Załącznik nr 1- Usługi Utrzymania

1 Zakres Usług Utrzymania

Usługami Utrzymania objęte są wszystkie elementy Systemu CPD CANARD będącego własnością Zamawiającego oraz wszystkie elementy Systemu CPD CANARD dostarczone przez Wykonawcę w ramach Usług Rozwoju. Wykonawca świadczy Usługi Utrzymania Systemu, w zakresie podanym poniżej:

1.1 Zarządzanie ciągłością działania
1.2 Utrzymanie Działania Operacyjnego
1.3 Zarządzanie poziomem usług
1.4 Zarządzanie zasobami (pojemnością)
1.5 Service Desk
1.6 Zarządzanie Incydentami
1.7 Zarządzanie Problemami
1.8 Zarządzanie zmianami
1.9 Zarządzanie konfiguracją i Bazą Wiedzy
1.10 Zarządzanie bezpieczeństwem
1.11 Wykonywanie przeglądów Oprogramowania Użytkowego pod kątem planowania zmian
1.12 Aktualizacja Oprogramowania Obcego
1.13 Usprawnienie infrastruktury

2 Zarządzanie ciągłością działania

2.1 Celem usługi Zarządzania ciągłością działania jest przygotowanie i utrzymywanie w ciągłej gotowości narzędzi i zasobów na użytek ewentualnych awarii godzących w podstawowe funkcje Systemu oraz usuwanie skutków tych awarii w możliwie najkrótszym czasie.

2.2 Wykonawca będzie świadczyć usługę zarządzania ciągłością działania poprzez:

2.2.1 Analizę wpływu – przewidywanie wpływu Awarii całości Systemu lub jego części na realizację procesów biznesowych Użytkowników,

2.2.2 Ocenę ryzyka – określanie prawdopodobieństwa wystąpienia Awarii,

2.2.3 Podejmowanie działań zmierzających do minimalizacji ryzyka wystąpienia Awarii,

2.2.4 Utrzymywanie i aktualizację procedur wykonywania kopii zapasowych oraz odtwarzania z kopii zapasowych w przypadku wystąpienia Awarii, dla wszystkich wymaganych elementów konfiguracji, wymagającej przywrócenia ciągłości działania Systemu poprzez odtworzenie z kopii zapasowej,

2.2.5 Realizację planów testów procedur odtwarzania z kopii zapasowych oraz przygotowanie miesięcznych raportów z wykonanych testów, zawierających informację o wykonanych testach, ich wynikach, wnioskach i rekomendacjach z nich wynikających,

2.2.6 Utrzymywanie polityki kopii zapasowych dla Systemu CPD CANARD, poprzez jej weryfikację raz na pół roku oraz wprowadzenie ewentualnych aktualizacji wynikających ze zmian wprowadzonych w Systemie, w dokumentacji oraz

dostosowanie do wymagań, oczekiwań oraz możliwości technicznych Zamawiającego,

2.2.7 Utrzymywanie planu ciągłości działania (BCP) dla Systemu CPD CANARD, poprzez wykonywanie raz na pół roku analizy wpływu oraz ocenę ryzyka. Przeglądy raz na pół roku planu BCP, w wyniku wprowadzonych zmian w Systemie i zmian organizacyjnych u Zamawiającego.

2.2.8 Identyfikowanie potrzeb usprawnienia działania lub wymiany Infrastruktury Sprzętowej.

2.3 W raportach miesięcznych Wykonawca będzie przedstawiał informacje o stanie realizacji poszczególnych aktywności zdefiniowanych dla usługi zarządzania ciągłością działania.

3 Utrzymanie Działania Operacyjnego

3.1 Wykonawca będzie świadczyć usługę Utrzymania Działania Operacyjnego poprzez:

a. Obsługę zgłoszeń przekazywanych przez Service Desk,
b. Opracowanie, przegląd i aktualizacja Dokumentacji Systemu CPD CANARD.
c. Administrowanie, konfigurację, strojenie i monitorowanie Infrastruktury teleinformatycznej,
d. Wdrażanie zmian w konfiguracji Infrastruktury teleinformatycznej,
e. Aktualizację konfiguracji Systemu w przypadku wymiany przez Zamawiającego elementów Infrastruktury teleinformatycznej,
f. Utrzymanie dokumentacji eksploatacyjnej Systemu,
g. Realizację procedur eksploatacyjnych (operacyjnych), obejmujących m.in:

- Obsługę kopii zapasowych i ich odtwarzanie,
- Monitorowanie Infrastruktury teleinformatycznej,
- Monitorowanie poziomu świadczonych usług (SLA),
- Monitorowanie poprawności działania usług Systemu,
- Nadzór nad dostępem do zasobów Systemu,
- Dodawanie i modyfikację kont i uprawnień w Systemie.

