**Назва документа:** План відновлення після катастроф: CB Automation

**Версія:** 1.5.0

**Видавець:** ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «КОНСАЛТИНГ УА-РО»

## 1. МЕТА ТА СФЕРА ЗАСТОСУВАННЯ

Цей План відновлення після катастроф (DRP) визначає необхідні процедури для відновлення Додатка CB Automation та пов'язаних із ним баз даних MariaDB/MySQL у разі апаратного збою, кібератаки або критичного пошкодження програмного забезпечення.

**2. ПРОТОКОЛИ РЕЗЕРВНОГО КОПІЮВАННЯ** Щоб гарантувати відсутність втрати даних щодо виданих сертифікатів та звітності до IAF CERTSEARCH, Системний адміністратор повинен дотримуватися наступних графіків:

### Резервні копії бази даних:

Автоматизовані SQL-дампи бази даних cb_automation повинні виконуватися щодня.

### Резервні копії файлової системи:

Уся веб-директорія (наприклад, /home/sites/cb) та папка /includes, що містить критичні файли конфігурації (такі як cb_cert_functions.php), повинні копіюватися щотижня або перед будь-яким оновленням системи.

### Зовнішнє зберігання:

Усі резервні копії повинні безпечно передаватися на віддалений сервер або в захищене хмарне сховище, незалежне від основного середовища хостингу.

**3. ПРОЦЕДУРА ВІДНОВЛЕННЯ (RTO та RPO)** У разі катастрофічного збою:

### Підготовка середовища:

Розгорніть чисте середовище Linux/Windows з Apache/Nginx, PHP 8.2/8.4 та MariaDB 10.4+.

### Відновлення файлів:

Розпакуйте останню резервну копію файлової системи у визначену кореневу веб-директорію. Забезпечте правильні права власності та доступу (наприклад, www-data або apache).

### Відновлення бази даних:

Створіть нову базу даних та імпортуйте останній щоденний SQL-дамп.

**Перевірка конфігурації:**

Переконайтеся, що облікові дані бази даних у файлі конфігурації та IAF_API_KEY у файлі /includes/cb_cert_functions.php не пошкоджені.

**Відновлення роботи:**

Перезапустіть веб-сервер і переконайтеся, що Клієнтський портал та Панель адміністратора повністю доступні.