КРОК 1 . Компанія «Фінанс» має такі ключові фінансові процеси:

Процес формування та подання податкової звітності.

Збір фінансових даних за звітний період, їх перевірка, розрахунок податкових зобов'язань.

Процес управління кредиторською заборгованістю та оплати рахунків.

Реєстрація вхідних рахунків від постачальників, перевірка їх на відповідність умовам договорів.

Процес бюджетування та фінансового планування.

Розробка бюджетів підрозділів на наступний рік.

КРОК 2. Розробка рольової моделі

Роль: Адміністратор системи
Опис позиції: Технічний спеціаліст, відповідальний за функціонування ПЗ, але не за фінансовий зміст.
Повноваження:
- керування обліковими записами
- керування ролями та правами доступу
- моніторинг продуктивності системи, створення резевних копій
- **НЕ МАЄ ПРАВА на перегляд, створення чи редагування фінансових даних**

Системний адміністратор також має дотримуватися принципу щоб не допустити конфлікт інтересів, адміністратор має доступ до «системи», але не до «даних». Не може приховати свої дії в фінансових операціях.

==========

Роль: Бухгалтер
Опис позиції: Виконує операційні задачі, введення даних, проведення оплат.
Повноваження:
- введення даних, обробка договорів
- формування платіжних доручень
- формування податкових звітів

Користувач рівня **ВИКОНАВЕЦЬ**, користувач має право на створення та коригування документів, але **НЕ МАЄ ПРАВА НА ПІДПИС ТА ВІДПРАВКУ** документів.

==========

Роль: Фінансовий аналітик
Опис позиції: готує аналітичні фінансові звіти, прогнози та пропозиції для керівництва.
Повноваження:
- **ПЕРЕГЛЯД** всіх фінансових даних, звітів

- погодження бюджетів компанії
- перегляд лог файлів з метою аудиту фінансових операцій
- **НЕ МАЄ ПРАВА** на проведення платежів, редагування бюджетних даних, звітів.

Забезпечує готовність та відкритий доступ до основних фінансових показників компанії. А також треба УНЕМОЖЛИВИТИ КОРИГУВАННЯ ВЖЕ ПОДАНОЇ ЗВІТНОСТІ ТА АНАЛІЗІВ ФІНАНСОВИХ СПРАВ, ЯКІ ВЖЕ БУЛИ ЗАТВЕРДЖЕНІ КЕРІВНИКОМ

==========

Роль: Керівник
Опис позиції: приймає стратегічні рішення на основі фінасових даних.
Повноваження:
- ПЕРЕГЛЯД всіх фінансових даних, звітів
- погодження та підпис бюджетів та фінансових операцій
- перегляд лог файлів з метою аудиту
- **НЕ МАЄ ПРАВА** на підготовку та внесення змін у фінансові документи, проведення платежів, створення звітності

КРОК 3 . Вибір методів автентифікації

Обраний метод: Багатофакторна автентифікація (MFA/2FA) з різним рівнем строгості залежно від ролі.

1. Для всіх користувачів (**Бухгалтер, Аналітик, Керівник**):
Обов'язкова MFA на основі:
Фактор 1: **Знаю — Строгий пароль** (12+ символів, різні регістри, цифри, спец. символи), який змінюється кожні 90 днів.
Фактор 2: **Маю — Push-сповіщення** через мобільний додаток автентифікації (наприклад, Google Authenticator, Microsoft Authenticator).
Обґрунтування: Це значно підвищує безпеку порівняно з просто паролем, захищаючи від витоків облікових даних та фішингу. Зручність забезпечується використанням звичайного смартфона.

2. Для привілейованих користувачів (**Адміністратор системи**):
Посилена MFA на основі:
Фактор 1: **Знаю — Строгий пароль** (14+ символів), який змінюється кожні 60 днів.
Фактор 2: **Маю — Апаратний токен** (наприклад, YubiKey) або сертифікат.
Додатково для Адміністратора: Вхід до системи з правами адміністратора дозволяється тільки з виділених, безпечних робочих станцій в межах офісної мережі компанії (або через VPN).

Обґрунтування: Апаратні токени є найбезпечнішим фактором «володіння», стійким до фішингу та викрадення сесії. Для адміністратора з максимальними правами необхідний максимальний захист, оскільки компрометація цього акаунта призведе до повного заволодіння системою.

КРОК 4: Періодичний перегляд та аудит

Встановлений графік та процедури:

Щоквартальний перегляд:
Що перевіряється: Актуальність призначених ролей. Чи відповідають права посаді кожного співробітника? Чи не з'явилися надлишкові привілеї?
Хто проводить: Головний бухгалтер разом із Адміністратором системи та менеджером з безпеки.
Результат: Створення звіту про відповідність та завдання на виправлення невідповідностей.
==========
При настанні події:
Звільнення співробітника: Адміністратор системи негайно блокує обліковий запис на підставі наказу від відділу кадрів.
Переведення співробітника: Адміністратор системи вносить зміни до ролей облікового запису на підставі офіційного запиту від керівника підрозділу та відділу кадрів. Старі права відбираються, надаються нові.
==========
Щорічний аудит:
Що перевіряється: Логи входу в систему (особливо невдалі спроби, вхід у позаробочий час), логі змін критичних даних (проводки, реквізити, суми платежів), логі призначення прав.
Хто проводить: Внутрішній або зовнішній аудитор, незалежний від фінансового відділу та IT-адміністрації.
Результат: Аудиторський висновок про ефективність контролю, дотримання політик безпеки та виявлення потенційних аномалій.
==========