



Regulamin aplikacji ESO9 Profi w ESO9 Cloud

1. Wprowadzenie

Niniejszy regulamin określa zasady i warunki eksploatacji programu oraz korzystania z powiązanych usług w relacji z Klientem, a także procedury prawidłowego korzystania z programu przez Klienta.

Regulamin jest wiążący dla Klienta. W przypadku jego nieprzestrzegania przez Klienta Dostawca nie ponosi odpowiedzialności za prawidłowe działanie programu ani za należyte świadczenie powiązanych usług.

Regulamin oraz jego zmiany są publikowane na stronie internetowej pod adresem <https://eso9.cz/provozni-rad-cloud>.

2. Zmiany regulaminu

1. Dostawca jest uprawniony do uzupełniania i zmieniania regulaminu w związku ze zmianami technicznymi i organizacyjnymi, dodawaniem nowych funkcji programu lub wymaganiami Klientów.
2. Przed zmianą regulaminu Dostawca poinformuje Klientów o planowanej zmianie pocztą elektroniczną (e-mailem) lub poprzez opublikowanie tej informacji na stronie startowej aplikacji. Informacja będzie zawierać między innymi opis przygotowywanych zmian oraz datę ich wejścia w życie.
3. Poprzedni regulamin automatycznie traci moc w dniu wejścia w życie nowego regulaminu.

3. Godziny dostępności

1. Część serwerowa programu jest dostępna w dni robocze od godz. 6:00 do 22:00, a w dni wolne od pracy i święta od godz. 6:00 do 18:00. W tych godzinach Klienci mogą korzystać z programu bez ograniczeń.
2. Dostawca może przeprowadzać nadzwyczajne planowane przerwy w działaniu części serwerowej programu wyłącznie w niezbędnych przypadkach, gdy z przyczyn technicznych nie można ich przeprowadzić podczas standardowych przerw serwisowych. W takim przypadku Dostawca ma obowiązek poinformować upoważnioną osobę Klienta o planowanej przerwie co najmniej 2 dni wcześniej, pocztą elektroniczną lub poprzez opublikowanie tej informacji na stronie startowej aplikacji.
3. W przypadku zdarzeń nadzwyczajnych zagrażających bezpieczeństwu systemu, danych lub infrastruktury (np. cyberataku, krytycznej podatności albo podejrzenia wycieku danych) Dostawca jest uprawniony do natychmiastowego wstrzymania działania części serwerowej programu, również bez uprzedniego powiadomienia. Dostawca ma jednak obowiązek bez zbędnej zwłoki poinformować upoważnioną osobę Klienta o takiej interwencji, podając przyczyny przerwy oraz środki podjęte w celu wznowienia działania i zapewnienia bezpieczeństwa.

4. Dostęp do części serwerowej programu

1. Każdy Klient uzyskuje dostęp do programu za pośrednictwem przeglądarki internetowej (np. Google Chrome lub Microsoft Edge) pod adresem URL <https://cloud.eso.cz/název-aplikace>, gdzie segment „název-aplikace” oznacza indywidualną nazwę aplikacji Klienta i części klienckiej

programu.