3.2 Wykonawca jest zobowiązany do utrzymywania i aktualizowania procedur związanych z bieżącym utrzymaniem Systemu, obejmujących obszary m.in:

a. Organizacji pracy operatorów i administratorów (obowiązki wynikające z trybu zmianowego, rejestrowanie wykonywanych aktywności),
b. Rozwiązywanie Incydentów i Problemów,
c. Monitorowanie działania kluczowych elementów Systemu,
d. Wykonywanie kopii zapasowych elementów Systemu,
e. Odtwarzania z kopii zapasowych w przypadku Awarii,
f. Wprowadzanie zmian w Systemie,
g. Postępowanie w sytuacjach awaryjnych,
h. Administrowanie uprawnieniami i kontami użytkowników Systemu.

3.3 W raportach miesięcznych Wykonawca będzie przedstawiał informacje o aktywnościach podjętych w ramach danego miesiąca w ramach Utrzymania

Działania Operacyjnego. Dla każdej aktywności musi być wskazany termin i wykonawca czynności.

4 Zarządzanie poziomem usług

4.1 Celem usługi Zarządzania poziomem usług jest wykonywanie oraz nadzorowanie działań służących utrzymaniu wymaganych parametrów poziomu usług Systemu CPD CANARD – w tym monitorowanie i raportowanie wartości tych parametrów.

4.2 Wykonawca będzie świadczyć usługę zarządzania poziomem usług poprzez:

a. Zarządzanie katalogiem usług świadczonych w systemie CPD CANARD, obejmującego wszystkie kluczowe funkcjonalności Systemu, poprzez jego aktualizację, przeglądy, dostosowywanie do wprowadzanych Zmian,
b. Dotrzymywanie wymagań na poziom usług systemu (SLA). Na SLA składają się parametry dostępności, wydajnościowe i wolumetryczne,
c. Monitorowanie i raportowanie poziomu usług Systemu do Zamawiającego,
d. Zapewnienie Wydajności i Dostępności usług przy określonej Wolumetrii zgodnie z poziomem określonym w katalogu usług.
e. Identyfikowanie potrzeb usprawnienia działania lub wymiany Infrastruktury teleinformatycznej.
f. Prowadzenie logu (dziennika) SLA, w którym będą rejestrowane wszystkie wywołania (transakcje), związane z usługami Systemu CPD CANARD, na podstawie, którego będzie można jednoznacznie wyznaczyć wolumetrię usług, średni i maksymalny czas odpowiedzi. Log SLA powinien zawierać:

- Identyfikator transakcji,
- Kod usługi, funkcji,
- Czas rozpoczęcia i zakończenia transakcji,
- Datę rejestracji w logu SLA,
- Czas trwania transakcji,
- Ilość zwracanych rekordów,
- Identyfikator użytkownika wywołującego usługę.

4.3 W raportach miesięcznych Wykonawca będzie przedstawiał informacje umożliwiające weryfikację przez Zamawiającego czy dotrzymywany jest poziom usług systemu (SLA) wyrażony parametrami na dostępność, wydajność i wolumetrię, wyjaśnienie przekroczeń parametrów SLA, działania podjęte w celu zapobiegania przekroczeniom w przyszłości.

4.4 Wykonawca udostępni narzędzie umożliwiające samodzielną weryfikację poziomu usług Systemu przez Zamawiającego.

5 Zarządzanie zasobami (pojemnością)

5.1 Celem usługi Zarządzania zasobami (pojemnością) jest monitorowanie zdolności produkcyjnych poszczególnych elementów konfiguracji (Infrastruktury teleinformatycznej) oraz przygotowywanie analiz i prognoz, co do wykorzystania i

ewentualnej rozbudowy zasobów Systemu, w celu zapewnienia wymaganego aktualnego i przyszłego poziomu usług.

5.2 Wykonawca będzie świadczyć usługę zarządzania zasobami (pojemnością) poprzez:

a. Monitorowanie i ewidencjonowanie określonych parametrów Systemu (np. CPU, RAM, I/O, zasoby dyskowe, itp.),
b. Analizę danych pochodzących z monitorowania pod kątem trendów i odchyleń od przewidywań w celu prognozowania wykorzystania zasobów i potrzeb produkcyjnych. Analiza będzie wykonywana raz w miesiącu a jej wynikiem powinien być raport, który będzie zawierał informacje o bieżącym wykorzystaniu zasobów, prognozach wykorzystania w następnym miesiącu oraz perspektywie kwartału i roku,
c. Strojenie elementów Systemu w celu lepszego wykorzystania zasobów. Aktywności związane ze strojeniem będą wykonywane nie rzadziej niż raz na kwartał i muszą być poparte przygotowaną analizą. Aktywności związane ze strojeniem będą raportowane raz na miesiąc. Raporty muszą zawierać:
   - informacje umożliwiające weryfikację przez Zamawiającego, jakie elementy Systemu były strojone,
   - wyjaśnienie, jakie rezultaty zostały osiągnięte w wyniku strojenia,
   - wskazanie, czy wymagane są dalsze działania zmierzające do lepszego wykorzystania zasobów,
d. Podejmowanie działań w celu zapewnienia wymaganych zasobów Systemu poprzez obsługę Incydentów, Problemów i Zmian.

