RyzykoDesk

Instrukcja instalacji i pierwszego uruchomienia

Program do analizy ryzyka bezpieczeństwa informacji zgodnej z ustawą o krajowym systemie cyberbezpieczeństwa, ISO/IEC 27001:2022 i ISO/IEC 27005:2022.

Wersja programu: 1.0.0

Data instrukcji: 19.11.2026

Najważniejsze w skrócie

1. Pobierz instalator z linku od ResData i sprawdź jego sumę kontrolną (rozdział 2).
2. Zainstaluj program – nie są potrzebne uprawnienia administratora (rozdział 3).
3. Osoba prowadząca analizę (Pełnomocnik) tworzy plik organizacji i **drukuje klucz odzyskiwania** (rozdział 4).
4. Pełnomocnik zakłada konta pozostałym osobom (rozdział 5).

1. Zanim zaczniesz

Wymagania

- Windows 10 lub Windows 11 (64-bitowy).
- Ok. 400 MB wolnego miejsca na dysku.
- Instalacja nie wymaga uprawnień administratora – program instaluje się dla bieżącego użytkownika.
- Do automatycznych aktualizacji: dostęp do adresu aktualizacje.resdata.pl (HTTPS, port 443). Bez Internetu program działa normalnie, a aktualizacje instaluje się ręcznie.

Jak program przechowuje dane

Wszystkie dane organizacji – aktywa, ryzyka, kwestionariusze, plan postępowania i dziennik zdarzeń – są w jednym zaszyfrowanym pliku z rozszerzeniem .ryzyko. Plik pozostaje wyłącznie w Państwa organizacji: program nie wysyła danych do ResData ani nigdzie indziej. Bez konta w programie (albo klucza odzyskiwania) nikt nie odczyta zawartości pliku – również ResData.

Kto z programu korzysta

Program przewiduje kilka ról. Zwykle wygląda to tak:

Rola	Kto to zwykle jest	Co robi w programie
Administrator aplikacji	Pełnomocnik lub informatyk	Zakłada konta, ustawia kopie i aktualizacje
Koordynator	Pełnomocnik ds. cyberbezpieczeństwa	Prowadzi całą analizę i przygotowuje raport dla Zarządu
Właściciel obszaru	Kierownicy komórek	Wypełniają kwestionariusze, oceniają ryzyka swojej komórki
Ekspert IT/OT	Administratorzy systemów, IOD	Wskazują podatności i zabezpieczenia
Zarząd	Członkowie Zarządu	Zatwierdzają raport i akceptują ryzyka nieakceptowalne
Audytor	Audytor wewnętrzny lub zewnętrzny	Tylko odczyt, w tym dziennika zdarzeń
Respondent	Wybrani pracownicy	Tylko wypełnienie przydzielonego kwestionariusza

2. Pobranie programu

1. Otwórz link otrzymany od ResData: `https://aktualizacje.resdata.pl/ryzykodesk/`
2. Kliknij **Pobierz instalator**. Plik RyzykoDesk-Setup-1.0.0.exe ma ok. 89 MB.
3. Sprawdź, czy plik nie został zmieniony po drodze. Otwórz PowerShell w folderze z pobranym plikiem i wpisz:

   ```
   Get-FileHash .\RyzykoDesk-Setup-1.0.0.exe -Algorithm SHA256
   ```

   Wynik musi być identyczny z sumą kontrolną:

481259CF23A0938736E8498DEE2EDA9BB6831148566C9642C6FF5A1A27754EC0

Jeśli suma się nie zgadza

Nie uruchamiaj pliku. Usuń go, pobierz ponownie i skontaktuj się z ResData.

3. Instalacja

1. Kliknij dwukrotnie pobrany plik **RyzykoDesk-Setup-1.0.0.exe**.
2. Jeśli Windows wyświetli okno „System Windows ochronił komputer”, kliknij **Więcej informacji**, a następnie **Uruchom mimo to**. To standardowe ostrzeżenie dla nowych programów (szczegóły w ramce poniżej).
3. Wybierz folder instalacji (możesz zostawić domyślny) i kliknij **Zainstaluj**.
4. Po zakończeniu program uruchomi się sam. Na pulpicie i w menu Start pojawi się skrót **RyzykoDesk**.

Informacja dla działu IT

Jeżeli w organizacji obowiązują reguły blokujące nieznane programy (Microsoft Defender, reguły ASR, AppLocker, Intune), dopuść instalator według sumy SHA-256 podanej w rozdziale 2.

