USAID
FROM THE AMERICAN PEOPLE

SOERA

Діяльність
у рамках реформи
державних
підприємств
України

ІТ АУДИТ: ЧАСТИНА ІІ

Підвищення рівня якості внутрішнього аудиту

5 вересня
2024 р.

ТЕХНІЧНІ ПРОБЛЕМИ. Якщо ви зіткнулися з технічними проблемами, зверніться по допомогу до нашої команди технічної підтримки. Також ви можете написати у чат.

МАТЕРІАЛИ КУРСУ. Матеріали курсу будуть розіслані електронною поштою після сьогоднішнього тренінгу та відображатимуться на екрані протягом усієї навчальної сесії (поточні/попередні матеріали тренінгів будуть розміщені на веб-сайті Міністерства Фінансів України у розділі Департаменту гармонізації ДВФК за посиланням https://mof.gov.ua/uk/provedeni-zahodi-z-pitan-dvfk або QR-кодом).

ЗАПИТАННЯ. В кінці нашого тренінгу буде сесія питань та відповідей. Не зволікайте задавати питання через чат. Команда викладачів опрацює питання, на які не вдасться відповісти відразу, ми надішлемо учасникам відповіді на їх електронну пошту.

МІКРОФОНИ. Мікрофони потрібно вимкнути, щоб усунути зайвий фоновий шум. Якщо хочете поставити запитання, будь-ласка, напишіть у чат.

ПОПЕРЕДЖЕННЯ ПРО ЗАПИС. Зауважте, що заняття буде записуватися для цілей навчання та документування. Беручи в ньому участь, ви погоджуєтеся на запис.

ІТ АУДИТ: ЧАСТИНА ІІ

Стандарти USAID (ADS) вимагають, щоб учасники були присутніми мінімум протягом 90% загальної тривалості курсу, щоб вважатися такими, що його пройшли.

Присутність на тренінгах.

Присутність важлива, щоб забезпечити отримання всіма учасниками необхідної програмної інформації та навчальних матеріалів.

Зверніть увагу, що для отримання сертифіката про проходження курсу необхідно виконати такі вимоги:

- Бути присутніми протягом принаймні 90% тривалості заняття.
- Пройти опитування перед початком курсу та після його завершення.
- Пройти оцінювання курсу.

У разі оголошення повітряної тривоги, будь-ласка, перейдіть у безпечне місце. Зверніть увагу, що тренінг буде проходити без перерв, оскільки здійснюється запис для навчальних та документальних цілей.

Цей тренінг був розроблений для Департаменту гармонізації державного внутрішнього фінансового контролю Міністерства фінансів України і не призначений для використання будь-якими іншими сторонами. Крім того, цей тренінг ґрунтується на галузевих практиках і вимогах чинних законів і нормативно-правових актах станом на 05 вересня 2024 року. Такі практики, закони й нормативні акти можуть змінюватися, тому учасникам тренінгу слід регулярно стежити за оновленими рекомендаціями щодо змісту цього тренінгу.

Програма

1. Вступ
2. Підготовка
3. Домен I: Практичні аспекти аудиту щодо процесу управління доступами
4. Домен II: Безпека людських ресурсів.
   Домен III: Фізична безпека та безпека інфраструктури
5. Сесія запитань та відповідей

Цілі

- Підвищення рівня знань з аудиту інформаційних технологій серед фахівців внутрішнього аудиту.
- Сприяння формуванню сталого рівня компетенцій функції внутрішнього аудиту.
- Створення основи для довіри до результатів роботи та професійних суджень внутрішніх аудиторів.
- Покращення іміджу функції внутрішнього аудиту як професійного консультанта.

Цей тренінг являє собою 2,5 годинний курс, який проводиться 05 вересня 2024 року з 10:00 до 12:30 за київським часом.

USAID
FROM THE AMERICAN PEOPLE

ДОМЕН І:
Практичні аспекти аудиту щодо процесу управління доступами

ПОВТОРЕННЯ І ПРАКТИКА

Зона ризиків ІТ: Захист доступу

ЦІЛІ, РИЗИК, ТА КОНТРОЛЬ ПРОЦЕСУ.

УПРАВЛІННЯ ДОСТУПОМ – це процес ідентифікації, відстеження, контролю та керування правами доступу користувачів до інформаційних систем та відповідних даних. Будь-який користувач, який запитує доступ до систем, додатків або даних, повинен бути ідентифікований, автентифікований, та авторизований.

РИЗИК І КОНТРОЛЬ

Процес управління доступом в організації, з відповідними контролями**, покликаний зменшити (мітигувати) ризик**, того, що користувачі мають привілеї доступу, що виходять за межі необхідних для виконання покладених на них обов'язків, що може призвести до неналежного розподілу обов'язків та зловживання відповідними правами.

Зона ризиків IT: Захист доступу

РЕЄСТРАЦІЯ ТА ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА (ВКЛЮЧАЮЧИ ПРИВІЛЕЙОВАНІ ПРАВА)

Ціль:

Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.

Вимога:

Має бути впроваджено **процес реєстрації** та зняття з реєстрації для того, щоб була можливість управляти правами доступу.

Реєстрація та зняття з реєстрації **користувача** покладається на:

- **отримання дозволу** від власника інформаційної системи чи послуги для використання інформаційної системи чи послуги
- перевірку, **що рівень доступу наданий відповідно до політик доступу** та погоджений з іншими вимогами, такими як **розділення обов'язків**
- гарантування, що права доступу не активовані (наприклад, сервіс-провайдером) до того, як процедури авторизації буде завершено
- підтримки головного журналу прав доступу, наданих ID користувача для доступу до інформаційних систем чи послуг
- зміна прав доступу користувачам, які змінили ролі чи роботу, та негайне вилучення чи блокування прав доступу користувачам, які звільнилися з організації
- **періодичний перегляд прав доступу** разом із власниками інформаційних систем або послуг

Зона ризиків IT: Захист доступу

РЕЄСТРАЦІЯ ТА ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

Політика управління доступом

ВІДПОВІДНИЙ КОНТРОЛЬ:

Керівництво затверджує характер та обсяг привілеїв доступу для нових користувачів, включаючи стандартні профілі/ролі додатків, критичні операції з фінансовою звітністю та розподіл обов'язків.

Зона ризиків ІТ: Захист доступу

РЕЄСТРАЦІЯ ТА ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Зверніться до відповідальних осіб на підприємстві, щоб зрозуміти процес, згідно якому запрошується та затверджується новий доступ чи виконується зміна доступу (модифікація). Зокрема, розгляньте можливість отримати розуміння наступних атрибутів:	Дивіться нижче	Дивіться нижче
Політики та процедури з наданням доступу користувачам до систем та даних	Аудитор ознайомився з політикою інформаційної безпеки та політикою управління доступом і визначив вимоги щодо надання доступу (ким, кому, на якій основі, тощо).	Політики та процедури вивчені. Відповідні процеси проаналізовані перед тестуванням.
Особи або групи, відповідальні за затвердження доступу	Аудитор визначив осіб, або групи (робочі), відповідальних за перевірку та затвердження доступу.	Відповідальні за затвердження доступу визначені, інтерв'ю проведені.
Окремі особи або групи, відповідальні за адміністрування доступу	Аудитор визначив осіб або групи (робочі), відповідальних за валідацію та надання доступу.	Відповідальні за адміністрування доступу визначені, інтерв'ю проведені.
Визначено та проаналізовано процес затвердження та документування запиту на доступ користувачів	Аудитор проаналізував процес надання, або зміни прав співробітників у всіх відповідних випадках.	Приклад запиту на доступ для користувача отримано.

Зона ризиків ІТ: Захист доступу

РЕЄСТРАЦІЯ ТА ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Чи використовується інструмент для надання нового доступу та як використання цього інструменту контролюється	Аудитор визначив, чи існує інструмент для адміністрування доступу та встановив відповідальних за контроль такого інструменту.	Інструмент оцінено та провалідовано (якщо інструмент такий використовується).
Чи існує розподіл обов'язків між особою, яка затверджує, та особою, яка надає доступ до систем	Аудитор визначив, чи існує розподіл обов'язків між особою, або групою осіб, які схвалюють доступ, і особою, або групою осіб, які адмініструють доступ.	Документ\Матриця розподілу обов'язків вивчена та проаналізована в розрізі процесу надання доступів.
Чи існують різні процеси для надання доступу особам, які не є співробітниками (постачальники, підрядники)?	Аудитор проаналізував та перевірив процеси надання доступу іншим особам, які не є співробітниками (постачальниками, підрядниками) і визначив, що такий процес виконується відповідно.	Політики та процедури вивчені. Відповідні процеси проаналізовані.
Наявні процеси, пов'язані з розподілом обов'язків під час надання чи відкликання доступів	Аудитор проаналізував та перевірив механізм розподілу обов'язків під час процесу надання прав доступу та визначив, що такий механізм є відповідними.	Політики та процедури вивчені. Відповідні процеси проаналізовані.

Зона ризиків ІТ: Захист доступу

РЕЄСТРАЦІЯ ТА ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

АУДИТОРСЬКІ ПРОЦЕДУРИ

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Отримайте популяцію нових запитів для цільової системи на надання доступу користувачів протягом періоду аудиту. Зробіть вибірку таких запитів і протестуйте наступні атрибути: • Запит на доступ користувача схвалено відповідним керівництвом (A); • Запитуваний доступ узгоджується з доступом, наданим у системі (B); • Наданий доступ відповідає обов'язкам, призначеним користувачем, і забезпечує належний розподіл обов'язків (B); • Розподіл обов'язків підтримується між тим, хто затверджує, і особою, яка надає доступ до системи (C);	Визначена цільова популяція Визначена вибірка Дотримано всіх відповідних критеріїв тестування при тестувані окремих елементів вибірки Надано висновок по відповідності (ефективності) контролю; визначенні	Цільова популяція Вибірка Атрибути тестування

									Атрибути			
Номер	USER_ID	User Name	Посада	Ім'я привілейованого користувача	Дані створення в системі	Доступ ухвалено	Запитані ролі/атрибути	Надані ролі\атрибути	A	B	C	Відхилиня
1	1000	YPASH	Фінансовий Аналітик	Євген Пащенко	Департамент Фінансового Аналізу	Начальник Департаменту	Атрибут 1, Атрибут 2, Атрибут 3	Атрибут 1, Атрибут 2, Атрибут 3	Так	Так	Так - відповідно до вимог посади	No

Зона ризиків ІТ: Захист доступу

ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

Політика управління доступом

ВІДПОВІДНИЙ КОНТРОЛЬ:

Доступ звільнених та/або переведених користувачів своєчасно видаляється або змінюється (модифікується).