5.3 W raportach miesięcznych Wykonawca będzie przedstawiał informacje o wykorzystaniu zasobów Systemu, na podstawie danych z narzędzi monitorowania. Raporty muszą zawierać informacje umożliwiające weryfikację przez Zamawiającego stopnia wykorzystania zasobów Systemu dziennego w danym miesiącu oraz miesięcznego w roku.

6 Service Desk

6.1 Celem usługi Service Desk jest przyjmowanie i rejestracja wszystkich zgłoszeń od użytkowników Systemu za pomocą określonych kanałów komunikacji oraz ich obsługa lub przekazywanie do odpowiednich linii wsparcia.

6.2 Wykonawca będzie świadczył usługę Service Desk poprzez:

a. Przyjmowanie i rejestrację wszystkich Zgłoszeń od użytkowników Systemu zgłaszanych telefonicznie, pocztą elektroniczną lub za pośrednictwem elektronicznego systemu zgłoszeń HP Service Manager,
b. Wstępną klasyfikację zgłoszeń na:
   - Incydenty dotyczące Oprogramowania Użytkowego,
   - Incydenty dotyczące Oprogramowania Obcego,
   - Incydenty dotyczące Infrastruktury teleinformatycznej,
   - Zgłoszenia w ramach Usługi Rozwoju Systemu,
   - Zgłoszenia inne (niebędące incydentami, np. zapytanie o działanie usługi).

c. Wstępne nadawanie priorytetów zgłoszeń zgodnie z kryteriami opisanymi w parametrach jakościowych,
d. Przekazanie zgłoszenia do właściwego zespołu wsparcia lub podmiotów zewnętrznych w tym w szczególności serwisujących Oprogramowanie Obce, , Infrastrukturę teleinformatyczną lub systemy zewnętrzne,
e. Potwierdzenie użytkownikowi przekazującemu zgłoszenie faktu jego przyjęcia i przekazania do właściwego zespołu wsparcia lub podmiotu zewnętrznego
f. Koordynowanie obsługi zgłoszeń w ramach zespołu wytwórczego oraz dostawców zewnętrznych,
g. Eskalowanie w przypadku przekroczenia czasu obsługi,
h. Informowanie użytkowników o statusie Zgłoszenia,
i. Informowanie użytkowników o przerwach w działaniach Systemu i zmianach,
j. Potwierdzanie z użytkownikiem rozwiązania i zamykanie zgłoszeń.

6.3 Czas Reakcji na zgłoszenie od użytkowników nie może być dłuższy niż 1 godzina, niezależnie od priorytetu zgłoszenia.

6.4 Czas Reakcji jest liczony od przekazania zgłoszenia przez użytkownika do Service Desk,

6.5 Czas Reakcji obejmuje czynności opisane w 6.2 lit. a. – e. i kończy się potwierdzeniem przekazania sklasyfikowanego zgłoszenia do właściwego zespołu wsparcia lub podmiotów zewnętrznych.

6.6 Wykonawca przygotuje dla użytkowników Systemu procedurę sposobu przekazywania i zakresu informacyjnego zgłoszeń przekazywanych do Service Desk.

6.7 Wykonawca świadcząc usługę Service Desk będzie przyjmował zgłoszenia od Interesantów zarejestrowanych w Elektronicznym Biurze Obsługi Klienta (eBOK).

6.8 W raportach miesięcznych Wykonawca będzie przedstawiał detaliczną listę zgłoszeń od użytkowników, które nie zostały zakwalifikowane, jako Incydenty, a dotyczą Usług Rozwoju Systemu.

7 Zarządzanie Incydentami

7.1 Celem usługi Zarządzania Incydentami jest utrzymanie lub przywracanie normalnego, zgodnego z dokumentacją działania Usług Systemu poprzez przyjmowanie, klasyfikowanie, ewidencjonowanie i usuwanie skutków Incydentów, a także identyfikowanie Problemów oraz monitorowanie i raportowanie parametrów obsługi Incydentów.

7.2 Wykonawca będzie świadczył usługę zarządzania Incydentami poprzez:
a. Wykrywanie Incydentów w Systemie CPD CANARD,
b. Klasyfikację Incydentów,
c. Analizę i diagnozę Incydentów,
d. Opracowanie rozwiązania Incydentów,
e. Przywracanie funkcjonalności Systemu, poprzez zastosowanie docelowego rozwiązania lub Obejścia.

7.3 W raportach miesięcznych Wykonawca będzie przedstawiał detaliczną informację o Incydentach, które były w obsłudze. O każdym Incydencie musi być przynajmniej następujący zakres informacji:

a. unikalny identyfikator,
b. opis,
c. data rejestracji,
d. priorytet,
e. diagnoza,
f. rozwiązanie,
g. data rozwiązania,
h. czas naprawy,
i. wyjaśnienia, wnioski i rekomendacje w przypadku przekroczenia Czasu Naprawy.