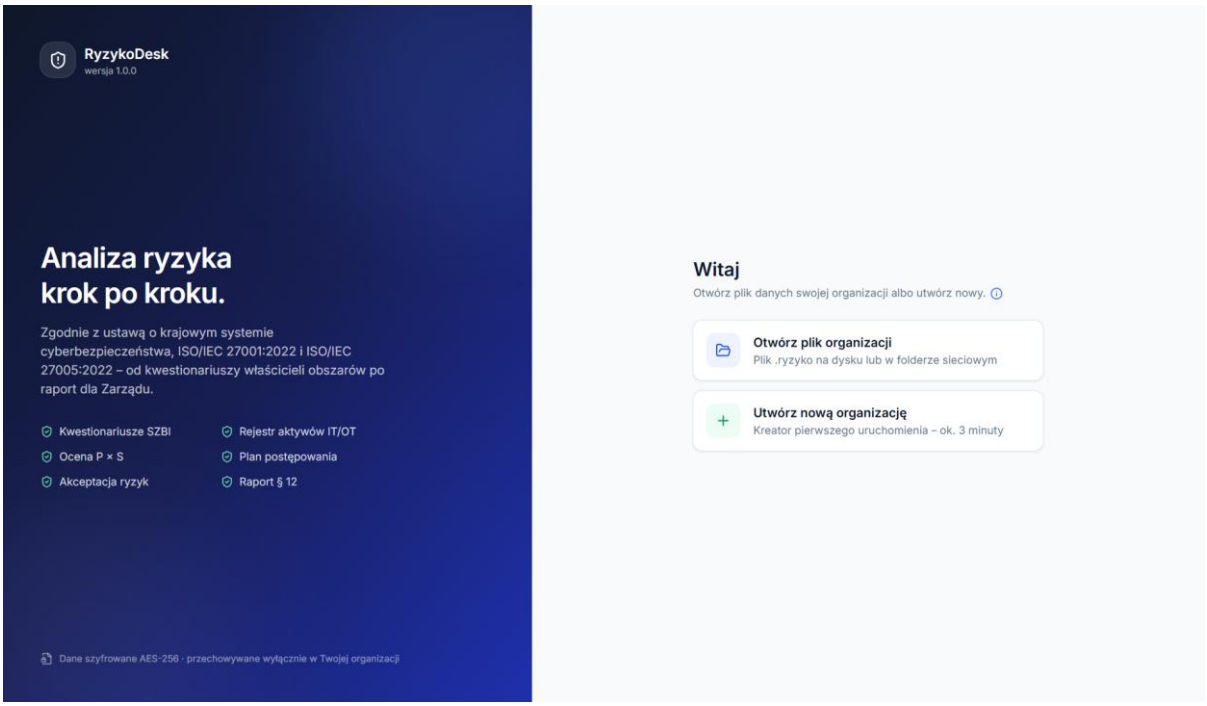
Program instaluje się w profilu użytkownika (`%LOCALAPPDATA%\Programs`). Ustawienia programu – bez danych organizacji – zapisuje w `%APPDATA%\RyzykoDesk`.

Program łączy się z Internetem wyłącznie w celu sprawdzenia aktualizacji: HTTPS do aktualizacje.resdata.pl. Nie wysyła danych ani telemetrii.

Każda osoba korzystająca z programu instaluje go na swoim komputerze. Instalację można też przeprowadzić narzędziem do dystrybucji oprogramowania (np. Intune lub GPO).

