Załącznik nr 1 do Zapytania ofertowego 4/2026 po zm. z dn. 14.07.2026r.

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

Przedmiotem zamówienia jest usługa polegająca na pełnym wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w Transportowym Dozorze Technicznym.

1. Założenia dotyczące Zamówienia

1.1. Ocena stopnia zgodności organizacji z wymaganiami normy ISO 27001:2023-08 lub równoważną, obejmująca zarówno System Zarządzania Bezpieczeństwem Informacji, jak i proces zarządzania ryzykiem wraz ze spełnieniem wymogów wynikających z UKSC/NIS2 oraz normą PN-EN ISO 22301:2019 lub równoważną w kontekście ciągłości działania;

1.2. Ocena poziomu bezpieczeństwa sieci/architektury i stosowania dobrych praktyk w zakresie architektury informatycznej;

1.3. Identyfikacja luk w zabezpieczeniach oraz obszarów wymagających poprawy;

1.4. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI) oraz Systemu Zarządzania Ciągłością Działania (dalej: SZCD), w tym Polityki Bezpieczeństwa Informacji (dalej: PBI), zgodnego z:

1.4.1. ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024r. poz.1557 z późn. zm.);

1.4.2. ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022r. poz.902);

1.4.3. ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026r. poz.252) (dalej: UKSC);

1.4.4. rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej: RODO);

1.4.5. rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (dalej: KRI), minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024r. poz.773) (dalej: KRI);

1.4.6. innymi niż ww. ustawami i rozporządzeniami, którym podlega Zamawiający w zakresie bezpieczeństwa informacji włączenie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2024r. poz.632 z pożn.zm.);

1.4.7. normą PN-EN ISO/IEC 27001:2023-08 lub równoważną;

1.4.8. normą PN-EN ISO 22301:2019 lub równoważną w kontekście ciągłości działania.

2. Zakres zamówienia

Podstawowe wymagania w zakresie zaprojektowania dokumentów, procedur i wdrożenia SZBI, w tym PBI:

2.1. Usługa zaprojektowania dokumentów, procedur i wdrożenia SZBI w tym PBI, będzie obejmować swoim zakresem:

2.1.1. etap I – Audyt przedwdrożeniowy;

2.1.2. etap II – Klasyfikację aktywów informacyjnych;

2.1.3. etap III – Analizę ryzyka oraz wsparcie w jej przeprowadzeniu - Szacowanie ryzyka;

2.1.4. etap IV – Przygotowanie dokumentacji - Opracowanie dokumentacji SZBI i SZCD spełniającej wymogi UKSC/NIS2;

2.1.5. etap VI – Wykonanie audytu SZBI i SZCD pod względem zgodności systemu z KRI i UKSC/NIS2.

2.2. Wszelkie informacje dotyczące usługi przekazywane między Wykonawcą a Zamawiającym za pomocą środków komunikacji elektronicznej na adres e-mail: informatyka@tdt.gov.pl.

2.3. Zamawiający wymaga, aby Wykonawca do realizacji zamówienia skierował co najmniej:

2.3.1. osobę pełniącą funkcję Kierownika projektu / koordynatora wdrożenia (odpowiada z harmonogram, komunikację, jakość, odbiory i koordynację zespołu), która:

- posiada co najmniej dwa certyfikaty zgodnie z obowiązującymi normami (w szczególności ISO/IEC 27001, ISO 22301) lub kwalifikacje, z których co najmniej jeden dotyczy audytowania albo wdrażania SZBI, a co najmniej jeden dotyczy audytu bezpieczeństwa informacji, cyberbezpieczeństwa, zarządzania ryzykiem, ciągłości działania albo audytu systemów informacyjnych, lub równoważne, posiada minimum 2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa;
- posiada minimum 3-letnie doświadczenie w prowadzeniu projektów z zakresu SZBI, cyberbezpieczeństwa, compliance, audytu lub ciągłości działania oraz udział w co najmniej 2 projektach dotyczących ISO 27001, UKSC/NIS2, KRI lub ISO 22301 oraz doświadczenie w przeprowadzaniu przeglądu, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach sektora finansów publicznych określonymi w Ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U.z 2024r. poz. 1530 z późn. zm.)