7.4 Incydent będzie traktowany, jako rozwiązany w przypadku, kiedy zostanie przywrócona funkcjonalność Systemu sprzed wystąpienia Incydentu, poprzez jego docelowe rozwiązanie (usunięcie przyczyn występowania) lub poprzez zastosowanie Obejścia (zastosowanie rozwiązania, które pozwala na realizację funkcji biznesowych przez użytkownika, w sposób inny niż opisany w dokumentacji Systemu).

7.5 Wykonawca będzie przestrzegał wymagania bezpieczeństwa dla systemów, danych oraz zapewni ochronę danych osobowych w procesie obsługi Incydentu w zakresie przekazywania danych z Systemu pomiędzy Zamawiającym a Wykonawcą, wymaganych do rozwiązania Incydentu, które będą zwierały informacje niejawne.

8 Zarządzanie Problemami

8.1 Celem usługi Zarządzania Problemami jest utrzymanie lub przywracanie normalnego, zgodnego z dokumentacją działania usług Systemu poprzez identyfikowanie, przyjmowanie, klasyfikowanie, ewidencjonowanie i usuwanie skutków Problemów oraz monitorowanie i raportowanie obsługi Problemów.

8.2 Wykonawca będzie świadczyć usługę zarządzania problemami poprzez:

a. Identyfikację, rejestrację i klasyfikację Problemów,
b. Rozwiązywanie Problemów poprzez usunięcie Incydentów na podstawie, których Problem został zidentyfikowany lub zniwelowanie zagrożenia wystąpienia Incydentów, na podstawie, których Problem został zidentyfikowany.

8.3 W raportach miesięcznych Wykonawca będzie przedstawiał detaliczną informację o stanie obsługi Problemów. O każdym Problemie musi być przynajmniej następujący zakres informacji:

a. unikalny identyfikator,
b. opis,
c. data rejestracji,
d. priorytet,

e. diagnoza,
f. rozwiązanie,
g. data rozwiązania,
h. czas naprawy,
i. wyjaśnienia, wnioski i rekomendacje w przypadku przekroczenia czasu naprawy.

9 Zarządzanie zmianami

9.1 Celem usługi zarządzania zmianami jest przyjmowanie, klasyfikowanie i ewidencjonowanie wniosków o zmianę oraz nadzorowanie wszystkich etapów wprowadzania zmiany, tak, aby utrzymać spójność oraz wymagane parametry użytkowe Systemu.

9.2 Wykonawca będzie traktował, jako zmianę każdą modyfikację Oprogramowania Użytkowego, konfiguracji, Oprogramowania Obcego oraz Infrastruktury teleinformatycznej Systemu CPD CANARD.

9.3 Wykonawca będzie świadczyć usługę zarządzania zmianami w Systemie CPD CANARD, wynikającymi z obsługi Incydentów, Problemów, strojenia Systemu, przeglądów Oprogramowania Użytkowego, aktualizacji Oprogramowania Obcego, modyfikacji danych w bazie danych Systemu, modyfikacja spraw w Systemie, zasilania danymi dostarczonymi przez Zamawiającego itp. poprzez:

a. Planowanie wprowadzania zmian.
b. Rejestrację i klasyfikację wniosków o zmianę,
c. Ocenę zmiany (analiza wpływu na system),
d. Uzyskanie akceptacji zmiany przez Zamawiającego,
e. Przygotowanie i opracowanie zmiany,
f. Wdrożenie zmiany w Systemie,
g. Przygotowywanie i udostępnianie Zamawiającemu tygodniowych (do wtorku) i miesięcznych (do 5 dnia roboczego miesiąca), raportów z obsługiwanych zmian. Raporty muszą zawierać informacje umożliwiające weryfikację przez Zamawiającego skutków wprowadzonych zmian, wnioski i rekomendacje z przeprowadzonych zmian,
h. Przygotowanie i wdrożenie procedur zarządzania zmianą.

9.4 W raportach miesięcznych Wykonawca będzie przedstawiał detaliczną informację o stanie obsługi zmian. O każdej zmianie musi być przynajmniej następujący zakres informacji:

a. unikalny identyfikator,
b. opis,
c. priorytet
d. ocena zmiany (analiza wpływu na System),
e. data akceptacji i osoba akceptująca po stronie Zamawiającego,
f. data wprowadzenia zmiany do Systemu,
g. ocena skutków wprowadzenia zmiany,

h. wnioski i rekomendacje w przypadku negatywnych skutków wprowadzenia zmiany.

9.5 Wykonawca opisując procedury zarządzania zmianami określi czasy trwania poszczególnych kroków procesu, z uwzględnieniem opiniowania i akceptacji zmian wdrażanych na Środowisko Produkcyjne przez Zamawiającego, z wykorzystaniem zintegrowanego narzędzia HP Service Manager.

9.6 Wykonawca opisując procedury zarządzania zmianami określi czas realizacji zmian dla modyfikacji danych w bazie danych Systemu, modyfikacji spraw w Systemie, zasilania danymi dostarczonymi przez Zamawiającego uwzględniając potrzeby, wymagania Zamawiającego oraz z uwzględnieniem wykorzystania poziom wykorzystania Systemu CPD CANARD przez Użytkowników, z zastrzeżeniem, że czas realizacji nie może być dłuższy niż 14 dni kalendarzowych.