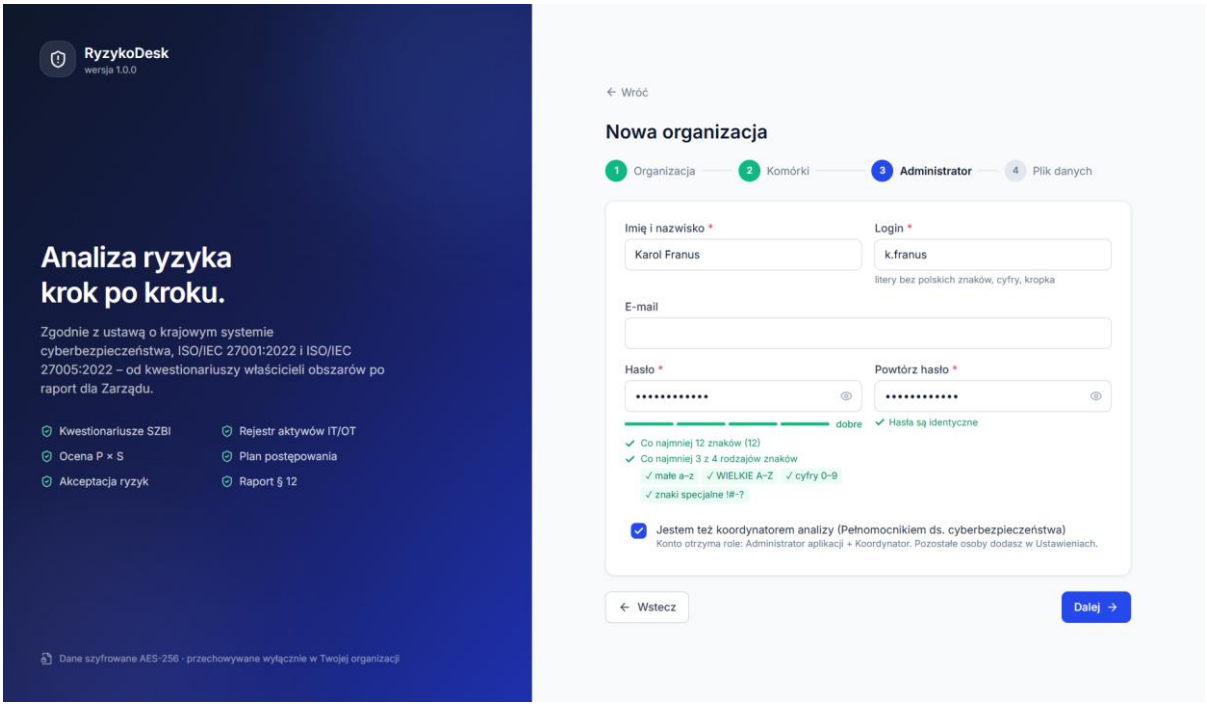
4. Pierwsze uruchomienie – utworzenie organizacji

Ten krok wykonuje jedna osoba – najczęściej Pełnomocnik ds. cyberbezpieczeństwa. Pozostali użytkownicy będą otwierać już utworzony plik.



Ekran startowy – wybierz „Utwórz nową organizację”

1. Na ekranie startowym kliknij **Utwórz nową organizację**.
2. **Organizacja** – wpisz nazwę pełną i skróconą, wybierz sektor. Sektor decyduje o przykładach w katalogu zagrożeń i skali skutków; wszystko można później zmienić.
3. **Komórki** – popraw proponowaną listę komórek organizacyjnych według schematu organizacyjnego (symbol i nazwa).
4. **Administrator** – wpisz swoje imię i nazwisko, login oraz hasło. Hasło musi mieć co najmniej 12 znaków i co najmniej 3 z 4 rodzajów znaków: małe litery, wielkie litery, cyfry, znaki specjalne. Program na bieżąco pokazuje, czego brakuje.
5. **Plik danych** – wskaż, gdzie zapisać plik .ryzyko (patrz ramka poniżej) i kliknij **Utwórz organizację**.



Kreator – krok „Administrator”: wymagania hasła są odhaczane na bieżąco

Gdzie zapisać plik .ryzyko?

Jedna osoba pracuje w programie – dowolny folder na dysku, objęty kopią zapasową.

Kilka osób z różnych komputerów – folder sieciowy (udział), do którego dostęp mają **wyłącznie uczestnicy analizy**. Program pilnuje, by zapisy różnych osób się nie nadpisywały, i co kilka sekund pokazuje zmiany wprowadzone przez innych.

Plik i folder kopii obok niego zawierają informacje o podatnościach organizacji – są informacją chronioną.