Зона ризиків IT: Захист доступу

УПРАВЛІННЯ ДОСТУПАМИ: ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Зверніться до відповідальних осіб на підприємстві, щоб зрозуміти процеси, пов'язані з видаленням доступу до програми для звільнений користувачів, або користувачів чиї права були модифіковані. Зокрема, розгляньте можливість отримати розуміння наступних атрибутів, якщо це доречно:	Дивіться нижче	
Політики або процедури, пов'язані з зняттям з реєстрації користувачів\відкликанням доступів	Аудитор проаналізував політику інформаційної безпеки та політику управління доступом і визначив вимоги до зняття з реєстрації користувачів чи зміни доступів (ким, кому, на якій основі, тощо).	Політики та процедури вивчені. Відповідні процеси проаналізовані перед тестуванням.
Механізм інформування IT-менеджменту про відкликання чи зміну прав користувачів		Механізм інформування IT-менеджменту
Як доступ змінюється, або відкликається після припинення чи зміни повноважень, я також, чи використовується той самий процес для штатних та нештатних працівників (таких як постачальники, підрядники тощо)?		Політики та процедури вивчені. Відповідні процеси проаналізовані перед тестуванням.

Зона ризиків IT: Захист доступу

УПРАВЛІННЯ ДОСТУПАМИ: ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Чи процес видалення доступу є ручним чи автоматизованим?	Аудитор визначив та проаналізував механізм видалення доступу.	Політики та процедури: процес відкликання доступу проаналізовано.
Чи використовується інструмент для відкликання доступу?	Аудитор визначив та проаналізував чи використовується інструмент для відкликання доступу.	Інструмент оцінено та провалідовано (якщо інструмент такий використовується).
Спосіб припинення доступу до програм та систем (наприклад, заблокувати або видалити).	Аудитор визначив та проаналізував спосіб припинення доступу до програм та систем.	Вимоги щодо механізму припинення доступу до програм та систем **проаналізовані.**
Хто несе відповідальність за адміністрування безпеки та зміну доступу користувачів у разі звільнення чи переведення (зміни статусу працівника)?	Аудитор визначив та проаналізував відповідальних за адміністрування безпеки та зміну доступу користувачів у разі звільнення чи переведення.	Політики та процедури: адміністрування безпеки в процесі зміни доступу користувачів проаналізовано.
Якими є очікування щодо своєчасного скасування доступу користувача?	Аудитор визначив та проаналізував адекватність періоду на протязі якого змінюється доступ користувачів.	Політики та процедури: вимоги щодо своєчасного відкликання чи зміни доступів.

Зона ризиків ІТ: Захист доступу

УПРАВЛІННЯ ДОСТУПАМИ: ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очіуваний результат	Елементи тестування
Отримайте від відділу кадрів повний список звільнених (чи переведених) співробітників і підрядників на період аудиторської перевірки. Виходячи з частоти та ризику, пов'язаного з контролем, зробіть вибірку користувачів, доступи яких було припинено (знято з реєстрації). Для кожного вибраного користувача, перевірте такі атрибути та надайте висновок щодо ефективності контролю: Права доступу для звільненого користувача більше не активні в системі. Такий доступ було видалено або заблоковано своєчасно (на основі дати припинення повноважень). Приклади:	Визначена цільова популяція Визначена вибірка Дотримано всіх відповідних критеріїв тестування при тестувані окремих елементів вибірки Надано висновок по відповідності (ефективності) контролю; визначенні відхилення та причини.	Цільова популяція Вибірка Атрибути тестування

						Атрибути		
Номер	Користувачь	Ім'я Користувача	Дата Звільнення	LOCK_DATE в Системі	Дата останьої активності згідно MS AD	A	Статус в Системі	Відхилення
1	Пащенко Євген	YPASHCH	03.02.2023	03.02.2023 17:09:07	2/3/2023 3:46	Так	Заблоковано	No

Зона ризиків IT: Захист доступу

ЗНЯТТЯ З РЕЄСТРАЦІЇ КОРИСТУВАЧА: МОДИФІКАЦІЯ ДОСТУПУ

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Отримайте популяцію нових запитів для цільової системи на модифікацію доступу користувачів протягом періоду аудиту. Зробіть вибірку таких користувачів і протестуйте наступні атрибути: • Роль, яка змінюється внаслідок переведення працівника, є відповідною та відповідає авторизованим ролям для нової посади переведеного працівника. (A); • Зміни посад у зв'язку з переведенням співробітників були своєчасно санкціоновані відповідним рівнем керівництва (B). Приклад:	Визначена цільова популяція Визначена вибірка Дотримано всіх відповідних критеріїв тестування при тестуванні окремих елементів вибірки Надано висновок по відповідності (ефективності) контролю; визначенні відхилення та причини.	Цільова популяція Вибірка Атрибути тестування

Transferred Employees									
Attributes									
A	Роль, яка змінюється внаслідок переведення працівника, є відповідною та відповідає авторизованим ролям для нової посади переведеного працівника.								
B	Зміни посад у зв'язку з переведенням співробітників були своєчасно санкціоновані відповідним рівнем керівництва.								
						Attributes			
Номер	Користувачь	Ім'я Користувача	Дата трансферу	Посада до трансферу	Нова посада	A	B	Зміна прав?	Discrepancy noted?
1	Пащенко Євген	YPASHCH	03.02.2023	Менеджер	Заступник голови департаменту	Так	Так	Права не змінено - права відповідні посаді	No

Зона ризиків IT: Захист доступу

ПЕРЕГЛЯД ПРАВ ДОСТУПУ КОРИСТУВАЧІВ

Політика управління доступом

ВІДПОВІДНИЙ КОНТРОЛЬ:

Доступ користувачів періодично переглядається.

Зона ризиків ІТ: Захист доступу

УПРАВЛІННЯ ДОСТУПАМИ: ПЕРЕГЛЯД ПРАВ ДОСТУПУ КОРИСТУВАЧІВ

АУДИТОРСЬКІ ПРОЦЕДУРИ

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Зверніться до відповідальних осіб на підприємстві, щоб зрозуміти процес, згідно якому переглядається доступ та виконується зміна доступу за потреби (модифікація). Зокрема, розгляньте можливість отримати розуміння наступних вимог та процесів:	Дивіться нижче	Дивіться нижче
Політики та процедури управління доступом в установі	Аудитор ознайомився з політикою інформаційної безпеки та політикою управління доступом і визначив вимоги до перегляду прав доступу (ким, кому, на якій основі, тощо).	Політики та процедури вивчені. Відповідні процеси проаналізовані перед тестуванням.
Особи або групи, відповідальні за перегляд прав доступу	Аудитор проаналізував організаційну структуру інформаційної безпеки та визначив послідовність кроків, необхідних для перегляду, затвердження та надання та зміни доступу користувачів.	Відповідальні за перегляд прав доступу визначені, інтерв'ю проведені
Окремі особи або групи, відповідальні за адміністрування та зміну прав доступу користувачів	Аудитор визначив, ким є особи або групи, відповідальні за перегляд та зміну прав доступу користувачів.	Відповідальні за адміністрування та зміну прав доступу визначені, інтерв'ю проведені
Як подаються, затверджуються, та документуються запити на зміну прав доступу користувачів	Аудитор визначив співробітників, відповідальним за модифікацію прав доступу користувачів і встановив, що права таких співробітники не порушують принципу розподілу обов'язків.	Проаналізовано запит на зміну доступів, якщо такий був, як результат перегляду прав доступу.

Зона ризиків IT: Захист доступу

УПРАВЛІННЯ ДОСТУПОМ: ПЕРЕГЛЯД ПРАВ ДОСТУПУ КОРИСТУВАЧІВ

АУДИТОРСЬКІ ПРОЦЕДУРИ - ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Отримайте звіти з перегляду прав доступу для всіх користувачів організації та переконайтеся, що: Перевірка доступу проводиться власниками активів з періодичністю на основі властивого ризику активу/системи/даних, щоб гарантувати, що доступ залишається відповідним на основі посадових обов'язків. Протестуйте наступні атрибути: • Перегляд доступу користувачів включав повну та точну популяцію користувачів; • Перегляд було належним чином задокументовано та виконано з відповідним рівнем деталізації, щоб переконатися, що доступ відповідав поточним посадовим обов'язкам кожного користувача на момент перегляду прав; • Перегляд проводився відповідним персоналом із належним розподілом обов'язків; • Доступ до системи було своєчасно належним чином змінено для користувачів, позначених як «винятки» під час перевірки	Визначена цільова популяція Визначена вибірка Дотримано всіх відповідних критеріїв тестування при тестуванні окремих елементів вибірки Надано висновок по відповідності (ефективності) контролю; визначенні відхилення та причини.	Цільова популяція (звіти про перегляд прав користувачів) Вибірка (зазвичай, незастосовна) Атрибути тестування

Номер	Період покриття	Назва Документу	Повна Популяція Користувачів	Відповідальні за перевірку	Рівень деталізації звіту	Модифікація доступів	Розподіл обов'язків перевіряючих	Відхилення	Comments
1	01.01.2022-06.01.2022	Звіт: Піврічний Перегляд Прав Користувачів	Так: виконано реконсиляцію користувачів та перевірку повноти даних	Департамент ІБ Відповідні департаменти	Обліковий запис\співробітник	Не застосовно	Дотримано	No	
2	01.01.2022-06.01.2022	Звіт: Піврічний Перегляд Прав Користувачів	Так: виконано реконсиляцію користувачів та перевірку повноти даних	Департамент ІБ Відповідні департаменти	Обліковий запис\співробітник	Не застосовно	Дотримано	No	

Зона ризиків IT: Захист доступу

Реєстрація користувача: привілейовані права

Політика управління доступом

ВІДПОВІДНИЙ КОНТРОЛЬ:

Доступ привілейованого рівня (наприклад, адміністратори) авторизований і відповідним чином обмежений.