10 Zarządzanie konfiguracją i bazą wiedzy

10.1 Celem usługi Zarządzania konfiguracją i Bazą Wiedzy jest przygotowanie projektu oraz wdrożenie Bazy Konfiguracji, obejmującej elementy konfiguracji dla oprogramowania użytkowego, Oprogramowania Obcego oraz Infrastruktury teleinformatyczną w Systemu CPD CANARD oraz udostępnianie Zamawiającemu aktualnej wiedzy o Systemie, sposobach jego budowy, utrzymania oraz o bieżącym utrzymaniu w postaci raportów, dokumentów, repozytoriów składających się na Bazę Wiedzy.

10.2 Wykonawca będzie utrzymywał i aktualizował Bazę Konfiguracji będącą w posiadaniu Zamawiającego, zawierającą elementy konfiguracji dla Oprogramowania Użytkowego, Oprogramowania Obcego i Infrastruktury teleinformatycznej Systemu,

10.3 Baza konfiguracji będzie zawierać informację o:

a. Rodzaju, liczby i konfiguracji Infrastruktury teleinformatycznej Systemu CPD CANARD,
b. Wersjach aplikacji Oprogramowania Użytkowego działających w Systemie CPD CANARD,
c. Usługach świadczonych przez System CPD CANARD (katalog usług),
d. Relacjach pomiędzy usługami a Infrastrukturą teleinformatyczną ;,
e. Grupy wsparcia, które serwisują poszczególne elementy Oprogramowania Użytkowego, Oprogramowania Obcego oraz Infrastruktury teleinformatycznej;
f. Liczbie Incydentów, Problemów i zmian związanych z danym elementem konfiguracji.

10.4 Wykonawca będzie świadczyć usługę zarządzania konfiguracją poprzez:

a. Planowanie zarządzania konfiguracją Systemu CPD CANARD,
b. Identyfikację elementów konfiguracji,

c. Zapewnienie aktualizacji danych w bazie konfiguracji, w cyklach tygodniowych, poprzez aktualizację stanu elementów konfiguracji o wprowadzone zmiany,
d. Audyt elementów Bazy Konfiguracji, wykonywany raz w miesiącu, w celu identyfikacji nieautoryzowanych zmian lub braku aktualizacji Bazy Konfiguracji mimo wykonanych zmian.

10.5 W raportach miesięcznych Wykonawca będzie przedstawiał:
a. Wyciąg z Bazy Konfiguracji zawierający listę zmienionych elementów bazy wraz z wyszczególnieniem parametrów które zostały zmienione oraz jednoznaczne powiązanie zmienianego elementu bazy z przeprowadzoną zmianą systemową (wprowadzoną pod kontrolą usługi zarządzanie zmianą),
b. Raport z audytu Bazy Konfiguracji, który będzie zawierał informacje o wykrytych niezgodnościach w Bazie Konfiguracji, podjętych działaniach i rekomendacjach mających na celu usprawnienie realizacji zarządzania konfiguracją.

10.6 Wykonawca będzie utrzymywał Bazę Wiedzy będącą w posiadaniu Zamawiającego. Usługa utrzymania Bazy Wiedzy polegać będzie na udostępnianiu Zamawiającemu aktualnej wiedzy o Systemie CPD CANARD, sposobie jego budowy, utrzymania oraz o bieżącym utrzymaniu w postaci raportów, dokumentów, repozytoriów składających się na Bazę Wiedzy. Wszelkie informacje gromadzone przez Wykonawcę w ramach realizacji Umowy są własnością Zamawiającego. Wykonawca w ramach realizacji Umowy będzie cyklicznie raz w miesiącu przekazywał Zamawiającemu informację o zmianach w Bazie Wiedzy. Na usługę utrzymania Bazy Wiedzy składają się zadania:
a. gromadzenie informacji w Bazie Wiedzy,
b. aktualizacja i udostępnianie Bazy Wiedzy w zakresie opisującym sposób budowy Systemu,
c. aktualizacja i udostępnianie Bazy Wiedzy w zakresie opisującym sposób utrzymania Systemu,
d. aktualizacja i udostępnianie Bazy Wiedzy w zakresie opisującym bieżące utrzymanie Systemu,
e. aktualizacja i udostępnianie Bazy Wiedzy o Systemie.

11 Zarządzanie bezpieczeństwem

11.1 Celem usługi Zarządzania bezpieczeństwem jest zapewnienie bezpieczeństwa Systemu zgodnie z wymaganiami zewnętrznymi i wewnętrznymi oraz świadczenie usług Systemu na poziomie określonym w SLA.