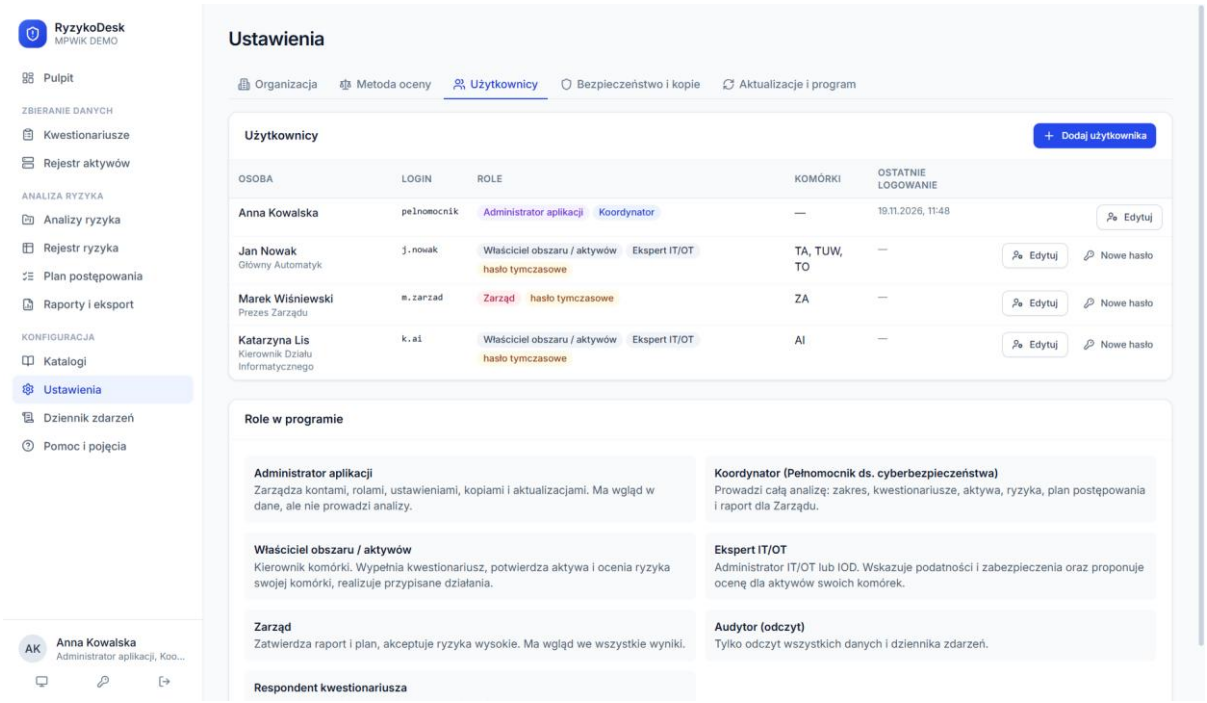
Klucz odzyskiwania – bardzo ważne

Po utworzeniu organizacji program wyświetli klucz odzyskiwania, np. XXXXX-XXXXX-XXXXX-XXXXX-XXXXX. Tylko ten klucz pozwoli odzyskać dostęp do danych, jeśli wszyscy administratorzy zapomną haseł.

- **Wydrukuj go** (przycisk Drukuj) lub przepisz i przechowuj w sejfie, oddzielnie od komputera.
- **Program pokazuje klucz tylko raz.** Nowy klucz może później wygenerować administrator (Ustawienia → Bezpieczeństwo i kopie) – poprzedni przestaje wtedy działać.
- Nie przesyłaj klucza pocztą e-mail ani komunikatorem i nie przekazuj go ResData.

