

ЗАТВЕРДЖЕНО
Рішенням Спостережної Ради
КРЕДИТНОЇ СПІЛКИ
«ФІНАНСОВА ПІДТРИМКА»
Протокол № 329 від «19» березня 2023 ро
Голова Спостережної ради



/Н.В.Мироненко/

ПОЛОЖЕННЯ
ЩОДО НАДАННЯ, СКАСУВАННЯ ТА КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ
СИСТЕМ КРЕДИТНОЇ СПІЛКИ «ФІНАНСОВА ПІДТРИМКА», ЩО
ВИКОРИСТОВУЮТЬСЯ ДЛЯ ПРИЙМАННЯ, РЕЄСТРАЦІЇ, ОБРОБЛЕННЯ,
ЗБЕРІГАННЯ, НАДСИЛАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

м. Харків, 2024 рік

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Це Положення про надання, скасування та контролю доступу до інформаційних систем КРЕДИТНОЇ СПІЛКИ «ФІНАНСОВА ПІДТРИМКА» (далі – Спілка/установа), що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів (далі – Положення) є внутрішній документом, який встановлює вимоги щодо надання, скасування та контролю доступу до інформаційних систем установи, що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів.

1.2. Положення розроблене відповідно до вимог чинного законодавства України, Закону України «Про електронні документи та електронний документообіг», Законів України "Про електронну ідентифікацію та електронні довірчі послуги", Положення про використання електронного підпису та електронної печатки, затвердженого постановою Правління Національного банку України від 20.12.2023 № 172, інших нормативних документів Національного банку України та внутрішніх документів Спілки.

Положення є обов'язковим для виконання всіма працівниками Спілки й уповноваженими представниками.

1.3. Для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів Спілка використовує зовнішні сервіси, наприклад, сервіс «ВЧАСНО» або «Дія.Підпис», М.Е.Дос.

1.4. При використанні зовнішніх сервісів, приймання, реєстрація, оброблення, зберігання, надсилання електронних документів здійснюється виключно з правилами цих сервісів. Клієнти та контрагенти Спілки під час вчинення будь-яких вищезазначених дій із електронними документами обізнані із тим, що це здійснюється не безпосередньо Спілкою, а зовнішнім сервісом.

1.5. Спілка не несе відповідальності за протоколи доступу або захисту інформації, що застосовуються зовнішніми сервісами.

2. ЗАГАЛЬНІ ВИМОГИ ДО ІДЕНТИФІКАЦІЇ, АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ КЛІЄНТІВ

2.1. Клієнти Спілки мають самостійний доступ до зовнішніх інформаційних систем(сервісів).

2.2. Ідентифікація, автентифікація, авторизація клієнтів здійснюється зовнішніми інформаційними системами(сервісами) у відповідності до існуючих правил/положень/регламенту таких систем(сервісів).

2.3. Вимоги до ідентифікації, автентифікації, авторизації в системі(сервісі).

Вимоги до ідентифікації, автентифікації, авторизації в системі(сервісі) встановлюються системами(сервісами) у відповідності до існуючих правил/положень/регламенту .

3. ПОСЛІДОВНІСТЬ ДІЙ ПІД ЧАС УПРАВЛІННЯ ДОСТУПОМ, ПОСЛІДОВНІСТЬ ДІЙ ПІД ЧАС УПРАВЛІННЯ ВІДДАЛЕНИМ ДОСТУПОМ (РЕЄСТРАЦІЯ, НАДАННЯ ПОВНОВАЖЕНЬ, ПЕРЕГЛЯД ТА СКАСУВАННЯ ДОСТУПУ)

3.1. Доступ до зовнішніх інформаційних систем(сервісів) є віддаленим. Працівники та клієнти Спілки зобов'язані виконувати інструкції/правила інформаційних систем(сервісів) та чинного законодавства України щодо інформаційної безпеки, вчиняти всі дії для уникнення несанкціонованого доступу третіх осіб до інформаційних систем.

Послідовність дій під час управління віддаленим доступом (реєстрація, надання повноважень, перегляд та скасування доступу) регламентуються правилами/положеннями/регламентами зовнішніх інформаційних систем(сервісами) .

3.2. До інформаційних зовнішніх систем(сервісів) з боку Спілки мають доступ обмежене коло працівників(керівник та головний бухгалтер).

3.3. Надання повноважень іншим працівникам Спілки для доступу до зовнішніх інформаційних систем(сервісів) з боку Спілки не передбачено.

3.4. Доступ скасовується у разі звільнення працівника, стороннього доступу до зовнішньої системи(сервісів) з використанням даних працівника.

4. ПЕРЕЛІК ТИПОВИХ ФУНКЦІЙ ТА ПРАВ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ(СЕРВІСІВ)

Щодо системи «Вчасно».

4.1. Застосовується розділення прав на виконання типів дій на рівні кожного користувача:

- Перегляд документів
- Коментування документів
- Завантаження документів у сервіс
- Збереження документів на локальному комп'ютері
- Друк документів
- Видалення документів
- Підписання та відхилення документів
- Запрошення працівників
- Редагування інформації про компанію
- Редагування та видалення працівників

4.2. Усі ключі шифрування та паролі стають доступними для програми тільки в момент запуску програми у середовищі. Паролі користувачів зберігаються в зашифрованому вигляді. Управління ключами шифрування здійснюється за допомогою AWS KMS.

4.3. Архітектура рішення передбачає обмеження доступу до файлів клієнтів співробітниками компанії в декілька етапів.

4.4. Двухфакторна аутентифікація (2FA) здійснюється за телефоном.

Щодо інших систем:

4.5. Права адміністратора Спілки інформаційної системи(сервісу), які передбачають можливість скасування дій користувача, додання, видалення користувачів перебувають у керівника Спілки.

5. ВИМОГИ ЩОДО ЗДІЙСНЕННЯ ЗАХОДІВ КОНТРОЛЮ ДОСТУПУ, ПЕРІОДИЧНІСТЬ КОНТРОЛЮ НАДАНИХ ПРАВ ДОСТУПУ

5.1. Керівник Спілки проводять контроль наданих доступів до інформаційних систем(сервісів) 1 раз на місяць.

Щодо системи «Вчасно».

5.2. Для зберігання документів використовується сервер Amazon S3 із дзеркалом сховища в іншому регіоні. Стійка інфраструктура Amazon S3 забезпечує надійне зберігання об'єктів. Для збереження конфіденційності файлів клієнтів використовується шифрування AES-256.

5.3. Здійснюється логування дій користувачів.

6. ВИМОГИ ДО ПРОТОКОЛЮВАННЯ ДІЙ ПІД ЧАС УПРАВЛІННЯ ДОСТУПОМ

Загальні положення

6.1. Політика журналювання та перегляду журналів. Журнали можуть ідентифікувати авторизовані та неавторизовані спроби доступу до ресурсів із зазначенням точного часу та місця походження. Перевірка журналу системи та мережі виконується довільно принаймні раз на тиждень; після відповідних інцидентів.

6.2. З метою запобігання порушень інформаційної безпеки та уникнення кіберінцидентів здійснюється такі заходи:

6.2.1. встановлюється чіткий розподіл прав доступу до засобів захисту мережі, серверів та застосунків;

6.2.2. всі технічні, службові та операції протоколюються системою автоматично;

6.2.3. забезпечується можливість відновлення до робочого стану всіх мережевих засобів захисту інформації та серверного обладнання у випадку збоїв.

Щодо системи «ВЧАСНО»:

6.3. Здійснюється логування дій користувачів. Сервіс записує дії користувачів компанії у сервісі для можливості перегляду адміністраторами клієнтів.