11.2 Wykonawca będzie świadczył usługę zarządzania bezpieczeństwem poprzez:
a) Weryfikację i ocenę wpływu planowanych i realizowanych Zmian na bezpieczeństwo teleinformatyczne Systemu CPD CANARD,
b) Monitorowanie zgodności działania Systemu CPD CANARD z obowiązującymi przepisami prawa dotyczącymi Krajowych Ram Interoperacyjności, RODO i Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, nie rzadziej niż raz na

rok, w tym we współpracy z Zamawiającym okresowe prowadzenie samoocen zgodności, analiz ryzyka oraz ocen skutków dla ochrony danych, oraz wsparcie w okresowych audytach, o których mowa w par. 20 ust. 2 pkt 14 KRI,

c) Bieżące monitorowanie pracy Systemu CPD CANARD pod względem bezpieczeństwa krytycznych elementów Systemu, w ramach usługi Utrzymania działania operacyjnego, w obszarach:
   - dostępności Systemu,
   - integralności logów i plików konfiguracyjnych,
   - kontroli dostępu,
   - wystąpienia błędów lub nieuprawnionych operacji,
   - stanu uruchomionych usług, również pod kątem wystąpienia usług potencjalnie niebezpiecznych,
   - przeglądanie logów systemowych,
   - występowania podatności i zagrożeń i reagowania na nie (w tym aktualizacje Oprogramowania Obcego).

d) Realizowanie zadań związanych z wprowadzeniem stopni alarmowych oraz stopni alarmowych CRP, w przypadku ich wprowadzenia:
   - ALFA-CRP
     - Prowadzenie wzmożonego monitoringu stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zalecenia Szefa ABW, ze szczególnym uwzględnieniem:
       a) monitorowania i weryfikacji ewentualnego naruszenia bezpieczeństwa komunikacji elektronicznej;
       b) sprawdzania dostępności usług elektronicznych;
       c) w razie potrzeby dokonywania zmian w dostępie do systemów GITD.
     - Przegląd i weryfikacja istniejących procedur postępowania w związku z wprowadzeniem stopnia alarmowego CRP, dokonanie weryfikacji posiadanych kopii zapasowych systemów teleinformatycznych GITD kluczowych dla funkcjonowania GITD oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemów oraz bazy danych teleadresowych.
     - Sprawdzenie aktualnego stanu bezpieczeństwa systemów GITD oraz dokonanie oceny wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.
     - Informowanie na bieżąco o efektach przeprowadzanych działań.
   - BRAVO-CRP (ALFA-CRP + poniższe)
     - Prowadzenie wzmożonego monitoringu stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zalecenia Szefa ABW, ze szczególnym uwzględnieniem:
       a) monitorowania i weryfikacji ewentualnego naruszenia bezpieczeństwa komunikacji elektronicznej;
       b) sprawdzania dostępności usług elektronicznych;
       c) w razie potrzeby dokonywania zmian w dostępie do systemów GITD.

- Przegląd i weryfikacja istniejących procedur postępowania w związku z wprowadzeniem stopnia alarmowego CRP, dokonać weryfikacji posiadanej kopii zapasowej systemów kluczowych dla funkcjonowania GITD, weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemów oraz bazy danych teleadresowych.
- Zapewnienie dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych.
- Sprawdzenie aktualnego stanu bezpieczeństwa systemów GITD oraz dokonanie oceny wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.
- Informowanie na bieżąco o efektach przeprowadzanych działań.
- Utrzymanie gotowości do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla GITD.
- Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania GITD oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych GITD.

• CHARLIE-CRP (ALFA-CRP+BRAVO-CRP + poniższe)

- Prowadzenie wzmożonego monitoringu stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zalecenia Szefa ABW, ze szczególnym uwzględnieniem:
  a) monitorowania i weryfikacji ewentualnego naruszenia bezpieczeństwa komunikacji elektronicznej;
  b) sprawdzania dostępności usług elektronicznych;
  c) w razie potrzeby dokonywania zmian w dostępie do systemów GITD.
- Przegląd i weryfikacja istniejących procedur postępowania w związku z wprowadzeniem stopnia alarmowego CRP, dokonanie weryfikacji posiadanych kopii zapasowych systemów kluczowych dla funkcjonowania GITD, weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemów, oraz bazy danych teleadresowych.
- Zapewnienie dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych.
- Sprawdzenie aktualnego stanu bezpieczeństwa systemów GITD oraz dokonanie oceny wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.
- Informowanie na bieżąco o efektach przeprowadzanych działań.
- Utrzymanie gotowości do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla GITD.
- Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania GITD oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych GITD.
- Dokonanie przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w wypadku zaistnienia ataku.