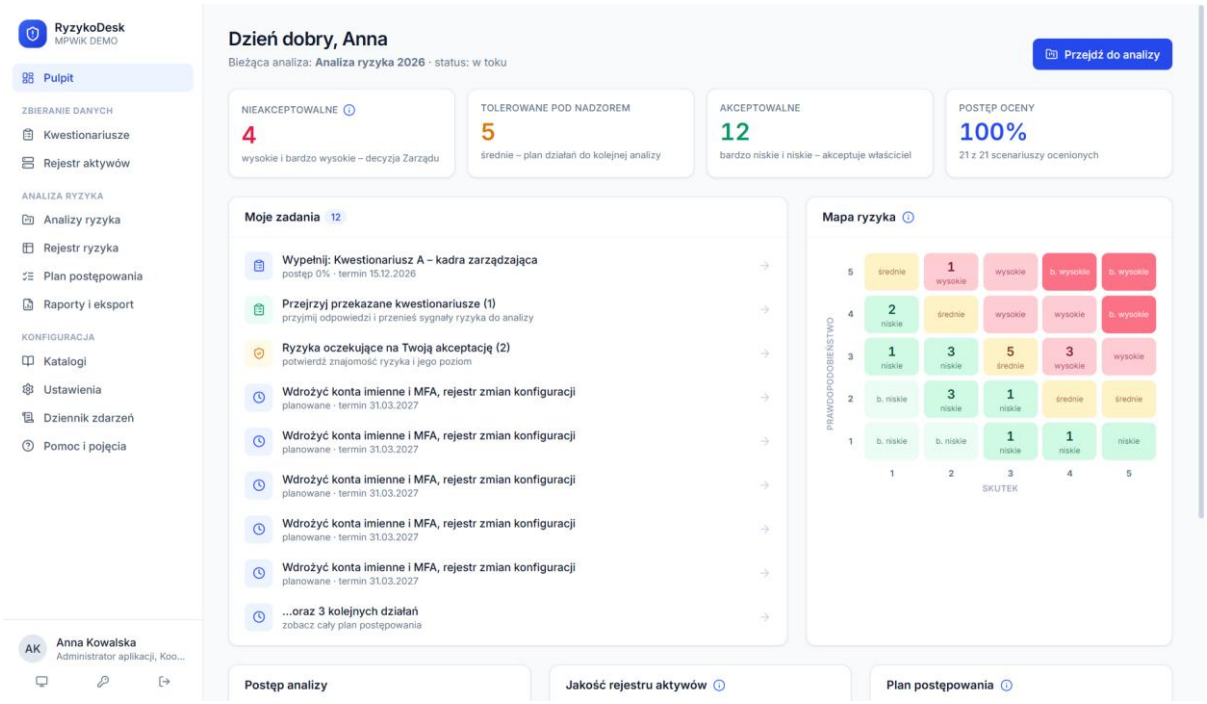
5. Dodanie użytkowników

1. Wejdź w **Ustawienia → Użytkownicy** i kliknij **Dodaj użytkownika**.
2. Wpisz imię i nazwisko, login, stanowisko; zaznacz **role** i **komórki organizacyjne**. Właściciel obszaru i ekspert widzą tylko aktywa i ryzyka swoich komórek.
3. Program zaproponuje **hasło tymczasowe**. Przekaż je osobie bezpiecznym kanałem – osobiście lub telefonicznie. Przy pierwszym logowaniu program wymusi ustawienie własnego hasła.
4. Przekaż użytkownikowi informację, gdzie leży plik .ryzyko. Użytkownik instaluje program (rozdział 3), na ekranie startowym wybiera **Otwórz plik organizacji** i loguje się. Program zapamięta plik na kolejne uruchomienia.