Зона ризиків IT: Захист доступу

РЕЄСТРАЦІЯ КОРИСТУВАЧА: ПРИВІЛЕЙОВАНІ ПРАВА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Визначте засоби контролю, пов’язані з доступом привілейованого рівня. Зокрема, розгляньте можливість отримати розуміння наступних атрибутів процесу надання привілейованих прав користувачів:	Дивіться нижче	Дивіться нижче
Політики, пов'язані з інформаційною безпекою та захистом привілейованого рівня доступу.	Аудитор отримав і ознайомився з політикою інформаційної безпеки та політикою управління доступом і визначив вимоги до надання привілейованого доступу (ким, кому, на якій основі, тощо).	Політики та процедури вивчені: адміністрування привілейованого доступу
Організаційна структура функції управління безпекою.	Аудитор проаналізував організаційну структуру інформаційної безпеки та визначив послідовність кроків, необхідних для перегляду, затвердження та надання привілейованого доступу.	Політики та процедури вивчені: структура функції управління безпекою
Опис профілів користувачів, яким призначено привілейований рівень доступу.	Аудитор проаналізував описи профілів користувачів, яким призначено привілейований доступ, і зазначив, що такі профілі відповідають обов’язкам, покладеним на власників профілів.	Опис привілейованих користувачів проаналізовано.
Особи, які мають право використовувати привілейований рівень доступу.	На підставі перевірки вищезазначених документів аудитор визначив працівників, які мають право користуватися привілейованим доступом до IT-систем організації.	Опис привілейованих користувачів проаналізовано.

Зона ризиків IT: Захист доступу

РЕЄСТРАЦІЯ КОРИСТУВАЧА: ПРИВІЛЕЙОВАНІ ПРАВА

АУДИТОРСЬКІ ПРОЦЕДУРИ – ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Визначте, що особи, яким призначено привілейований доступ, не мають суперечливих привілеїв, які призводять до конфлікту розподілу обов'язків (тобто, привілеї адміністратора не надано бізнес-користувачам).	Аудитор проаналізував та визначив, що працівники, яким надано привілейований доступ, не виконують функцій, що призводить до порушення розподілу обов'язків.	Документ\Матриця розподілу обов'язків вивчена та проаналізована в розрізі процесу надання привілейованих доступів
Профілі зовнішніх користувачів, наприклад профілі третіх сторін, консультантів або профілі «екстрених» користувачів із привілейованим рівнем доступу.	Аудитор проаналізував профілі зовнішніх сторін (третіх осіб), а також профілі «екстрених користувачів» та інших типів користувачів, яким можуть бути надані тимчасові підвищені привілейовані права, і перевірив такі профілі користувачів (і облікові записи) на відповідність.	Опис профілів «екстрених користувачів», привілейований доступ третіх сторін.

Зона ризиків ІТ: Захист доступу

РЕЄСТРАЦІЯ КОРИСТУВАЧА: ПРИВІЛЕЙОВАНІ ПРАВА

АУДИТОРСЬКІ ПРОЦЕДУРИ - ПРИКЛАД

Опис процедури – дії аудитора	Очікуваний результат	Елементи Тестування
Отримайте повну та точну сукупність привілейованих користувачів для кожної системи та перевірте ці облікові записи на відповідність таким атрибутам: • Права доступу відповідно авторизовані та відповідають призначеним користувачам обов'язкам на основі запитів до менеджменту (A); • Права доступу авторизовані та відповідають призначеним користувачам обов'язкам на основі перевірки їх посадових обов'язків (B); • Загальні облікові записи привілейованого рівня використовуються на основі бізнес потреб, і доступ до таких облікових записів належним чином обмежується та контролюється (C);	Визначена цільова популяція (аміністратори) Визначена вибірка Дотримано всіх відповідних критеріїв тестування при тестувані окремих елементів вибірки Надано висновок по відповідності (ефективності контролю; визначенні відхилення та причини)	Цільова популяція Вибірка Атрибути тестування

								Атрибути					
Номер	USER_ID	User Name	Посада	Ім'я привілейованого користувача	Організаційний підрозділ	Обліковий запис користувача затверджений	Статус	A	B	C	Створено в системі	Термін придатності	Відхилення?
1	1000	YPASH	Системний Адміністратор	Євген Пащенко	Департамент ІТ	Петро Петренко, Директор Департаменту ІТ, Іван Іванченко, Директор Департаменту ІБ	Активний	Так	Так	NA	01.01.2020	01.01.2028	No

USAID
FROM THE AMERICAN PEOPLE

ДОМЕН II:
Безпека людських ресурсів

Зона ризиків ІТ: Договірні невизначеності

Формалізований документ: Положення про найм працівників

ТЕРМІНИ ТА УМОВИ НАЙМУ

ПОЛОЖЕННЯ ПРО НАЙМ ПРАЦІВНИКІВ – це офіційний внутрішній документ установи, який регулює процес найму працівників, визначає права та обов'язки роботодавця та працівників, а також встановлює загальні правила, яких слід дотримуватись під час працевлаштування.

Ціль процесу:
Забезпечити високий рівень інформаційної безпеки в організації через встановлення чітких вимог і процедур для працівників, які мають доступ до інформаційних систем та конфіденційної інформації.

Вимоги:
Чітка відповідність нормам трудового законодавства на всіх етапах відбору, обов'язкова перевірка кваліфікації кандидатів, а також забезпечення прозорості та об'єктивності у прийнятті рішень.

ОПИС РИЗИКУ:

Можливість непрозорого відбору кандидатів, що може призвести до недовіри серед працівників і порушень трудових відносин, ризик юридичних санкцій і штрафів у разі порушення трудового законодавства, а також втрати репутації установи через недобросовісність у процесі найму.

Зона ризиків IT: Договірні невизначеності

ТЕРМІНИ ТА УМОВИ НАЙМУ

Положення про найм працівників повинні погоджуватися з політикою безпеки організації, роз'яснювати та встановлювати:

- що весь найманий персонал, яким наданий доступ до чутливої інформації, повинен підписати угоду щодо конфіденційності/нерозголошення інформації;
- правову відповідальність сторін та права найманого персоналу, наприклад, стосовно законів про авторське право або законодавства про захист даних;
- відповідальності за управління активами установи, пов'язаними з інформаційними системами та послугами;
- відповідальності установи щодо поводження з персональною інформацією, в тому числі персональною інформацією, створеною в результаті або в ході найму в цю організацію;
- відповідальності поза межами службових приміщень установи та поза межами звичайного робочого часу, наприклад, у випадку роботи віддалено;
- дії, яких треба вжити, якщо найманий персонал нехтує вимогами безпеки організації.

Зона ризиків IT: Договірні невизначеності

ТЕРМІНИ ТА УМОВИ НАЙМУ

Положення про найм працівників

ВІДПОВІДНИЙ КОНТРОЛЬ:

Як частину своїх зобов'язань найманий персонал повинен погодити і підписати терміни та умови свого договору з найму, який повинен встановити взаємні відповідальності щодо інформаційної безпеки.

Зона ризиків IT: Договірні невизначеності

ТЕРМІНИ ТА УМОВИ НАЙМУ

Операційна ефективність контролів: атрибути перевірки

Опис процедури	Відповідь	Коментарі
Створити вибірку працівників і перевірити їхні трудові договори на відповідність політикам та процедурам установи.		
Перевірити, чи всі трудові договори відповідають вимогам трудового законодавства.		
Переглянути процес рекрутингу для працівників, включаючи оголошення про вакансії, інтерв'ю, перевірки рекомендацій, перевірки попередніх місць роботи і т.д. Переконатися, що всі етапи рекрутингу задокументовані і відповідають встановленим політикам.		
Оцінити процес відбору кандидатів, включаючи використання тестів, інтерв'ю та інших методів оцінки. Переконатися, що всі кандидати оцінюються об'єктивно і на основі встановлених критеріїв.		
Переглянути адаптаційні програми для нових працівників, щоб переконатися, що вони містять необхідну інформацію про установу, її політики, процедури та інше. Перевірте, чи підписують нові працівники документи про ознайомлення з політиками та процедурами установи.		
Оцінити наявність механізмів для збору зворотного зв'язку від нових працівників щодо процесу найму та адаптації. Перевірити, чи установа використовує цей зворотний зв'язок для покращення своїх процесів.		

Зона ризиків IT: Недостатній рівень знань і практик

Формалізований документ: Політика інформаційної безпеки

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

включають усвідомлення працівниками загроз інформаційній безпеці, навички захисту конфіденційної інформації, уміння виявляти та відвертати кібератаки, а також дотримання внутрішніх політик і процедур щодо інформаційної безпеки.

Ціль процесу:

Забезпечення того, щоб працівники були належно підготовлені та усвідомлювали загрози та ризики інформаційної безпеки, вміли ефективно захищати конфіденційну інформацію та діяли відповідно до встановлених стандартів і політик безпеки організації.

Вимоги:

Обов'язкова участь всіх працівників у навчанні, освітлення потенційних загроз, ознайомлення з внутрішніми політиками безпеки, перевірку знань та постійне оновлення навчальних матеріалів.

ОПИС РИЗИКУ:

Можливість витоку конфіденційної інформації через недбале ставлення до захисту даних, зростання кібератак внаслідок несвідомих дій персоналу, що може призвести до фінансових збитків, пошкодження репутації установи, а також можливість юридичних наслідків в результаті порушення вимог законодавства про захист персональних даних.

Зона ризиків IT: Недостатній рівень знань і практик

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Обов'язковість участі	• Всі працівники повинні брати участь у навчальних заходах з інформаційної безпеки, включаючи вступне навчання для нових співробітників та періодичні оновлення для існуючих працівників.
Висвітлення загроз	• Навчання повинно включати ознайомлення з потенційними загрозами інформаційної безпеки, такими як фішинг, віруси, соціальна інженерія тощо.
Правила внутрішнього користування	• Залучення до ознайомлення з внутрішніми політиками та процедурами інформаційної безпеки, включаючи вимоги до паролів, використання захисних програм тощо.
Тестування знань та Постійне оновлення	• Проведення тестів або інших форм оцінки знань після завершення навчання для перевірки розуміння та засвоєння матеріалу. • Забезпечення оновлення навчальних матеріалів та програм з урахуванням нових загроз і технологічних змін.
Підтримка та консультації	• Надання працівникам можливості звертатися за допомогою і консультаціями щодо питань інформаційної безпеки.

Зона ризиків IT: Недостатній рівень знань і практик

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчання повинно розпочинатися з офіційної процедури, яка передбачає ознайомлення з політикою безпеки організації та очікуваними вимогами перед наданням доступу до інформації або послуг.

Продовження навчання повинно охоплювати вимоги безпеки, правові відповідальності та контролі, а також навчання коректному використанню засобів оброблення інформації, наприклад, процедурі реєстрації, використанню пакетів програмного забезпечення та інформації щодо дисциплінарного процесу.

