паролем. Користувач із звичайними правами доступу не має можливості змінювати мережеву конфігурацію робочого комп’ютера. Маршрутизація між зовнішніми мережевими інтерфейсами ПК кінцевих користувачів адміністративно відключена на рівні ядра операційної системи хоста. Мережеве обладнання захищене та налаштоване відповідно до рекомендацій постачальників та кращих галузевих практик. Налаштування робочої конфігурації мережевого обладнання супроводжується змінами збереженої конфігурації та контролем версій, щоб уникнути завантаження слабшого стану безпеки. Робиться резервна копія конфігурації мережевого обладнання щоразу до і після внесення змін.

Використовується технологія захисту проти ARP спуфінгу. Мережеве обладнання розміщується тільки в серверних, телекомунікаційних кімнатах або шафах, доступ до яких обмежено виключно авторизованим персоналом, відповідно до обмежень фізичного доступу визначених в розділі “ФІЗИЧНА БЕЗПЕКА” Політики інформаційної безпеки.

16. Заходи щодо обмеження доступу до персональної ідентифікаційної інформації з використанням інтернет та/або хмарних обчислень

Персональна ідентифікаційна інформація (PII), що передається загальнодоступними мережами передачі даних, зашифрована до її передачі. Якщо доступ до збереженої в хмарі PII є більш ніж у одного користувача, то з метою ідентифікації, автентифікації та авторизації кожен з них має унікальний ідентифікатор користувача. Відповідальний за інформаційну безпеку веде актуальний облік користувачів або профілів користувачів, які мають санкціонований доступ до PII. Для всіх користувачів, чий доступ авторизований процесором PII публічної хмари, підтримується актуальний профіль користувача. Профіль користувача містить сукупність даних про користувача, включаючи ідентифікатор користувача, необхідний для реалізації технічних заходів безпеки, які забезпечують санкціонований доступ до PII.

Договори між процесором PII публічної хмари та будь-якими субпідрядниками, що обробляють PII встановлюють мінімально необхідні технічні та організаційні заходи, які відповідають заявленим зобов'язанням щодо забезпечення заходів безпеки та захисту PII в публічній хмарі. Такі заходи не зазнають скорочення субпідрядником в односторонньому порядку. Заходи безпеки PII поширюються на зберігання резервних копій субпідрядників.

Процесор PII публічної хмари гарантує, що як тільки споживачеві служб хмарних обчислень буде виділено область пам'яті, будь-які дані, що раніше були в ній, не стануть доступні цьому споживачу служб хмарних обчислень.

Процесор PII публічної хмари визначив та документально зафіксував країни, в яких можуть зберігатися PII. Ідентичність (справжність) країн, де зберігаються PII, доступна для споживачів служб хмарних обчислень. Ідентичність країн, що виникають при залученні до обробки PII субпідрядників, включена. Процесор PII публічної хмари у строк, встановлений у договорі, інформує споживача служб хмарних обчислень про будь-які намічені зміни, щоб у споживача служб хмарних обчислень була можливість заперечити проти таких змін або припинити договір.

17. Заходи щодо реєстрації подій

Для уможливлення запису та виявлення дій, які можуть впливати чи бути пов’язані з інформаційною безпекою, на всіх активних компонентах та вузлах мережі застосується автоматична реєстрація подій та моніторинг за допомогою системи виявлення вторгнення. Інформація про інциденти інформаційної безпеки, пов’язані з хмарною

службою та реагування на повідомлення системи виявлення вторгнення відбувається відповідно до встановленого порядку реагування на інциденти інформаційної безпеки.

18.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.