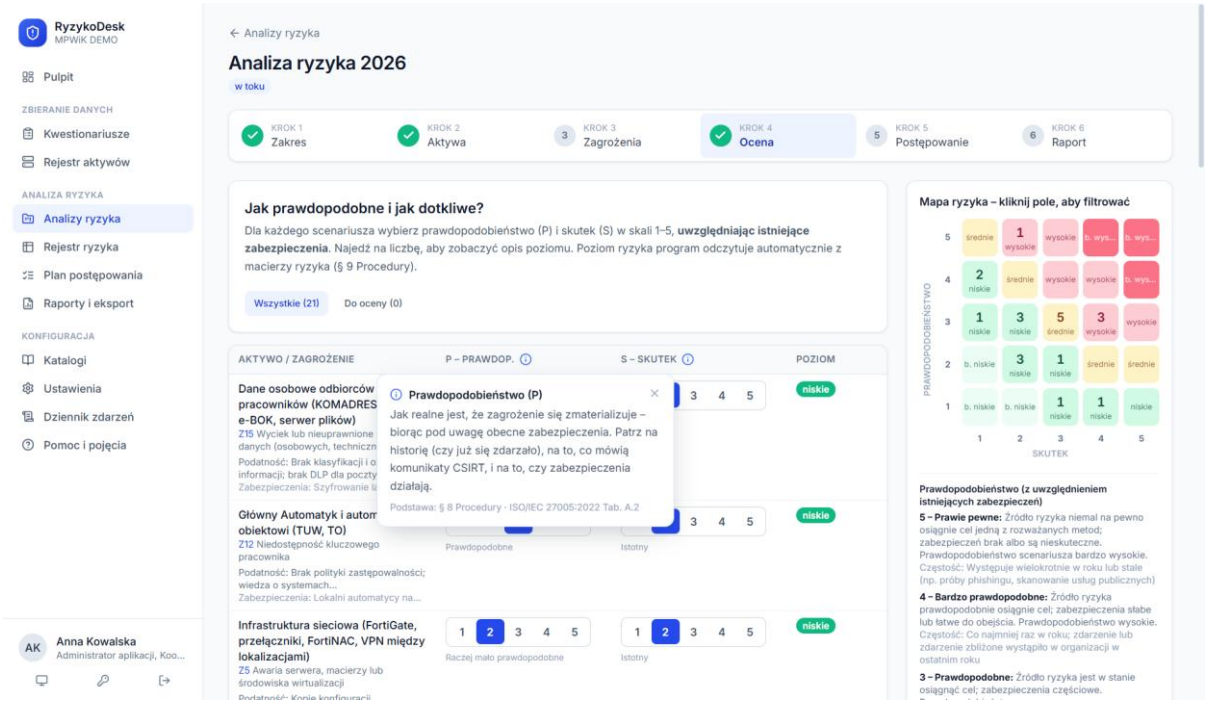
6. Jak przebiega praca w programie

1. **Kwestionariusze** – koordynator przydziela kwestionariusz A kierownikom i B wybranym pracownikom. Ryzykowne odpowiedzi stają się podpowiedziami podatności.
2. **Rejestr aktywów** – uzupełnij ręcznie albo zaimportuj z arkusza Excel (przycisk Importuj z Excela).
3. **Analiza ryzyka** – kreator w 6 krokach: zakres → aktywa → zagrożenia i podatności → ocena P i S → postępowanie z ryzykiem → akceptacja i raport.
4. **Raporty** – raport dla Zarządu (Word/PDF) oraz Rejestr ryzyka i Rejestr aktywów (Excel).



Pulpit: moje zadania, ryzyka według oceny, mapa ryzyka

Przy ważnych pojęciach jest ikona ⓘ – po kliknięciu wyświetla wyjaśnienie prostym językiem z odwołaniem do procedury lub normy. Wszystkie pojęcia są też w menu **Pomoc i pojęcia**.



Wyjaśnienie pod ikoną ⓘ

7. Bezpieczeństwo i kopie zapasowe

- Dane w pliku są szyfrowane algorytmem AES-256. Każdy użytkownik ma własne hasło.
- Po 5 błędnych próbach logowania konto blokuje się na 15 minut.
- Po 15 minutach bezczynności program sam się blokuje (czas zmienia administrator).
- Program codziennie wykonuje kopię pliku do folderu `<nazwa pliku> – kopie` obok pliku danych (domyślnie ostatnie 30 kopii).
- Kopia ręczna: **Ustawienia → Bezpieczeństwo i kopie → Zapisz kopię zapasową**. Zalecamy objęcie pliku i folderu kopii również kopiami zapasowymi organizacji.
- Każda zmiana jest zapisywana w **Dzienniku zdarzeń** (kto, co, kiedy). Przycisk **Sprawdź integralność** wykrywa ręczne modyfikacje historii.

8. Aktualizacje

Program sprawdza aktualizacje przy każdym uruchomieniu. Nowa wersja pobiera się w tle; w menu po lewej pojawi się komunikat „Nowa wersja gotowa – kliknij, aby zainstalować”. Aktualizacja nie zmienia danych w pliku .ryzyko.

Aktualizację można też sprawdzić ręcznie: **Ustawienia → Aktualizacje i program → Sprawdź teraz**. Na komputerach bez Internetu wystarczy uruchomić nowszy instalator – nadpisze program, dane pozostaną.

9. Rozwiązywanie problemów

Sytuacja	Co zrobić
Użytkownik zapomniał hasła	Administrator: Ustawienia → Użytkownicy → Nowe hasło. Użytkownik zaloguje się hasłem tymczasowym i ustawi własne.

Sytuacja	Co zrobić
Konto zablokowane po błędnych hasłach	Odczekaj 15 minut albo poproś administratora o nowe hasło (odblokowuje konto).
Wszyscy administratorzy zapomnieli haseł	Na ekranie logowania kliknij link pod przyciskiem Zaloguj i użyj klucza odzyskiwania.
„Plik danych jest chwilowo zablokowany przez inny komputer”	Inna osoba właśnie zapisuje zmiany – spróbuj ponownie za kilka sekund.
„Brak dostępu do pliku”	Sprawdź uprawnienia do folderu sieciowego i czy plik nie jest otwarty w innym programie.
Windows blokuje instalator	Patrz rozdział 3 („Więcej informacji → Uruchom mimo to”) lub poproś dział IT o dopuszczenie pliku.

10. Wsparcie

ResData – **[adres e-mail i telefon wsparcia ResData]**

Zgłaszając problem, podaj wersję programu (Ustawienia → Aktualizacje i program) i opis sytuacji. Nie przesyłaj pliku .ryzyko ani haseł – ResData nie potrzebuje dostępu do Państwa danych.