Навчання з інформаційної безпеки повинні бути суттєвими і відповідати ролі, відповідальності та навичкам особи, та охоплювати інформацію щодо відомих загроз, належних каналів звітування щодо інцидентів інформаційної безпеки і того, з ким контактувати для отримання подальших інструкцій/рекомендацій з безпеки.

Навчання з інформаційної безпеки призначене для того, щоб надати можливість працівникам усвідомити проблеми та інциденти інформаційної безпеки і реагувати згідно з існуючих інструкцій.

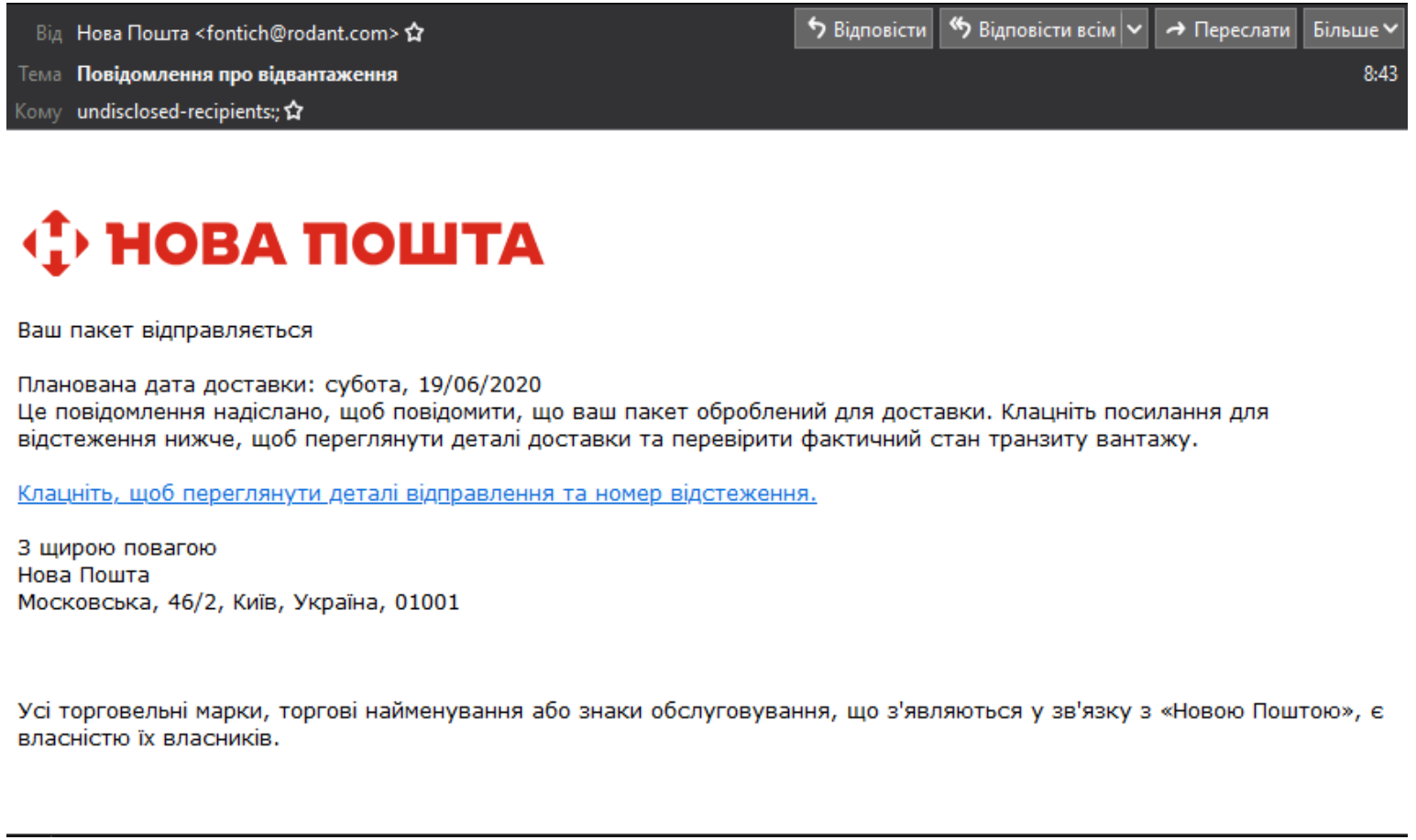
Зона ризиків IT: Недостатній рівень знань і практик

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Хорошою практикою являється проведення тестування службою інформаційної безпеки установи.

Через певний період після проведення навчання працівників служба інформаційної безпеки власноруч формує фішингові листи та розсилає всім співробітникам установи.

Далі збирається аналітика по працівниках, які не пройшли дане тестування (не змогли розпізнали фішинговий лист і перейшли по посиланню) і приймається рішення про організацію для них додаткового навчання.



Зона ризиків IT: Недостатній рівень знань і практик

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Політика інформаційної безпеки

ВІДПОВІДНИЙ КОНТРОЛЬ:

Увесь найманий персонал організації, там де це суттєво, повинен одержати належне навчання для поінформованості та регулярно отримувати оновлені дані щодо політик і процедур організації, суттєвих для їх посадових функцій.

Зона ризиків IT: Недостатній рівень знань і практик

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Операційна ефективність контролів: атрибути перевірки

Опис процедури	Відповідь	Коментарі
Переглянути документи, що описують програми навчання з інформаційної безпеки, включаючи навчальні матеріали, презентації та інструкції. Переконатися, що програми охоплюють основні теми з інформаційної безпеки, такі як виявлення фішингових атак, використання сильних паролів, управління доступом та реагування на інциденти.		
Перевірити частоту проведення тренінгів з інформаційної безпеки для співробітників. Оцінити, чи проводяться регулярні оновлення навчання, особливо при зміні політик або при виникненні нових загроз (внутрішніх і зовнішніх).		
Перевірити записи відвідуваності тренінгів, щоб переконатися, що всі співробітники, особливо ті, хто мають доступ до конфіденційної інформації, пройшли необхідне навчання. Оцінити наявність механізмів для повторного навчання працівників, які не пройшли тренінг у встановлений час.		
Переглянути результати тестувань або опитувань, що проводяться після навчання для оцінки рівня знань співробітників. Перевірити, чи проводяться додаткові тренінги для тих співробітників, які не пройшли тестування або показали низькі результати.		
Провести аналіз реальних випадків інцидентів з інформаційної безпеки, щоб оцінити, наскільки ефективно співробітники застосовували знання та навички, отримані під час навчання. Оцінити швидкість і правильність дій працівників під час виникненні інцидентів.		

Зона ризиків IT: Недостатній рівень знань і практик

ПОІНФОРМОВАНІСТЬ, ОСВІТА І НАВЧАННЯ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Операційна ефективність контролів: атрибути перевірки

Опис процедури	Відповідь	Коментарі
Переглянути заходи, спрямовані на підвищення поінформованості співробітників про інформаційну безпеку, такі як інформаційні бюлетені, плакати, внутрішні комунікації тощо. Оцінити, наскільки регулярно ці заходи проводяться і чи враховують вони поточні загрози та кращі практики.		
Провести інтерв'ю з випадковою вибіркою співробітників, щоб оцінити їхню обізнаність про політики інформаційної безпеки, процедури та методи захисту. Перевірити, чи можуть співробітники правильно реагувати на гіпотетичні сценарії загроз.		
Переглянути механізми збору зворотного зв'язку від співробітників щодо програм навчання з інформаційної безпеки. Оцінити, як організація використовує цей зворотний зв'язок для покращення програм навчання.		

Зона ризиків ІТ: Недостатнє або неефективне реагування на порушення

Формалізований документ: Положення про дисциплінарну відповідальність

ДИСЦИПЛІНАРНИЙ ПРОЦЕС

ПОЛОЖЕННЯ ПРО ДИСЦИПЛІНАРНУ ВІДПОВІДАЛЬНІСТЬ - це формалізований документ, який встановлює правила і процедури стосовно ведення дисциплінарних справ з працівниками, включаючи порушення внутрішніх правил підприємства, процедур безпеки, недисциплінована поведінку або інші порушення, які можуть призвести до застосування дисциплінарних санкцій, таких як попередження, штрафи, тимчасове призупинення або звільнення з роботи.

Ціль процесу:
Забезпечення дисциплінованості та порядку на робочому місці шляхом встановлення чітких правил і процедур щодо регулювання поведінки працівників, відповідального виконання трудових обов'язків та уникнення порушень внутрішніх правил підприємства.

Вимоги:
Чіткість правил поведінки, справедливість розгляду порушень, дотримання законодавства та систематичне оновлення політики.

ОПИС РИЗИКУ:

Можливість конфліктів на робочому місці, зниження морального духу серед працівників, збільшення числа судових позовів через неправомірність застосованих санкцій, а також втрату довіри і репутації установи від громадськості.

Зона ризиків ІТ: Недостатнє або неефективне реагування на порушення

ДИСЦИПЛІНАРНИЙ ПРОЦЕС

Чіткість і доступність правил	•Чітке визначення внутрішніх правил і стандартів поведінки на робочому місці
Прозорість процедур	•Визначені процедури і порядок реагування на порушення, включаючи інформування працівників про можливі наслідки.
Законність та справедливість	•Забезпечення дотримання законодавства при застосуванні дисциплінарних санкцій і забезпечення справедливого розгляду кожної справи
Постійний моніторинг і оновлення	•Постійне оновлення політики та процедур у відповідності зі змінами в законодавстві та внутрішніх потребах організації.
Освіта і навчання	•Проведення навчання та інформування працівників про внутрішні правила і очікування організації щодо дисципліни на роботі.

Зона ризиків IT:
Недостатнє або неефективне реагування на порушення

ДИСЦИПЛІНАРНИЙ ПРОЦЕС

- Дисциплінарний процес не повинен розпочинатися без попередньої верифікації того, що порушення безпеки сталося.

- Офіційно оформлений дисциплінарний процес повинен забезпечувати коректний та справедливий розгляд справи найманого персоналу, якого підозрюють у вчиненні порушень безпеки. Повинен існувати офіційно оформлений процес для диференційованого реагування, яке бере до уваги такі фактори: відповідне законодавство, сутність та тяжкість порушення і його вплив на діяльність установи, чи є це перше або повторне правопорушення, проходив чи ні порушник належне навчання, та інші фактори. У серйозних випадках неналежного поводження процес повинен передбачати невідкладне позбавлення обов'язків, прав доступу та повноважень і негайне випроваджування, за необхідності, з місцеперебування.