- Podjęcie działań mających na celu przygotowanie GITD do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
  a) dokonanie przeglądu i ewentualnego audytu planów awaryjnych oraz systemów GITD;
  b) przygotowanie GITD do ograniczenia operacji na serwerach celem szybkiego i bezawaryjnego zamknięcia w razie konieczności.
- DELTA-CRP (poprzednie + poniższe)
- Prowadzenie wzmożonego monitoringu stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zalecenia Szefa ABW, ze szczególnym uwzględnieniem:
  a) monitorowania i weryfikacji ewentualnego naruszenia bezpieczeństwa komunikacji elektronicznej;
  b) sprawdzania dostępności usług elektronicznych;
  c) w razie potrzeby dokonywania zmian w dostępie do systemów GITD.
- Przegląd i weryfikacja istniejących procedur postępowania w związku z wprowadzeniem stopnia alarmowego CRP, dokonanie weryfikacji posiadanych kopii zapasowych systemów kluczowych dla funkcjonowania GITD, weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemów, oraz bazy danych teleadresowych.
- Zapewnienie dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych.
- Sprawdzenie kanałów łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla rodzaju stopnia alarmowego CRP, dokonanie weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji.
- Sprawdzenie aktualnego stanu bezpieczeństwa systemów GITD oraz dokonanie oceny wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.
- Informowanie na bieżąco o efektach przeprowadzanych działań.
- Utrzymanie gotowości do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla GITD.
- Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania GITD oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych GITD.
- Dokonanie przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w wypadku zaistnienia ataku.
- Uruchomienie planów awaryjnych lub planów ciągłości działania GITD w sytuacji awarii lub utraty ciągłości działania.
- Stosownie do sytuacji, podjąć działania mające na celu przewrócenia ciągłości działania GITD.

11.3 W raportach miesięcznych Wykonawca będzie przedstawiał informacje o stanie bezpieczeństwa Systemu. Raporty muszą zawierać informacje umożliwiające weryfikację przez Zamawiającego czy nie zostało naruszone bezpieczeństwo Systemu, wyjaśnienie naruszeń bezpieczeństwa, działania podjęte w celu zapobiegania naruszeniom bezpieczeństwa w przyszłości.

12 Wykonywanie przeglądów Oprogramowania Użytkowego pod kątem planowania zmian

12.1 Wykonawca będzie świadczyć usługę wykonywania cyklicznych, (co 2 miesiące) przeglądów Oprogramowania Użytkowego:

a. Za zgodność z przepisami prawa i procedurami regulującymi działalność Zamawiającego określonymi w OPZ w pkt 5.8, celem identyfikacji elementów Oprogramowania użytkowego lub dokumentacji, dla których niezbędnym będzie wdrożenie zmian dostosowawczych.
b. Celem optymalizacji procesów wspieranych przez System np. identyfikacji tzw. „wąskich gardeł", eliminację zbędnych czynności, usprawnienie czynności, podniesienie lub zmniejszenie stopnia automatyzacji czynności, wdrożenia reorganizacji pracy Zamawiającego.

12.2 W zakresie Wykonywania okresowych, (co 2 miesiące) przeglądów Oprogramowania Użytkowego Wykonawca zobowiązany będzie do wykonywania analizy zgłoszonych przez Zamawiającego:

a. Incydentów i Problemów, które nie stanowią błędu w oprogramowaniu a sposobem ich rozwiązania jest wprowadzenie zmian optymalizujących procesy wspierane przez System. Wykonawca przeprowadzi wywiady z użytkownikami, którzy zgłosili Incydenty lub Problemy celem ustalenia/potwierdzenia przyczyn i warunków, w jakich one występują oraz ewentualnie zarejestrowanie oczekiwanych przez Użytkowników rozwiązań;
b. Zmian optymalizacyjnych m.in. w organizacji pracy Zamawiającego, zakresie i sposobie wykonywania czynności, poziomie automatyzacji, lokalizacji punktów decyzyjnych lub kontroli jakości, likwidacji „wąskich gardeł". Wykonawca przeprowadzi analizy z przedstawicielami Zamawiającego, którzy zgłosili propozycje zmian celem ustalenia powodów zmiany oraz spodziewanych efektów wdrożenia zmiany.

12.3 Analiza zmian będzie prowadzona z udziałem i pod kierunkiem Zamawiającego z zapewnieniem możliwości konsultowania proponowanych rozwiązań oraz skorzystania z ekspertów Zamawiającego w zakresie działalności GITD.

12.4 Wynikiem przeprowadzonego przeglądu będzie każdorazowo raport przygotowany przez Wykonawcę. Raport zawierał będzie:

a. Elementy Oprogramowania wymagające dostosowania w związku ze zmianami prawnymi, wraz z rekomendacjami, co do zakresu niezbędnych zmian dostosowawczych,
b. nazwy definicji procesów (BPMN) i/ lub elementy Oprogramowania wymagające optymalizacji wraz z rekomendacjami, co do zakresu niezbędnych zmian,

c. w przypadku braku potrzeby dostosowania - informacje o elementach oprogramowania i/lub definicjach procesów (BPMN), jakie zostały przeanalizowane w kontekście zgłoszonych zmian.

12.5 Informacje zawarte w Raporcie powinny pozwolić Zamawiającemu na podjęcie decyzji o uruchomieniu procedury wdrożenia zmiany projektowej.

12.6 Wykonawca będzie przygotowywać dla Zamawiającego projektowe wnioski o zmianę mające na celu realizację zmian w Oprogramowaniu użytkowym celem dostosowania Oprogramowania użytkowego do zmian prawnych i optymalizacji procesów wspieranych przez System.

