Document Title: Disaster Recovery Plan: CB Automation

Version: 1.5.0

Publisher: CONSULTING UA-RO LIMITED LIABILITY COMPANY

1. PURPOSE & SCOPE This Disaster Recovery Plan (DRP) outlines the necessary procedures to restore the CB Automation App and its associated MariaDB/MySQL databases in the event of hardware failure, cyberattack, or critical software corruption.

2. BACKUP PROTOCOLS To ensure zero data loss regarding issued certificates and IAF CERTSEARCH reporting, the following backup schedules must be maintained by the System Administrator:

Database Backups:

Automated SQL dumps of the CB Automation database must be executed daily.

File System Backups:

The entire web directory (e.g., /home/sites/cb) and the /includes folder containing critical configuration files (like cb_cert_functions.php) must be backed up weekly or before any system update.

Off-site Storage:

All backups must be securely transferred to an off-site server or secure cloud storage independent of the primary hosting environment.

3. RESTORATION PROCEDURE (RTO & RPO) In the event of a catastrophic failure:

Environment Provisioning:

Deploy a clean Linux/Windows environment with Apache/Nginx, PHP 8.2/8.4, and MariaDB 10.4+.

File Restoration:

Extract the latest File System backup into the designated web root directory. Ensure proper ownership and permissions (e.g., www-data or apache).

Database Restoration:

Create a new database and import the latest daily SQL dump.

Configuration Check:

Verify that the database credentials in the configuration file and the IAF_API_KEY in /includes/cb_cert_functions.php are intact.

Service Resumption:

Restart the web server and verify that the Client Portal and Admin Dashboard are fully accessible.