- Дисциплінарний процес повинен також використовуватися як фактор утримування від порушень політики та процедур безпеки, а також будь-яких інших порушень безпеки найманим персоналом.

Зона ризиків IT:
Недостатнє або неефективне реагування на порушення

ДИСЦИПЛІНАРНИЙ ПРОЦЕС

Положення про дисциплінарну відповідальність

ВІДПОВІДНИЙ КОНТРОЛЬ:

Повинен існувати офіційно оформлений дисциплінарний процес щодо найманого персоналу, який здійснив порушення безпеки.

Зона ризиків IT:
Недостатнє або неефективне реагування на порушення

ДИСЦИПЛІНАРНИЙ ПРОЦЕС

Операційна ефективність контролів: атрибути перевірки

Опис процедури	Відповідь	Коментарі
Перегляньте документацію, що описує дисциплінарні політики та процедури, щоб переконатися, що вони чітко визначені та доступні для всіх співробітників. Перевірте відповідність політик законодавчим вимогам та внутрішнім стандартам організації.		
Виберіть випадкову вибірку випадків дисциплінарних заходів і перевірте, чи були дотримані встановлені процедури. Перевірте, чи всі етапи процесу були документовані, включаючи розслідування, повідомлення працівника, інтерв'ю та прийняття рішень.		
Оцініть вибірку дисциплінарних справ, щоб перевірити, чи були прийняті заходи справедливими та пропорційними порушенням.		
Перевірте, чи були дисциплінарні заходи застосовані в розумні строки після виявлення порушення. Оцініть, чи відповідають часові рамки розгляду випадків встановленим політикам.		
Оцініть, чи всі співробітники були належним чином повідомлені про порушення та мали можливість висловитися.		
Перевірити, чи рішення приймаються на основі об'єктивних доказів і чи санкції пропорційні до порушень.		
Перевірити процес моніторингу поведінки співробітників після завершення дисциплінарного процесу.		

Зона ризиків IT:
Невчасне чи неповне скасування доступу до систем та ресурсів

Формалізований документ:
Угода про припинення відповідальностей

ПРИПИНЕННЯ ВІДПОВІДАЛЬНОСТЕЙ

УГОДА ПРО ПРИПИНЕННЯ ВІДПОВІДАЛЬНОСТЕЙ - визначає умови та процедури завершення обов'язків або зобов'язань сторін, що були закріплені у договорі чи угоді. Цей документ важливий для формалізації моменту, коли зобов'язання однієї або обох сторін припиняються і може використовуватись у різних правових та договірних контекстах.

Ціль процесу:

Юридичне чи офіційне завершення відповідальності сторін за певними зобов'язаннями, умовами або діями, що можуть бути закріплені в договорі, угоді або іншому правовому документі.

Вимоги:

Чітко визначені умови, відповідність законодавству, письмове оформлення, інформування сторін, взаємну згоду, юридичний супровід та виконання всіх зобов'язань до моменту припинення. Ці вимоги забезпечують законність і справедливість процесу, а також захист інтересів усіх залучених сторін.

ОПИС РИЗИКУ:

Можливість неправильного інтерпретування умов угоди або законодавчих норм, що може призвести до спорів і судових процесів, втрати фінансових або інших ресурсів при невдалому завершенні угоди, а також негативний вплив на репутацію сторін в результаті недосягнення взаємовигідного компромісу.

Зона ризиків IT:
Невчасне чи неповне скасування доступу до систем та ресурсів

ПРИПИНЕННЯ ВІДПОВІДАЛЬНОСТЕЙ

Угода про припинення відповідальностей повинна містити:

Чітко визначені умови	• Умови припинення повинні бути чітко визначені в договорі або угоді.
Відповідність законодавству	• Процес повинен повністю відповідати чинному законодавству і нормативним актам.
Письмове оформлення	• Усі дії щодо припинення відповідальностей повинні бути документально оформлені.
Інформування сторін	• Усі зацікавлені сторони повинні бути належним чином поінформовані про припинення відповідальностей.
Взаємну згоду	• Припинення відповідальностей, якщо це передбачено угодою, повинно відбуватися за взаємною згодою всіх сторін.
Юридичний супровід	• Залучення юридичних експертів для забезпечення правильності і законності процесу.
Погашення зобов'язань	• Забезпечення виконання всіх зобов'язань, які мають бути виконані до моменту припинення відповідальностей.

Зона ризиків IT:
Невчасне чи неповне скасування доступу до систем та ресурсів

ПРИПИНЕННЯ ВІДПОВІДАЛЬНОСТЕЙ

Угода про припинення відповідальностей

ВІДПОВІДНИЙ КОНТРОЛЬ:

Повинні бути чітко визначені та встановлені відповідальності за виконання процедур припинення найму або зміни умов найму.

Зона ризиків IT:
Невчасне чи неповне скасування доступу до систем та ресурсів

ПРИПИНЕННЯ ВІДПОВІДАЛЬНОСТЕЙ

Операційна ефективність контролів: атрибути перевірки

Опис процедури	Відповідь	Коментарі
Перевірити, чи припинення відповідальностей відбувається відповідно до встановлених політик та процедур.		
Оцінити, чи співробітники були належним чином повідомлені про припинення їхніх відповідальностей.		
Перевірити, чи рішення про припинення відповідальностей базуються на чітких і об’єктивних підставах.		
Перевірити, чи проводяться вихідні інтерв'ю з метою отримання зворотного зв’язку від співробітників, які припиняють відповідальності.		
Оцінити ефективність процесу передачі відповідальностей іншим співробітникам.		
Перевірити, чи дотримано конфіденційність під час процесу припинення відповідальностей.		
Перевірити, чи процес припинення відповідальностей відповідає законодавчим вимогам.		

Зона ризиків IT: Несвоєчасне або некоректне відкликання доступу

ВИЛУЧЕННЯ ПРАВ ДОСТУПУ

Формалізований документ: Політика інформаційної безпеки

ВИЛУЧЕННЯ ПРАВ ДОСТУПУ - це частина політики інформаційної безпеки, яка визначає умови та процедури відкликання або припинення доступу працівників чи інших осіб до інформаційних систем, даних та ресурсів організації.

Ціль процесу:
Ціль процесу вилучення прав доступу полягає в забезпеченні захисту інформаційних систем і даних організації шляхом своєчасного та коректного припинення доступу до них працівників або інших осіб, які більше не мають права доступу.

Вимоги:
Чітко визначені умови, оперативність, документування дій, інформування відповідних осіб, регулярний контроль, захист даних і відповідність законодавчим вимогам.

ОПИС РИЗИКУ:

Можливість несанкціонованого доступу до конфіденційної інформації у випадку несвоєчасного вилучення доступу, втрату або витік даних, а також потенційні юридичні наслідки та збитки для репутації організації через порушення політики безпеки.

Зона ризиків IT: Несвоєчасне або некоректне відкликання доступу

ВИЛУЧЕННЯ ПРАВ ДОСТУПУ

Процес вилучення прав доступу повинен містити

Чітко визначені умови	• Умови вилучення прав доступу повинні бути чітко визначені в політиках безпеки організації
Оперативність	• Процес вилучення доступу повинен бути оперативним, особливо у випадках звільнення або інших термінових ситуацій
Документування	• Усі дії щодо вилучення прав доступу повинні бути документально оформлені.
Інформування	• Відповідні особи та підрозділи повинні бути належним чином поінформовані про вилучення доступу
Перевірку та контроль	• Регулярні перевірки та контроль процесу вилучення доступу для забезпечення його ефективності.
Захист даних	• Забезпечення збереження та захисту даних при вилученні доступу.
Юридичну відповідність	• Процес повинен відповідати всім відповідним законодавчим та нормативним вимогам

Зона ризиків IT: Несвоєчасне або некоректне відкликання доступу

ВИЛУЧЕННЯ ПРАВ ДОСТУПУ

Політика інформаційної безпеки

ВІДПОВІДНИЙ КОНТРОЛЬ:

Після припинення найму, контракту чи угоди будь-якого найманого персоналу права їх доступу до інформації та засобів оброблення інформації повинні бути вилучені.

Зона ризиків IT: Несвоєчасне або некоректне відкликання доступу

ВИЛУЧЕННЯ ПРАВ ДОСТУПУ

Операційна ефективність контролів: атрибути перевірки

Опис процедури	Відповідь	Коментарі
Перевірити, чи своєчасно виявляється потреба у вилученні прав доступу.		
Перевірити, чи були відповідні співробітники належним чином повідомлені про вилучення їх прав доступу.		
Перевірити, чи процес вилучення прав доступу відбувається відповідно до встановлених процедур.		
Перевірити, чи рішення про вилучення прав доступу базуються на чітких і об'єктивних підставах.		
Перевірити, чи вилучення прав доступу відбувається своєчасно.		
Перевірити, чи здійснюється періодичний моніторинг прав доступу		
Перевірити чи в усіх випадках було забезпечено збереження та захист даних при вилученні доступу		
Перевірити, чи процес вилучення прав доступу відповідає законодавчим вимогам		

ОПИТУВАННЯ

1. Які дії повинні бути вжиті, якщо співробітник порушив правила безпеки?
a) Проведення дисциплінарного розслідування;
b) Надання зауваження;
c) Одразу звільнити співробітника;

2. Які заходи повинні бути прийняті для зниження ризиків після звільнення співробітника?
a) Надати звільненому співробітнику доступ до всіх систем ще на кілька днів, щоб завершити всі розпочаті завдання
b) Після звільнення співробітника потрібно просто повідомити про це колегам і продовжувати роботу без додаткових заходів
c) Відкликання доступу до ресурсів організації

3. Який процес є обов'язковим при зміні посадових обов'язків співробітника?
a) Організація зустрічі з керівництвом
b) Перегляд та оновлення доступів до інформаційних систем
c) Проведення нового тренінгу

4. Які заходи повинні бути прийняті для забезпечення безпеки перед доступом нових співробітників до систем?
a) Надати новим співробітникам доступ до всіх систем і даних
b) Проведення вступного інструктажу з безпеки
c) Оновити та перевірити політики безпеки, щоб забезпечити відповідність нових співробітників всім актуальним вимогам безпеки.

USAID
FROM THE AMERICAN PEOPLE

ДОМЕН III:
Фізична безпека та безпека інфраструктури

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ФІЗИЧНА БЕЗПЕКА ТА БЕЗПЕКА ІНФРАСТРУКТУРИ –
це заходи безпеки, спрямовані на унеможливлення несанкціонованого доступу до об'єктів, обладнання та ресурсів, а також на захист персоналу та майна від пошкоджень чи шкоди.