2. W celu zabezpieczenia dostępu do części serwerowej programu przed nieuprawnionym użyciem w części klienckiej stosuje się certyfikaty elektroniczne wydawane przez Dostawcę. Alternatywnie lub dodatkowo można stosować nowoczesne silne uwierzytelnianie z użyciem technologii WebAuthn (np. kluczy bezpieczeństwa, danych biometrycznych lub zintegrowanych mechanizmów uwierzytelniania urządzenia), jeśli pozwala na to konkretne wdrożenie programu. Wybór metody uwierzytelniania wymaga uzgodnienia między Dostawcą a Klientem, z uwzględnieniem wymaganego poziomu bezpieczeństwa.
3. Użytkownicy Klienta uzyskują dostęp do części serwerowej programu za pomocą imiennego certyfikatu wystawionego konkretnemu użytkownikowi. Certyfikat jest nieprzenoszalny i nie może być udostępniany innemu użytkownikowi ani żadnej innej osobie. W przypadku korzystania z WebAuthn dane uwierzytelniające są również powiązane z konkretnym użytkownikiem i urządzeniem oraz podlegają analogicznym zasadom nieprzenoszalności i ochrony. Użytkownicy mają obowiązek chronić swoje środki dostępu przed nadużyciem.
4. Szczegółowa instrukcja uzyskania i instalacji certyfikatu jest dostępna pod adresem: <https://wiki.eso9.cz>. Jeżeli certyfikat ma być wystawiany bezpośrednio z aplikacji Klienta, aplikacja musi być technicznie przygotowana do takiego sposobu wystawiania certyfikatów i prawidłowo skonfigurowana.
5. Dostawca nie tworzy kopii zapasowych certyfikatów użytkowników ani ich kluczy prywatnych. Wyłącznie odpowiedzialność za bezpieczne przechowywanie i ewentualne tworzenie kopii zapasowych tych certyfikatów i kluczy ponosi Klient, a w praktyce jego poszczególni użytkownicy. W razie utraty certyfikatu lub klucza prywatnego należy wystąpić o wydanie nowego certyfikatu; Dostawca nie może odtworzyć utraconych ani przejętych danych dostępowych.
6. Wydanie nowego certyfikatu poza okresem ważności dotychczasowego certyfikatu podlega opłacie zgodnie z aktualnym Cennikiem usług. O zbliżającym się terminie wygaśnięcia certyfikatu użytkownik jest informowany podczas logowania do aplikacji.
7. W przypadku utraty, kradzieży lub naruszenia bezpieczeństwa certyfikatu bądź klucza prywatnego, a także rozwiązania stosunku pracy użytkownika z Klientem lub wygaśnięcia uprawnienia dostępu z innej przyczyny, Klient ma obowiązek niezwłocznie zgłosić ten fakt do usługi Hotline Dostawcy za pośrednictwem osoby upoważnionej. Dostawca unieważni następnie dany certyfikat i w razie potrzeby podejmie inne niezbędne działania zabezpieczające. Jeżeli Dostawca sam stwierdzi taką okoliczność, jest uprawniony do niezwłocznego unieważnienia certyfikatu bez uprzedniego powiadomienia Klienta w celu zapewnienia bezpieczeństwa systemu.
8. Dostawca zablokuje dostęp do programu z użyciem danego certyfikatu w ciągu 6 godzin od zgłoszenia tego faktu w dni robocze, w godzinach działania Hotline. Upoważniona osoba Klienta zostanie poinformowana o unieważnieniu certyfikatu. Jeżeli zgłoszenie nastąpi poza godzinami pracy, certyfikat zostanie unieważniony bez zbędnej zwłoki w najbliższym możliwym dniu roboczym.
9. Na podstawie zgłoszenia Klienta Dostawca może wydać nowy certyfikat. Warunkiem jest potwierdzenie tożsamości danego użytkownika oraz spełnienie wymagań technicznych i bezpieczeństwa określonych przez Dostawcę. Nowy certyfikat jest wydawany bez zbędnej zwłoki, zazwyczaj w ciągu 2 dni roboczych od otrzymania kompletnego wniosku. Do tego czasu dostęp danego użytkownika do systemu pozostaje zablokowany.
10. Dostawca nie ponosi odpowiedzialności za szkody powstałe wskutek nieuprawnionego użycia programu z wykorzystaniem certyfikatu, którego Klient nie zgłosił w odpowiednim czasie jako utraconego, skradzionego lub nieważnego z innej przyczyny. Odpowiedzialność Dostawcy

