Deklaracja gwarantowanego poziomu świadczenia usług (SLA)

dotyczy komponentu COTS

**Definicje**

Ilekroć poniższe pojęcia zostaną napisane w Deklaracji wielką literą, Strony nadają im znaczenie wskazane w definicjach:

* **Awaria –** jest to taki stan Systemu Informatycznego, w którym Użytkownik nie jest w stanie połączyć się do Systemu.
* **Dostawca usług –** LekSeek Polska
* **Czas Reakcji –** czas jaki upłynął od momentu otrzymania Zgłoszenia przez Dostawce Usług do momentu przyjęcia Zgłoszenia do realizacji.
* **Czas usunięcia awarii/usterki –** czas jaki upłynął od przyjęcia Zgłoszenia do realizacji do usunięcia awarii/usterki.
* **Oprogramowanie –** komponent COTS
* **Partner Projektu** – Licencjonobiorca
* **Priorytet Usterki -** Rozróżnia się kilka priorytetów w zakresie zgłoszeń dotyczących Usterek których lista wraz z definicjami została opisana w Załączniku nr 2 do niniejszej Deklaracji.
* **Serwis –** gwarantowane przez Dostawcę usług w ramach wsparcia technicznego oraz utrzymania Systemu Informatycznego. Szczegółowy zakres i parametry wyżej wymienionych usług oraz procedury realizacji Serwisu zostały opisane w paragrafie 3 niniejszej Deklaracji
* **Service Level Agreement (SLA) lub Deklaracja –**, deklaracja  gwarantowanego poziomu usług, która obejmuje gwarancje w pełnym spektrum: od zakresu i sposobu świadczenia usług (w tym np. sposób dokumentowania prac), poprzez parametry usług (czasy dostępności, czasy reakcji, częstotliwość wykonywania), aż po kwestie związane z bezpieczeństwem.
* **System Informatyczny –** system informatyczny złożony z Oprogramowania, oprogramowania firm trzecich, sprzętu komputerowego oraz innych urządzeń wymaganych do poprawnej pracy Oprogramowania.
* **Usługa -** całość serwisów udostępnianych na serwerze WWW, uruchamianych z przeglądarki WWW.
* **Usterka -** działanie systemu niezgodne zspecyfikacją funkcjonalności na chwilę bieżącą.
* **Użytkownik –** osoba używająca komponentu COTS na podstawie zawartej licencji (lekarz, personel medyczny, pielęgniarka, położna, personel administracyjny)
* **Zgłoszenie –** informacja o Usterce lub Awarii w pracy Systemu Informatycznego przekazana przez Użytkownika/Partnera Projektu do Dostawcy Usług.

**Przedmiot Deklaracji**

# Zgodnie z niniejszą Deklaracją Dostawca Usług zobowiązuje się świadczyć na rzecz Użytkownika/Partnera usługi Serwisu, związane z obsługą komponentu COTS

# Dostawca Usług oświadcza, że posiada wymagane uprawnienia do wykonywania prac określonych w niniejszej Umowie, a także odpowiednią wiedzę i doświadczenie w tym zakresie.

1. Dostawca Usług zobowiązuje się do realizacji niniejszej Deklaracji zgodnie   
   z najlepszą wiedzą, zachowaniem należytej staranności profesjonalisty oraz rzetelnie   
   i terminowo. Dostawca Usług oświadcza, że posiada wszelkie wymagane przepisami prawa uprawnienia, zezwolenia i zgody na realizację niniejszej Deklaracji.
2. Dostawca Usług może powierzyć osobom trzecim wykonanie części lub całości prac, będących przedmiotem niniejszej Deklaracji podwykonawcom jedynie po uzyskaniu uprzedniej, pisemnej zgody Zamawiającego. Dostawca Usług odpowiedzialny jest za działania oraz zaniechania działania osób trzecich, z których pomocą, świadczy lub świadczył usługi na rzecz Zamawiającego jak za własne działania oraz zaniechania działań.

**Zakres usług i parametry obsługi Serwisu (SLA)**

**I. Monitorowanie.**

Dostawca usług monitoruje działanie usług w trybie 24/7. Usługi są monitorowane automatycznie. Zgłoszenia wykrytych awarii są zgłaszane do dyżurującego administratora. Administrator podejmuje działania od razu po otrzymaniu informacji o awarii.

**II. Kanały zgłaszania awarii i usterek.**

1. Dostawca usług udostępnia co najmniej 3 niezależne kanały zgłaszania awarii. Kanałami tymi w szczególnością są:
   1. E-mail
   2. telefon
2. Dostawca usług zapewnia przechowywanie wszystkich zgłoszeń oraz jednoznaczne oznaczenie statusu każdego zgłoszenia.
3. Wszystkie usterki trafiające do systemu otrzymują priorytet.
4. Partner projektu (Licencjonobiorca) posiada ciągły wgląd do ewidencji zgłoszeń oraz może wpływać na zmianę priorytetu.
5. Zgłoszenia, które dotyczą tego samego problemu mogą być łączone w jeden wpis.