Цілі:

- Запобігти неавторизованому фізичному доступу, ушкодженню та вторгненню до службових приміщень організації та втручанню в її інформацію.
- Запобігти втратам, ушкодженню, крадіжці або компрометації активів та перериванню діяльності організації.

Засоби оброблення критичної або чутливої інформації повинні бути розміщені в зонах безпеки, захищених визначеними периметрами безпеки, з належними бар'єрами безпеки та контролями прибуття. Вони повинні бути фізично захищені від неавторизованого доступу, ушкодження та втручання.

Наданий захист повинен бути пропорційним ідентифікованим ризикам.

Обладнання повинне бути захищене від фізичних та екологічних загроз.

Для зменшення ризику неавторизованого доступу до інформації та для захисту від втрати та ушкодження обладнання повинне бути захищене (охоплюючи те, що використовується зовні, і те майно, що переміщується). При цьому треба також розглянути розміщення та вилучення обладнання. Для захисту від фізичних загроз і для охорони засобів життєзабезпечення, таких як електроживлення та кабельна інфраструктура, можуть бути потрібними спеціальні контролі.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ЗОНИ БЕЗПЕКИ

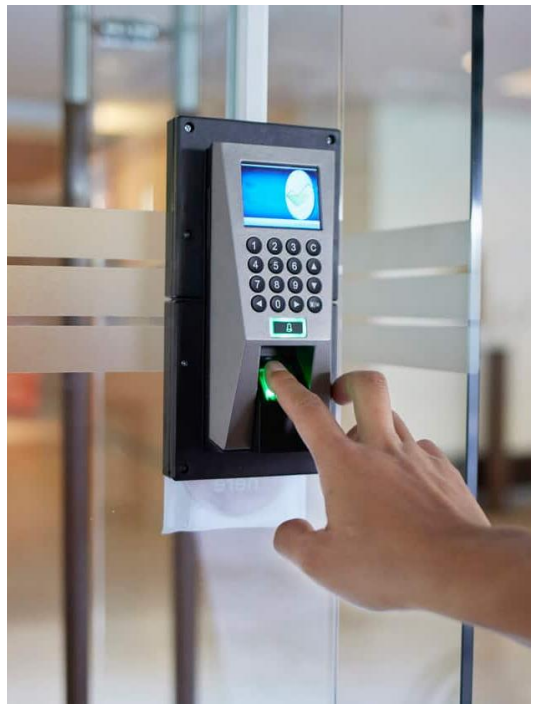
Мета: Визначити та контролювати доступ до різних зон безпеки, щоб мінімізувати ризик несанкціонованого доступу.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Визначення зон безпеки:** Визначення зон із різними рівнями безпеки залежно від критичності інформації або обладнання. Наприклад, дата-центри, серверні кімнати, кімнати зберігання архівів мають обмежений доступ.

- **Контроль доступу:**
  Встановлення механізмів контролю доступу, таких як замки, системи контролю доступу (карти, біометричні дані), відеоспостереження.
  - Замки
  - Системи контролю доступу
  - Біометричні дані
  - Відеоспостереження

- **Моніторинг і журналювання:**
  Ведення журналів доступу для контролю та аналізу подій.
  - Журнали відвідувачів
  - Аудит доступу



Зона ризиків IT: Фізична безпека та безпека інфраструктури

ПЕРИМЕТР ФІЗИЧНОЇ БЕЗПЕКИ

Мета: Забезпечити захист периметра будівлі або об'єкта, щоб запобігти несанкціонованому доступу.

ОСНОВНІ ПОЛОЖЕННЯ:

ОГОРОДЖЕННЯ:

Використання фізичних бар'єрів (огорожі, стіни) для запобігання доступу.

- Паркани
- Двері та ворота

СИСТЕМИ ВИЯВЛЕННЯ ПРОНИКНЕНЬ:

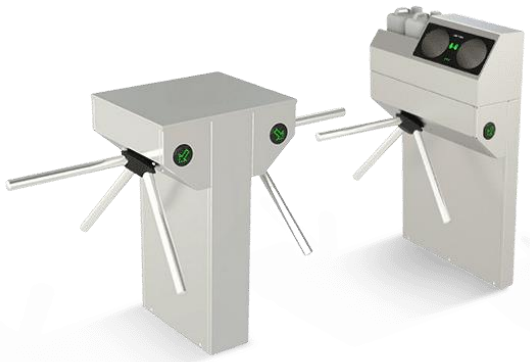
Використання датчиків руху, сигналізаційних систем.

- Датчики руху
- Сигналізація

КОНТРОЛЬ ВХОДУ ТА ВИХОДУ:

Використання охоронців, турнікетів, шлюзів.

- Охоронці
- Турнікети
- Шлюзи



Зона ризиків IT: Фізична безпека та безпека інфраструктури

ПЕРИМЕТР ФІЗИЧНОЇ БЕЗПЕКИ

Політика безпеки інфраструктури: периметр фізичної безпеки

ВІДПОВІДНИЙ КОНТРОЛЬ:

Для захисту зон, що містять інформацію чи засоби оброблення інформації, потрібно використовувати периметри безпеки (наприклад, бар'єри, стіни, картково-контрольовані вхідні брами або пости чергових).

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ПЕРИМЕТР ФІЗИЧНОЇ БЕЗПЕКИ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Перевірте наявність документів, що описують периметри безпеки, їх межі та вимоги до захищеності залежно від важливості зони безпеки.		
2. Огляньте конструкції зовнішніх стін, дверей, вікон приміщень, що містять засоби оброблення інформації. Перевірте їх на наявність проміжків або слабких місць.		
3. Оцініть фізичний стан засувів, замків, тривожної сигналізацію на дверях і вікнах. Оцініть їхню працездатність та ефективність у запобіганні несанкціонованому доступу.		
4. Перевірте наявність зон чергування або інших засобів контролю фізичного доступу до будівель та приміщень.		
5. Проаналізуйте процес надання доступу до приміщень. Оцініть, як здійснюється перевірка та авторизація персоналу.		
6. Перевірте наявність тривожної сигналізації на пожежних дверях та їх технічний стан (їх опірність та функціональність).		
7. Перевірте наявність систем виявлення порушників, включаючи покриття всіх зовнішніх дверей і доступних вікон.		
8. Переконайтеся, що засоби оброблення інформації організації розташовані в зонах, захищених від несанкціонованого доступу з боку третіх сторін.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ЗАХОДИ БЕЗПЕКИ ФІЗИЧНОГО ПРИБУТТЯ

Мета: Забезпечити процедури для перевірки та контролю осіб, що прибувають на об'єкт.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Реєстрація відвідувачів:**
  Ведення журналу відвідувачів з вказанням часу прибуття, мети візиту, особи, яка супроводжує.
  – Журнали реєстрації
- **Ідентифікація:**
  Використання посвідчень, бейджів для відвідувачів, щоб їх можна було легко ідентифікувати.
  – Бейджі для відвідувачів
- **Супровід відвідувачів:**
  Всі відвідувачі мають бути супроводжувані уповноваженими особами.
  – Супровід співробітниками

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ЗАХОДИ БЕЗПЕКИ ФІЗИЧНОГО ПРИБУТТЯ

Політика безпеки інфраструктури: безпека фізичного прибуття

ВІДПОВІДНИЙ КОНТРОЛЬ:

Зони безпеки повинні бути захищені належними контролями прибуття, щоб забезпечити доступ тільки авторизованому персоналу.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ЗАХОДИ БЕЗПЕКИ ФІЗИЧНОГО ПРИБУТТЯ

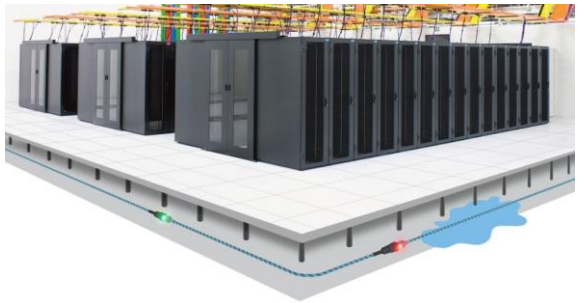
Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Огляньте журнали реєстрації або електронні системи, які мають фіксувати дату та час прибуття і відбуття відвідувачів.		
2. Огляньте та протестуйте системи контролю доступу (картки, ПІН-коди) до зон, де зберігається або обробляється чутлива інформація.		
3. Огляньте процес видачі та носіння видимої ідентифікації для відвідувачів, власного персоналу, та зовнішніх постачальників.		
4. Проведіть тестування реакції персоналу на відвідувачів без супроводу та осіб без видимої ідентифікації.		
5. Огляньте записи про моніторинг доступу стороннього персоналу до чутливої інформації, зокрема чи був їхній доступ обмежений лише до необхідних зон і чи був під постійним наглядом.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

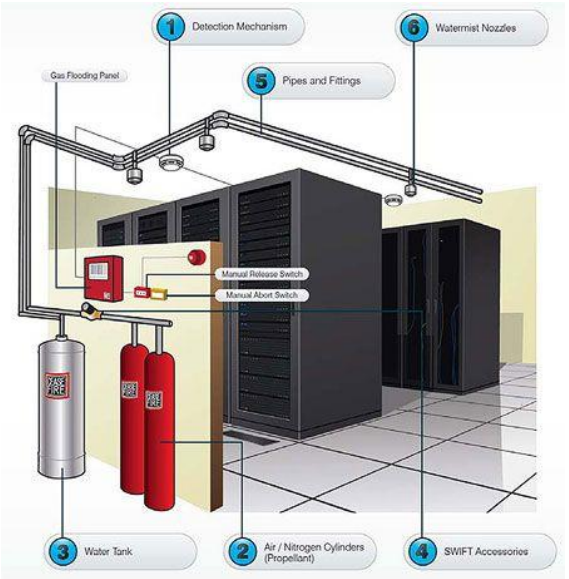
ЗАХИСТ ВІД ЗОВНІШНІХ ТА ІНФРАСТРУКТУРНИХ ЗАГРОЗ

Мета: Забезпечити заходи для захисту від зовнішніх загроз, таких як природні катастрофи, та загроз інфраструктурі.