13 Aktualizacja Oprogramowania Obcego

13.1 Celem usługi Aktualizacja Oprogramowania Obcego jest:

- Analiza poprawek i nowych wersji Oprogramowania Obcego,
- Ocena czy wymagana jest ich instalacja,
- W przypadku pozytywnej oceny wykonanie instalacji.

13.2 Wykonawca będzie świadczyć usługę aktualizacji Oprogramowania Obcego poprzez:

a. Wykonywanie kwartalnych przeglądów Oprogramowania Obcego wykorzystywanego w ramach realizacji Umowy celem aktualizacji lub instalacji nowych wersji Oprogramowania Obcego;
b. Przygotowywanie dla Zamawiającego projektowych wniosków o zmianę mających na celu realizację zmian w Oprogramowaniu Obcym ,
c. Aktualizację Oprogramowania Obcego i Dokumentacji.
d. Dostarczenie lub zapewnienie od producenta licencji dla Oprogramowania Obcego z Usługą Utrzymania, wsparcia, serwisu przez okres świadczenia tych usług przez Wykonawcę w ramach realizacji niniejszej Umowy.

13.3 W zakresie Wykonywania okresowych (kwartalnych) przeglądów Oprogramowania Obcego Wykonawca zobowiązany będzie do wykonywania następujących czynności:

a. Analizy wydawanych aktualizacji Oprogramowania Obcego oraz ich wpływu na funkcjonalność Systemu w tym Oprogramowanie Użytkowe. Analiza zmian będzie prowadzona bez udziału Zamawiającego z zapewnieniem możliwości konsultowania proponowanych rozwiązań z Zamawiającym;
b. Wynikiem przeprowadzonej analizy będzie każdorazowo Raport z przeprowadzonej analizy aktualizacji w Oprogramowaniu Obcym (dalej: Raport Oprogramowania) przygotowany przez Wykonawcę. Raport Oprogramowania zawierał będzie wersję Oprogramowania oraz opis zmian w stosunku do wersji poprzedniej oraz skutki jej wdrożenia na funkcjonalność Systemu w tym Oprogramowanie Użytkowe. Informacje zawarte w Raporcie Oprogramowania muszą pozwolić Zamawiającemu na podjęcie decyzji o uruchomieniu procedury wdrożenia zmiany rozwojowej;
c. W przypadku przyjęcia Raportu Oprogramowania zawierającego rekomendacje wdrożenia zmiany Zamawiający zleci Wykonawcy przygotowanie Wniosku o

zmianę projektową (aktualizacyjnego) podając kluczowe uwarunkowania dla jej wdrożenia.

d. W przypadku zdezaktualizowania obecnie wykorzystywanego Oprogramowania Obcego Wykonawca przekaże rekomendacje odnośnie aktualnego oprogramowania, Zamawiający podejmuje ostateczną decyzję o jego dostawie.
e. W przypadku dostarczenia nowego oprogramowania Wykonawca zobowiązany jest do jego skonfigurowania oraz skonfigurowania Systemu umożliwiając poprawne działanie.

13.4 Aktualny wykaz wykorzystywanego Oprogramowania Obcego zawarty jest w załączniku 3 do OPZ

13.5 W zakresie przygotowywania i zgłaszania projektowych wniosków o zmianę będzie miała zastosowanie procedura zarządzania zmianą. W szczególności Wykonawca zobowiązany będzie do przygotowania propozycji zmiany zawierającej specyfikacje aktualizacji dla Oprogramowania Obcego, opis zmian, opis wpływu na funkcjonalność Systemu w tym na Oprogramowanie Użytkowe pracochłonność, terminy i warunki wdrożenia zmiany. W wyniku akceptacji Propozycji zmiany Zamawiający przygotuje dla Wykonawcy Zlecenie wykonania zmiany (optymalizacji).

13.6 Na postawie zaakceptowanego przez Zamawiającego raportu z testów wersji Oprogramowania Systemu Wykonawca przygotuje Wniosek o wdrożenie wersji Oprogramowania w Środowisku Produkcyjnym Systemu.

13.7 W przypadku zmian w Oprogramowaniu Obcym, które będą pociągały za sobą konieczność dostosowania Oprogramowania Użytkowego, jego zmiany będą realizowane w ramach usługi Utrzymania Systemu.

14 Usprawnienie infrastruktury.

14.1 Wykonawca będzie świadczyć usługę usprawnienia Infrastruktury sprzętowej poprzez:

a. Wykonywanie raz w miesiącu analiz obsłużonych zgłoszeń o awariach, w celu identyfikowania potrzeb usprawnienia działania Infrastruktury sprzętowej,
b. W przypadku potrzeby usprawnienia Infrastruktury sprzętowej, wykonanie prac projektowych, wdrożeniowych i dokumentacji powykonawczej,
c. Przygotowywanie i zgłaszanie projektowych wniosków o zmianę mających na celu poprawę lub usprawnienie działającej Infrastruktury sprzętowej,
d. Wszystkie powyższe aktywności będą wykonywane w ramach Usługi Utrzymania nie obejmują dostarczenia Infrastruktury sprzętowej.