- rozpoczyna się dopiero z chwilą możliwego do udokumentowania zgłoszenia tego faktu przez upoważnioną osobę Klienta. Dostawca zastrzega również prawo do usunięcia z ustawień użytkownika, bez uprzedzenia, każdego nieważnego, unieważnionego lub w inny sposób niezdatnego do użycia certyfikatu w celu zachowania bezpieczeństwa systemu.
11. Klient ma obowiązek na bieżąco prowadzić aktualny wykaz ważnych certyfikatów swoich użytkowników i niezwłocznie informować Dostawcę o wszystkich zmianach, które mogą wpływać na ważność certyfikatów lub uprawnienie do korzystania z nich. Obowiązek ten dotyczy w szczególności zmian organizacyjnych, rozwiązania stosunku pracy, zmian ról użytkowników oraz incydentów technicznych związanych z certyfikatami. Dostawca zablokuje dostęp do programu z użyciem danego certyfikatu w ciągu 6 godzin od zgłoszenia w dni robocze.
 12. Dostawca nie ponosi odpowiedzialności za szkody spowodowane nieuprawnionym użyciem programu z wykorzystaniem takiego certyfikatu do chwili zgłoszenia Dostawcy jego nieważności. Dostawca zastrzega sobie również prawo do usunięcia z ustawień użytkownika nieważnego certyfikatu.
 13. Elementem początkowej konfiguracji aplikacji jest także zdefiniowanie uprawnień dostępu do wybranych czynności w programie. Wszyscy użytkownicy Klienta są przypisywani do grup zgodnie z wykonywanymi czynnościami. Do grupy „00” (administrator aplikacji) mogą należeć wyłącznie pracownicy Dostawcy oraz certyfikowani administratorzy spośród użytkowników Klienta. Użytkownicy nieprzypisani do grupy „00” nie mają dostępu do wybranych formularzy i stron.
 14. Klient może połączyć aplikację z zewnętrznym repozytorium obrazów lub dokumentów, pod warunkiem że są one przechowywane w zasobach ogólnodostępnych z internetu.
 15. Masowy eksport i import danych z aplikacji lub do niej może wykonywać wyłącznie Dostawca w ramach odrębnej usługi. Aplikację można również połączyć za pomocą zdefiniowanego interfejsu (np. usług internetowych lub API) z aplikacjami zewnętrznymi (np. sklepami internetowymi innych dostawców albo programem ESO9 Prodejna) lub wewnętrznymi (np. aplikacjami do terminali magazynowych, systemem zamówień ESO9 albo aplikacją ESO9 Tablet).
 16. Dostawca jest uprawniony do ograniczenia liczby rekordów wyświetlanych użytkownikowi, który nadmiernie obciąża program żądaniami wyświetlenia dużej ilości danych.
 17. Dostawca zastrzega sobie prawo do ograniczenia dostępu do aplikacji, jeżeli istnieją nieuregulowane należności przeterminowane o ponad 30 dni. W pierwszej kolejności w aplikacji zostanie wyświetlone ostrzeżenie widoczne dla wszystkich użytkowników. Jeżeli opóźnienie w płatności będzie się utrzymywać, Dostawca może podjąć dalsze działania, w tym czasowo zablokować dostęp do systemu do czasu uregulowania należnej kwoty.

5. Usługa Hotline

1. Usługa Hotline jest dostępna pod numerem telefonu +420 228 809 001, za pośrednictwem portalu <https://podpora.eso.cz> lub pocztą elektroniczną pod adresem podpora@eso9.cloud.
2. Usługa Hotline jest dostępna w dni robocze od godz. 8:00 do 16:00.
3. Kontaktując się telefonicznie z usługą Hotline, użytkownik ma obowiązek podać następujące dane identyfikacyjne:
 - a. nazwę firmy Klienta,
 - b. imię i nazwisko (tożsamość) dzwoniącego użytkownika,
 - c. adres URL aplikacji, której dotyczy zgłoszenie lub incydent.

4. Informacje te są niezbędne do potwierdzenia uprawnienia do dokonania zgłoszenia i zapewnienia skutecznej obsługi przez zespół wsparcia.
5. Zgłoszenia użytkowników, ich pytania, reklamacje i uwagi są rejestrowane w wewnętrznym systemie Dostawcy. Aktualny status obsługi zgłoszeń oraz ich historię można śledzić w portalu Dostawcy pod adresem <https://podpora.eso.cz>. Dostęp wymaga rejestracji. Czas reakcji określa umowa o świadczenie usług aplikacyjnych.

6. Tworzenie kopii zapasowych danych

1. Kopie zapasowe danych części serwerowej programu tworzy Dostawca.
2. Proces tworzenia kopii zapasowej jest uruchamiany w każdy dzień roboczy o godz. 23:00. Dienne kopie zapasowe są przechowywane przez 5 dni roboczych. Równolegle dane są również archiwizowane w cyklu tygodniowym, a kopie tygodniowe są przechowywane przez 4 tygodnie.
3. Na żądanie Klienta kopia zapasowa danych zostanie mu jednorazowo udostępniona na nośniku cyfrowym lub online — przez WWW albo FTP.
4. Każda aplikacja w ESO9 Cloud korzysta z trzech baz danych: bazy aplikacyjnej, bazy dokumentowej i bazy logów. Przez wielkość bazy danych rozumie się łączny fizyczny rozmiar bazy aplikacyjnej i dokumentowej. Baza aplikacyjna zawiera wszystkie dane utworzone przez użytkowników Klienta, natomiast baza dokumentowa — wszystkie pliki binarne zapisane przez nich w aplikacji.
5. Baza logów zawiera informacje serwisowe o wszystkich rekordach z bazy aplikacyjnej oraz o wszystkich operacjach destrukcyjnych wykonanych przez użytkowników w aplikacji ESO9 Cloud. Informacje są przechowywane w bazie logów maksymalnie przez 13 miesięcy od bieżącej daty; następnie informacje starsze niż 13 miesięcy są archiwizowane i usuwane z bazy. Na żądanie Klienta kopia zapasowa tej bazy może zostać jednorazowo udostępniona na nośniku cyfrowym lub online — przez WWW albo FTP.