ОСНОВНІ ПОЛОЖЕННЯ:

- **Оцінка ризиків:**
  Ідентифікація та оцінка потенційних зовнішніх загроз (повені, пожежі).
  - Аналіз ризиків
  - Карта ризиків
- **Заходи зниження ризиків:**
  Встановлення систем пожежогасіння, водовідвідних систем.
  - Системи пожежогасіння
  - Водовідвідні системи
- **Планування безперервності бізнесу:**
  Розробка планів дій у випадку виникнення надзвичайних ситуацій.
  - Резервне копіювання даних
  - Плани евакуації



Зона ризиків IT: Фізична безпека та безпека інфраструктури

ЗАХИСТ ВІД ЗОВНІШНІХ ТА ІНФРАСТРУКТУРНИХ ЗАГРОЗ

Політика безпеки інфраструктури: захист від зовнішніх та інфраструктурних загроз

ВІДПОВІДНИЙ КОНТРОЛЬ:

Повинен бути розроблений та застосований фізичний захист від пошкодження внаслідок пожежі, повені, землетрусу, вибуху, акцій громадської непокори та інших форм стихійного або спричиненого людьми лиха.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ЗАХИСТ ВІД ЗОВНІШНІХ ТА ІНФРАСТРУКТУРНИХ ЗАГРОЗ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Огляньте приміщення, які знаходяться поруч із зоною безпеки, щоб ідентифікувати можливі загрози, такі як ризик пожежі, протікання води або можливість вибуху.		
2. Перевірте, де зберігаються займисті або небезпечні матеріали відносно зони безпеки.		
3. Перевірте наявність і розміщення протипожежного обладнання в зоні безпеки. Оцініть його справність та відповідність вимогам пожежної безпеки.		
4. Оцініть розміщення обладнання для відновлення та носіїв резервних копій, зокрема чи знаходяться вони на безпечній відстані від основного приміщення, яке може бути піддане ризику лиха.		
5. Перевірте наявність плану відновлення після лиха, який включає сценарії пожежі, повені, землетрусу, вибуху або інших стихійних чи спричинених людьми лих.		
6. Перевірте, як часто проводяться інспекції щодо стану будівлі, приміщень, протипожежного обладнання та розміщення небезпечних матеріалів.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

РОЗМІЩЕННЯ ТА ЗАХИСТ ОБЛАДНАННЯ

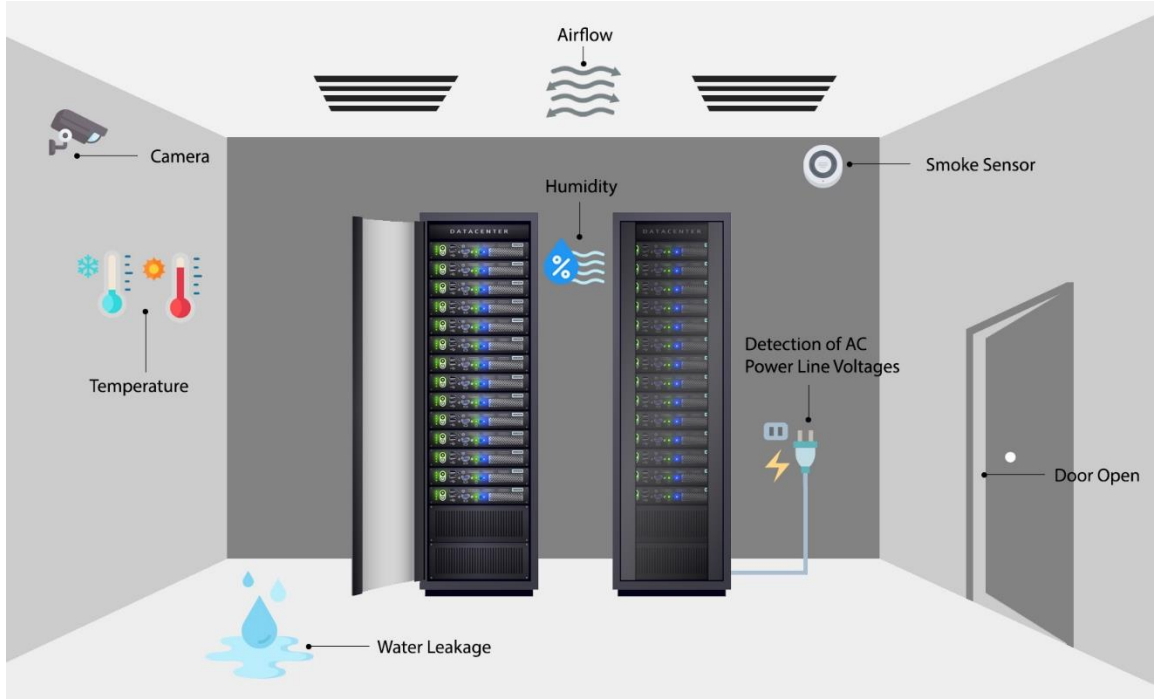
Мета: Забезпечити правильне розміщення обладнання та його захист від фізичних загроз.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Розміщення:**
  Установка обладнання в зонах з контрольованим доступом, уникнення розміщення поблизу вразливих місць (наприклад вікон, дверей).

- **Охолодження та вентиляція:**
  Забезпечення належної температури та вологості для запобігання перегріву.
  – Системи охолодження
  – Контроль вологості

- **Захист від фізичних пошкоджень:**
  Використання стійок, захисних корпусів, фіксація обладнання для запобігання падінню або пошкодженню.
  – Захисні корпуси
  – Фіксація обладнання



Зона ризиків IT: Фізична безпека та безпека інфраструктури

РОЗМІЩЕННЯ ТА ЗАХИСТ ОБЛАДНАННЯ

Політика безпеки інфраструктури: розміщення та захист обладнання

ВІДПОВІДНИЙ КОНТРОЛЬ:

Обладнання повинне бути розміщене чи захищене таким чином, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого неавторизованого доступу.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

РОЗМІЩЕННЯ ТА ЗАХИСТ ОБЛАДНАННЯ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Огляньте розташування обладнання в робочих зонах. Оцініть, чи розташоване обладнання таким чином, щоб мінімізувати непотрібний доступ до нього персоналу, який не має відповідних повноважень.		
2. Оцініть розміщення засобів оброблення інформації, особливо тих, які обробляють чутливі дані. Перевірте, чи є засоби оброблення інформації захищеними від несанкціонованого фізичного доступу.		
3. Оцініть впроваджені заходи безпеки, спрямовані на захист обладнання від фізичних загроз, таких як крадіжки, пожежі, вибухи, вода, пил, вібрації, електромагнітне випромінювання, вандалізм тощо.		
4. Перевірте, чи встановлено захист від блискавки на будівлях, та наявність фільтрів захисту від блискавки на вхідних лініях енергопостачання та комунікацій.		
5. Оцініть наявність та дотримання настанов щодо приймання їжі, напоїв та паління поблизу засобів оброблення інформації.		
6. Перевірте, чи здійснюється моніторинг умов довкілля, таких як температура та вологість у приміщеннях, де знаходиться обладнання оброблення інформації.		
7. Перевірте наявність заходів, спрямованих на захист обладнання, що обробляє чутливу інформацію, від витоку інформації через електромагнітне випромінювання.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕКА КАБЕЛЬНИХ МЕРЕЖ

Мета: Захист кабельних мереж від фізичних пошкоджень та несанкціонованого доступу.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Прокладання кабелів:**
  Використання спеціальних каналів, трубопроводів для прокладання кабелів.
  – Кабельні канали/трубопроводи

- **Маркування:**
  Чітке маркування кабелів для полегшення ідентифікації та технічного обслуговування.
  – Маркування кабелів

- **Захист від перехоплення:**
  Використання екранованих кабелів для захисту від електромагнітних перешкод та зменшення ризику несанкціонованого перехоплення.
  – Екрановані кабелі
  – Захисні покриття

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕКА КАБЕЛЬНИХ МЕРЕЖ

Політика безпеки інфраструктури: безпека кабельних мереж

ВІДПОВІДНИЙ КОНТРОЛЬ:

Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних послуг, повинні бути захищені від перехоплювання чи ушкоджень.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕКА КАБЕЛЬНИХ МЕРЕЖ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Оцініть, чи всі силові та телекомунікаційні лінії в засобах оброблення інформації заземлені або забезпечені альтернативним захистом.		
2. Перевірте наявність кабелепроводів для захисту кабельної мережі, та оцініть маршрутизацію кабелів, особливо уникання прокладання через загальнодоступні зони.		
3. Оцініть, чи забезпечено відокремлення силових кабелів від телекомунікаційних для запобігання взаємному впливу.		
4. Перевірте, чи кабелі та обладнання чітко ідентифіковані та промарковані для зменшення ризику неправильної комутації.		
5. Перевірте наявність задокументованого списку комутацій для мінімізації можливості помилок.		
6. Перевірте, чи використовуються оптоволоконні кабелі для підвищення безпеки передачі даних.		
7. Оцініть, чи застосовується електромагнітне екранування для захисту кабелів від перехоплення.		
8. Перевірте наявність технічних засобів та фізичних обстежень для виявлення неавторизованих пристроїв, приєднаних до кабелів.		
9. Перевірте, чи існують механізми контролю доступу до комутаційних панелей та кабельних приміщень.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ОБСЛУГОВУВАННЯ ОБЛАДНАННЯ

Мета: Забезпечити належне технічне обслуговування обладнання для забезпечення його надійної роботи.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Регулярне обслуговування:**
  Проведення регулярних перевірок і технічного обслуговування.
  – Графік обслуговування
  – Перевірки працездатності

- **Запасні частини:**
  Наявність запасних частин для оперативного ремонту та мінімізації простоїв.
  – Резерв запасних частин
  – Логістика запасних частин

- **Документація:**
  Ведення журналів обслуговування та технічних інструкцій.
  – Журнали обслуговування
  – Технічні інструкції

MACHINE MAINTENANCE SCHEDULE TEMPLATE

MACHINE NAME	CONDITION	LOCATION	ASSIGNED TO	LAST MAINTENANCE DATE	MAINTENANCE FREQUENCY in Days	NEXT MAINTENANCE DATE	NOTES
Machine 1	BAD	Floor B	Richard	01/21/2022	365	01/21/2023	The machine starts up slow and when pressing the buttons to navigate the machine it lags and the command will happen seconds later.
Machine 2	POOR	Floor A	Paul	01/09/2022	90	04/09/2022	
Machine 3	FAIR	Floor B	Terry	12/18/2021	60	02/16/2022	Will need a full shutdown next service cycle.
Machine 4	GOOD	Floor A	Allen	11/28/2021	30	12/28/2021	
Machine 5	GOOD	Floor C	Allen	10/05/2021	180	04/03/2022	