**III. Czas reakcji i działań naprawczych.**

1. Jako czas reakcji rozumie się czas od pojawienia się zgłoszenia do momentu sklasyfikowania zgłoszenia (jako Awaria lub Usterka) i przypisania Priorytetu.
2. Dostawca usługi gwarantuje następujące czasy reakcji na zgłoszenia:

|  |  |
| --- | --- |
| Dni powszednie od 6:00 – 20:00 | 5 minut |
| Dni powszednie – pozostałe godziny i soboty | 10 minut |
| Dni ustawowo wolne od pracy | 30 minut |

**IV. Łączny czas awarii i usterek.**

1. Dostawca usług gwarantuje, że łączny czas w ciągu roku kalendarzowego nie przekroczy:

|  |  |
| --- | --- |
| Awarie | 48 godziny |
| Usterki poziom Krytyczny | 72 godziny |
| Usterki poziom Istotny | 21 dni |

1. Jako łączny czas uważa się sytuacje, w której jest otwarte co najmniej jedno zlecenie danego typu.

**V. Okna serwisowe.**

1. Dostawca usług rezerwuje przedziały czasu na operacje serwisowe w obrębie usługi. Operacje serwisowe mogą prowadzić do czasowego wyłączenia części usług. Czas prowadzenia operacji serwisowych nie wlicza się do czasu niedostępności usług.
2. Dostawca każdorazowo informuje użytkowników o przewidywanych przerwach serwisowych co najmniej 12h przed ich wystąpieniem.
3. Dostawca ustala następujące okna serwisowe:

|  |  |
| --- | --- |
| Codziennie | Od 2:00 do 2:01 |
| Raz w tygodniu | W dzień ustawowo wolny od pracy od 2:01 do 2:05 |
| Raz w miesiącu | W dzień ustawowo wolny od pracy od 2:05 do 2:15 |
| Raz na kwartał | W dzień ustawowo wolny od pracy od 2:15 do 2:45 |

Przerwa techniczna może oznaczać przerwanie wszystkich sesji, automatyczne wylogowanie użytkowników. Odpowiedzialność w zakresie przygotowania się do przerwy technicznej po stronie użytkowników leży w gestii użytkowników.

**VI. Wyjątki i wyłączenia.**

1. Dostawca usług nie ponosi odpowiedzialności za elementy nie będące częścią jego infrastruktury. W szczególności Dostawca usług nie ponosi odpowiedzialności za wadliwe działania, sprzętu i oprogramowania u użytkownika oraz infrastruktury sieciowej użytkownika (dostawca Internetu). W skład tych elementów wchodzą między innymi:
   1. Drukarki
   2. Przeglądarki internetowe (Dostawca usług nie ponosi odpowiedzialności za błędy w przeglądarkach oraz używanie przeglądarek spoza listy zalecanych przeglądarek)
   3. Działanie programów antywirusowych.
   4. Działanie pluginów, rozszerzeń, motywów instalowanych w przeglądarce internetowej.

**Jakość i gwarancja**

# Jakość świadczonych usług, szybkość reakcji na zgłoszenia, jasno zdefiniowane procedury, a także dobra organizacja serwisu i przepływu informacji gwarantowane jest przez wdrożony w Zespole Dostawcy Usług - System Zarządzania Usługami IT zgodny z normą ISO/IEC 20000.

# Dostawca usług gwarantuje prowadzenie obsługi serwisowej Systemu Informatycznego w sposób minimalizujący powstawanie Awarii i Usterek oraz usuwanie uszkodzeń w możliwie najkrótszym czasie, jednak nie dłuższym niż wskazany w Par 3 niniejszej Deklaracji, w celu utrzymania parametrów niezawodności Systemu Informatycznego.

# Naprawa Oprogramowania polega na modyfikacji Oprogramowania Dostawcy Usług powodującej usunięcie Awarii/Usterki lub na podaniu procedury pozwalającej uniknąć Awarii/Usterki według zgodnej decyzji Dostawcy Usług i Użytkownika/Partnera Projektu. Szczegółowe procedury postępowania zostaną określone w odrębnym dokumencie.

# Oprogramowanie Firm Trzecich, wchodzące w skład Systemu Informatycznego, będzie gwarantowane zgodnie z warunkami producenta lub innego dostawcy. Dostawca Usług nie ponosi odpowiedzialności za niewywiązanie się podmiotów trzecich z warunków wspomnianego wsparcia.