7. Aplikacja testowa

1. Aplikacja testowa jest środowiskiem, w którym prowadzi się prace rozwojowe i testy w ramach wdrożenia, albo które tworzy się w celu sprawdzenia funkcji dodawanych do istniejącej aplikacji. Może być również wykorzystywana do szkolenia użytkowników.
2. Aplikację testową tworzy się tylko na niezbędny okres i do celów wskazanych w art. 7 ust. 1.
3. Dostawca może ją automatycznie usunąć, jeżeli nie była używana przez ponad 30 dni. Może ją również usunąć, jeżeli nie służy celom określonym w art. 7 ust. 1.
4. Aplikacja testowa działa w środowisku testowym oddzielnym od produkcyjnych baz danych.
5. Testowe bazy danych nie są standardowo objęte planami tworzenia kopii zapasowych ani pracami konserwacyjnymi baz danych.
6. Ponieważ jest to środowisko testowe, Dostawca może w każdej chwili, bez uprzedzenia, przerwać jego działanie na niezbędny okres.
7. Koszt eksploatacji aplikacji testowej nie jest wliczony w cenę eksploatacji.

8. Odtwarzanie danych z kopii zapasowych

Dostawca odtwarza dane z kopii zapasowych z dwóch powodów:

1. W związku z usuwaniem skutków sytuacji niestandardowych (awarii, usterek itp.)
 - a) Odtworzenie danych proponuje zazwyczaj Dostawca, który zwraca się telefonicznie lub e-mailem do upoważnionej osoby Klienta o zgodę na odtworzenie danych.
 - b) Upoważniona osoba Klienta udziela pisemnej zgody na odtworzenie danych i przesyła ją e-mailem lub pocztą.
 - c) Okres oczekiwania na zgodę upoważnionej osoby nie jest wliczany do czasu przewidzianego na usunięcie usterek, po którego upływie mogą zostać naliczone odpowiednie kary.
2. Na wyraźne żądanie Klienta
 - a) o odtworzenie danych może wystąpić wyłącznie upoważniona osoba Klienta albo bezpośrednio organ statutowy Klienta.
 - b) Wniosek o odtworzenie danych należy przesłać Dostawcy do usługi Hotline w formie pisemnej, e-mailem lub pocztą.
 - c) Wniosek musi zawierać datę, na którą dane mają zostać odtworzone, planowany termin odtworzenia, datę złożenia wniosku, aktualne dane kontaktowe umożliwiające weryfikację oraz podpis osoby upoważnionej. Wniosek niezawierający tych elementów uznaje się za nieważny.
 - d) Dostawca rozpocznie odtwarzanie danych w żądanym terminie, jednak nie później niż w ciągu 24 godzin w dni robocze od otrzymania wniosku. Czas odtwarzania zależy od ilości danych.
 - e) Podczas odtwarzania danych część serwerowa programu będzie niedostępna dla użytkowników. Okresu tego nie uznaje się za niedostępność programu w rozumieniu art. 3 ust. 1 umowy.
 - f) o zakończeniu odtwarzania danych Dostawca poinformuje upoważnioną osobę Klienta telefonicznie, a następnie potwierdzi tę informację e-mailem.

9. Aktualizacja programu

1. Aktualizację programu przeprowadza się w celu uwzględnienia zmian w przepisach oraz doskonalenia jego funkcji, zazwyczaj dwa razy w roku.
2. Dostawca poinformuje Klienta o terminie planowanej instalacji aktualizacji z odpowiednim wyprzedzeniem, pocztą elektroniczną lub poprzez opublikowanie tej informacji na stronie startowej aplikacji.
3. Dostawca poinformuje Klienta o wydaniu aktualizacji i jej zawartości pocztą elektroniczną, wysyłając wiadomość na adres upoważnionej osoby Klienta.
4. Podczas instalowania aktualizacji część serwerowa programu będzie niedostępna dla użytkowników. Okresu tego nie uznaje się za niedostępność programu w rozumieniu art. 3 ust. 1 umowy.
5. Dostawca poinformuje upoważnioną osobę Klienta o zakończeniu instalowania aktualizacji, wysyłając potwierdzenie e-mailem albo usuwając informację o trwającej aktualizacji ze strony startowej aplikacji.
6. Jeżeli aktualizacja, poza zmianami wynikającymi z przepisów, zawiera nowe lub ulepszone funkcje, Klient może zamówić ich udostępnienie za pośrednictwem Hotline. Usługa ta nie jest objęta miesięcznymi opłatami określonymi w umowie i jest rozliczana zgodnie z aktualnym cennikiem Dostawcy.