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ОБСЛУГОВУВАННЯ ОБЛАДНАННЯ

Політика безпеки інфраструктури: обслуговування обладнання

ВІДПОВІДНИЙ КОНТРОЛЬ:

Обладнання повинне обслуговуватися відповідно до вимог виробників, щоб забезпечити його постійну доступність та цілісність.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ОБСЛУГОВУВАННЯ ОБЛАДНАННЯ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Перевірте, чи проводиться обслуговування обладнання відповідно до рекомендованих специфікацій та періодів обслуговування, зазначених постачальником.		
2. Переконайтеся, що тільки авторизований обслуговуючий персонал здійснює ремонт та обслуговування обладнання.		
3. Оцініть, чи ведуться записи про всі очікувані або фактичні несправності обладнання, а також про всі запобіжні та коригувальні дії.		
4. Перевірте, чи передбачено відповідне планування обслуговування обладнання з належними контролями, зокрема щодо вивантаження чутливої інформації або інструктажу обслуговуючого персоналу.		
5. Оцініть, чи задовольняються всі вимоги, накладені страхуванням, стосовно обслуговування обладнання.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕКА ОБЛАДНАННЯ ПОЗА СЛУЖБОВИМИ ПРИМІЩЕННЯМИ

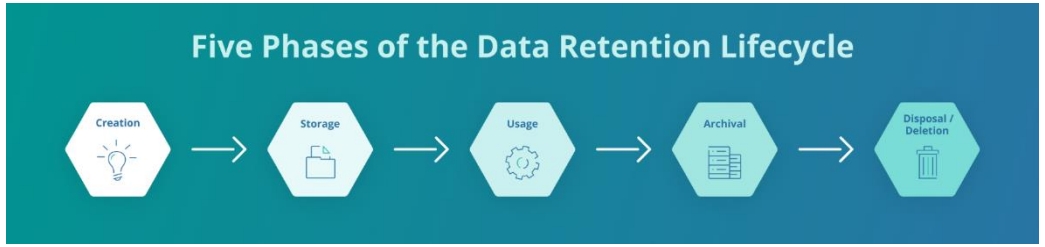
Мета: Забезпечити захист обладнання, яке використовується поза службовими приміщеннями.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Мобільне обладнання:**
  Використання захищених чохлів,
  шифрування даних на мобільних пристроях.
  – Захищені чохли
  – Шифрування даних

- **Втрата або крадіжка:**
  Впровадження механізмів відстеження
  та видалення даних на відстані.
  – Відстеження пристроїв
  – Віддалене видалення даних

- **Політика використання:**
  Розробка політик щодо використання мобільного
  обладнання.
  – Політики зберігання та транспортування
  – Навчання співробітників



Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕКА ОБЛАДНАННЯ ПОЗА СЛУЖБОВИМИ ПРИМІЩЕННЯМИ

Політика безпеки інфраструктури: безпека обладнання поза службовими приміщеннями

ВІДПОВІДНИЙ КОНТРОЛЬ:

До обладнання поза службовими приміщеннями повинен бути застосовний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕКА ОБЛАДНАННЯ ПОЗА СЛУЖБОВИМИ ПРИМІЩЕННЯМИ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Перевірте, чи отримано авторизацію керівництва на використання будь-якого обладнання оброблення інформації поза службовими приміщеннями організації.		
2. Оцініть, чи не залишаються обладнання та носії інформації без нагляду в загальнодоступних місцях, а також чи портативні комп'ютери переносяться як ручний багаж під час переїздів.		
3. Переконайтеся, що працівники дотримуються інструкцій виробника щодо захисту обладнання, наприклад, від впливу сильних електромагнітних полів.		
4. Перевірте, чи впроваджені необхідні контролі для захисту надомного обладнання, зокрема, політика чистого стола, використання шаф, що замикаються, безпечні комунікації з офісом та контролі доступу до комп'ютерів.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕЧНА УТИЛІЗАЦІЯ АБО ПОВТОРНЕ ВИКОРИСТАННЯ ОБЛАДНАННЯ

Мета: Забезпечити безпечне знищення або повторне використання обладнання для запобігання витоку інформації.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Знищення даних:**
  Використання методів перезапису, шредінгу, фізичного знищення для безпечного видалення інформації з пристроїв.
  – Методи перезапису
  – Фізичне знищення

- **Документування:**
  Ведення записів про утилізацію обладнання, включаючи методи знищення даних.
  – Журнали утилізації
  – Сертифікати знищення

- **Повторне використання:**
  Перевірка та очищення даних перед повторним використанням обладнання.
  – Перевірка обладнання
  – Очищення даних

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕЧНА УТИЛІЗАЦІЯ АБО ПОВТОРНЕ ВИКОРИСТАННЯ ОБЛАДНАННЯ

Політика безпеки інфраструктури: безпечна утилізація та повторне використання обладнання

ВІДПОВІДНИЙ КОНТРОЛЬ:

Всі елементи обладнання, які містять носії пам'яті, повинні бути перевірені, щоб забезпечити, що будь-які чутливі дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

БЕЗПЕЧНА УТИЛІЗАЦІЯ АБО ПОВТОРНЕ ВИКОРИСТАННЯ ОБЛАДНАННЯ

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Оцініть, чи перевіряються всі елементи обладнання, що містять носії пам'яті, для забезпечення видалення або безпечного перезапису будь-яких чутливих даних або ліцензійного програмного забезпечення перед вилученням обладнання.		
2. Переконайтеся, що для видалення інформації використовуються методи, які роблять початкову інформацію невідновлюваною, а не стандартні функції видалення або форматування.		
3. Оцініть, чи проводиться оцінка ризику для ушкоджених пристроїв, що містять чутливі дані, для визначення, чи краще фізично зруйнувати ці елементи, надіслати їх в ремонт або списати.		
4. Перевірте, чи обладнання, що містить носії пам'яті, при повторному використанні в організації проходить процес видалення або перезапису даних відповідно до стандартів безпеки.		
5. Оцініть, чи ведеться документація про процес видалення або перезапису чутливих даних на обладнанні перед його вилученням або повторним використанням.		

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ПЕРЕМІЩЕННЯ МАЙНА

Мета: Забезпечити захист обладнання під час його транспортування.

ОСНОВНІ ПОЛОЖЕННЯ:

- **Планування транспортування:**
  Вибір безпечного маршруту, надійна упаковка обладнання для запобігання пошкодженням.
  – Безпечний маршрут
  – Надійна упаковка

- **Супровід:**
  Використання охорони під час транспортування критичного обладнання.
  – Охоронний супровід
  – Системи відстеження

- **Документування:**
  Ведення записів про переміщення обладнання.
  – Журнали переміщення
  – Контрольні списки

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ПЕРЕМІЩЕННЯ МАЙНА

Політика безпеки інфраструктури: переміщення майна

ВІДПОВІДНИЙ КОНТРОЛЬ:

Обладнання, інформація чи програмне забезпечення не повинні виноситись назовні без попередньої авторизації цих дій.

Зона ризиків IT: Фізична безпека та безпека інфраструктури

ПЕРЕМІЩЕННЯ МАЙНА

Операційна ефективність контролів: атрибути перевірки

Опис процедури: задокументуйте результати виконання наступних кроків	Відповідь	Коментарі
1. Перевірте, чи всі випадки виносу обладнання, інформації або програмного забезпечення з організації попередньо авторизовані відповідними уповноваженими особами.		
2. Переконайтеся, що найманий персонал, постачальники, та користувачі третіх сторін, уповноважені дозволяти переміщення активів, чітко ідентифіковані та мають належні повноваження.		
3. Оцініть, чи встановлюються обмеження на термін переміщення обладнання і чи перевіряється відповідність при поверненні обладнання в організацію.		
4. Перевірте, чи ведеться реєстрація обладнання, яке переміщується з організації, а також чи реєструється його повернення.		
5. Оцініть, чи проводяться вибіркові перевірки для виявлення неавторизованого переміщення майна, пристроїв записування, зброї тощо.		

Опитування

1. Який з наступних варіантів є найкращою практикою для розміщення обладнання, що обробляє чутливу інформацію?

a) Розміщення обладнання в зоні з вільним доступом для забезпечення швидкого доступу до нього.
b) Розташування обладнання під обмеженим кутом огляду для зниження ризику спостереження інформації неавторизованими особами.
c) Розміщення обладнання в центрі приміщення для кращого охолодження.
d) Використання обладнання в загальнодоступних приміщеннях для економії простору.

2. Який з наступних заходів є необхідним для безпечного обслуговування обладнання?

a) Проведення обслуговування тільки під час робочих годин.
b) Здійснення обслуговування тільки авторизованим обслуговуючим персоналом.
c) Обслуговування обладнання будь-яким доступним працівником, щоб не затримувати процес.
d) Виконання обслуговування без фіксації несправностей у журналі.

3. Як слід поводитися з портативним комп'ютером під час переїзду, щоб забезпечити його безпеку?

a) Переносити як ручний багаж і, за можливості, приховувати.
b) Залишити у багажному відділенні для зручності.
c) Тримати його постійно ввімкненим, щоб уникнути втрати даних.
d) Переносити його у відкритому вигляді, щоб швидко отримати доступ до інформації.

4. Що слід робити з обладнанням, яке містить чутливу інформацію і більше не використовується?

a) Залишити його у приміщенні організації до подальшого рішення.
b) Подарувати його співробітникам для домашнього використання.
c) Фізично знищити або видалити дані таким чином, щоб інформація стала невідновлюваною.
d) Передати його іншій організації без перевірки.

USAID
FROM THE AMERICAN PEOPLE

ЗАПИТАННЯ ТА ВІДПОВІДІ

USAID
FROM THE AMERICAN PEOPLE

ДЯКУЄМО ВАМ ЗА УВАГУ ТА ОЧІКУЄМО НА НАСТУПНІ ТРЕНІНГИ

СТЕЖТЕ ЗА НОВИНАМИ
Наступний тренінг з ІТ Аудиту: Жовтень/листопад 2024 року.
Онлайн тренінг. Частина ІІІ.

Матеріали з попередніх/поточних тренінгів будуть розміщені на сайті Міністерства Фінансів України у розділі Департаменту гармонізації ДВФК — ви можете перейти за посиланням https://mof.gov.ua/uk/provedeni-zahodi-z-pitan-dvfk або скористатись QR-кодом, що наведений праворуч.