# Gwarancje opisane w tym paragrafie stanowią wyłączne zobowiązania Dostawcy Usług przysługujące Użytkownikowi z tytułu niniejszej Deklaracji czy też z innego tytułu (np. przepisów prawnych).

**Siła wyższa**

1. Strony nie ponoszą odpowiedzialności za niewykonanie lub nienależyte wykonanie Deklaracji spowodowane siłą wyższą tj. zdarzeniem nagłym, zewnętrznym, nieprzewidywalnym i niezależnym od woli Stron powstałym po zawarciu Umowy, któremu nie można zapobiec, ani przeciwdziałać przy zachowaniu należytej staranności Stron. Przejawami siły wyższej są w szczególności:

* klęski żywiołowe, w tym pożar, powódź, susza, trzęsienie ziemi, huragan, sadź;
* długotrwałe awarie zasilania, których usunięcie nie zależy od żadnej ze Stron Umowy;
* akty władzy państwowej, w tym stan wojenny, stan wyjątkowy, embarga, blokady itp.;
* działania wojenne, akty sabotażu; akty terroru;
* strajki powszechne, nie obejmujące personelu Stron.

1. Strona, która nie jest w stanie wykonać swoich zobowiązań z przyczyn stanowiących okoliczność siły wyższej niezwłocznie zawiadomi druga Stronę o takiej okoliczności i jej ustaniu.

**Bezpieczeństwo i Data Center**

1. Dostawca Usług informuje, że w Zespole Serwisu Dostawcy Usług wdrożony jest System Zarządzania Bezpieczeństwem (SZB) opracowany w zgodzie z normą ISO/IEC 27001.
2. Oferowane rozwiązania są skalowalne i posiadają fizyczne adresy na terenie UE
3. Nasze środowiska są budowane na platformach posiadających certyfikat ISO 27001 (bezpieczeństwo).
4. Wszystkie zasoby posiadają gwarancję 99,1% dostępności.
5. W przypadku archiwizacji i przestrzeni dyskowej, gwarantujemy niezawodność (trwałość) na poziomie 99,5% dla umieszczonych plików:
   1. Replikacja wielu stron;
   2. Kontrolowanie integralności plików;
   3. Przenoszenie tylko poprzez bezpieczne protokoły;
   4. Wymiana uszkodzonych zasobów w kilka minut.
6. Każdy element wchodzący w skład infrastruktury jest dedykowany. Oznacza to, wirtualne maszyny na fizycznych serwerach (hostach).
7. Każdy element infrastruktury jest redundantny. Zasilacze w serwerach, podłączenia elektryczne, przestrzeń dyskowa, routery, switche mają podwójną konfigurację i korzystają z dwóch systemów zasilających. Pozwala to na zapewnienie poziomu usługi bliskiego 100%.
8. Ochrona Fizyczna serwerów:
   1. Aby uniknąć włamań, każda strefa jest zabezpieczona ogrodzeniami wyposażonymi w drut kolczasty.
   2. System video monitoringu i wykrywania ruchu. Czynności wykonywane w centrach danych i poza budynkami są monitorowane i rejestrowane na zabezpieczonych serwerach.
   3. Zespoły monitorujące są dostępne 24/24, 7/7.
   4. Aby kontrolować i monitorować dostęp na teren, zostały uruchomione ścisłe procedury bezpieczeństwa. Każdy członek personelu jest wyposażony w indywidualny identyfikator RFID, do którego są przypisane jego uprawnienia. Uprawnienia te są regularnie sprawdzane.
9. Serwerownie korzystają z jeszcze bardziej zaawansowanej ochrony, ponieważ dostęp tu ma tylko uprawniony personel.
10. Każda sala w każdym centrum danych jest wyposażona w system wykrywania i gaszenia pożarów jak również w drzwi przeciwpożarowe. Wdrożona jest reguła APSAD R4 dotyczącą instalowania przenośnych gaśnic i posiada certyfikat zgodności N4 dla wszystkich serwerowni.
11. Centra danych są zasilane przez dwa niezależne podłączenia elektryczne i są również wyposażone w zasilacze. Grupy zasilające o wytrzymałości 48 godzin pozwalają na uniknięcie ewentualnej awarii sieci elektrycznej.
12. Certyfikaty bezpieczeństwa Data Center:
    1. certyfikat ISO 27001:2005 dla rozwiązań Dedicated Cloud;
    2. Standard ten potwierdza uruchomienie organizacji bezpieczeństwa;
    3. Poziom bezpieczeństwa usługi Dedicated Cloud został również uznany poprzez certyfikaty SOC 1 typ I (SSAE 16 i ISAE 3402) i SOC 2 typ I;
    4. Te międzynarodowe certyfikaty gwarantują wprowadzenie i skuteczność wewnętrznych kontroli związanych z bezpieczeństwem systemu informacji