2.3.2. osobę pełniącą funkcję Eksperta SZBI / ISO 27001 Lead Implementer posiadającego certyfikaty potwierdzające jego kwalifikacje i kompetencje w zakresie przeprowadzania audytów systemów zarządzania bezpieczeństwem informacji oraz ciągłości działania, zgodnie z obowiązującymi normami (w szczególności ISO/IEC 27001, ISO 22301) oraz określone w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999). Oznacza to, że musi legitymować się np. certyfikatem CISA, CISM lub innym wymienionym w załączniku do ww. rozporządzenia lub równoważnym oraz:

- posiada minimum 2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa;
- posiada doświadczenie polegające na opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w co najmniej dwóch projektach.

2.3.3. osobą pełniącą funkcję Audytora wiodącego ISO 27001/ posiadającego certyfikaty potwierdzające jego kwalifikacje i kompetencje w zakresie przeprowadzania audytów systemów zarządzania bezpieczeństwem informacji oraz ciągłości działania, zgodnie z obowiązującymi normami (w szczególności ISO/IEC 27001, ISO 22301) który:

- posiada certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025r. poz. 568), w zakresie certyfikacji osób lub równoważnym;

2.3.4. osobą pełniącą funkcję Eksperta ISO 22301 posiadającego certyfikaty potwierdzające jego kwalifikacje i kompetencje w zakresie ciągłości działania, zgodnie z obowiązującymi normami (ISO 22301) który:

- posiada certyfikat eksperta systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób lub równwaznym.
- posiada doświadczenie w BIA, RTO/RPO, planach ciągłości działania, planach odtworzeniowych i testach ciągłości.

2.3.5. osobą pełniącą funkcję eksperta cyberbezpieczeństwa technicznego / KRI / UKSC który:

- posiada rozległą wiedzę techniczną z zakresu bezpieczeństwa systemów i sieci potwierdzoną co najmniej jednym z certyfikatów (np.: VA - Certified Vulnerability Assessor, CSSA - Certified Cybersecurity Systems Auditor, CompTIA Security+) lub równoważnym;
- posiada doświadczenie w audytach technicznych IT, bezpieczeństwie sieci, architekturze bezpieczeństwa, KRI, UKSC/NIS2, zarządzaniu podatnościami lub

ocenie zabezpieczeń technicznych.

2.3.6. osobą pełniąca funkcję pełnomocnika posiadającą poświadczenia bezpieczeństwa oraz aktualne przeszkolenie w zakresie ochrony informacji niejawnych zgodnie z ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209 tj.)

2.4. Zamawiający dopuszcza łączenie maksymalnie dwóch ról przez jedną osobę, pod warunkiem spełnienia przez tę osobę wszystkich wymagań przewidzianych dla łączonych ról. Funkcja kierownika projektu nie powinna być łączona z więcej niż jedną funkcją ekspercką.

2.5. Osoby wskazane przez Wykonawcę na potwierdzenie spełnienia warunków udziału muszą faktycznie uczestniczyć w realizacji zamówienia. Zmiana osoby wskazanej w ofercie wymaga zgody Zamawiającego i jest dopuszczalna wyłącznie pod warunkiem wykazania, że osoba zastępująca posiada kwalifikacje i doświadczenie nie niższe niż osoba zastępowana

3. Etap I – Audyt przedwdrożeniowy

3.1. Wykonawca dokona audytu zgodności działań Zamawiającego z uregulowaniami prawnymi, którym podlega TDT w zakresie bezpieczeństwa informacji wymienionych w pkt. 1.4.1-6 oraz normami, o których mowa w pkt 1.4.7-8.

3.2. Audyt podlega przeprowadzeniu we wszystkich komórkach (wydziałach) organizacyjnych Transportowego Dozoru Technicznego.

3.3. W terminie 5 dni przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy plan audytu. Plan audytu Wykonawca przekaże w formie elektronicznej oraz przekaże Zamawiającemu pocztą elektroniczną na adresy email wskazane przez Zamawiającego.

3.4. Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:

3.4.1. zapoznanie się ze strukturą organizacyjną TDT;

3.4.2. analizę i ocenę dokumentacji w zakresie swojego działania, w tym polityk, procedur, zarządzeń, instrukcji oraz innych dokumentów, które Zamawiający udostępni Wykonawcy do analizy. Zamawiający zastrzega sobie prawo do udostępnienia dokumentacji wyłącznie w jego siedzibie;

3.4.3. wywiady analityczne z wyznaczonymi przez Zamawiającego pracownikami komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa określonych w KRI, normie PN-EN ISO/IEC 27001:2023-08 lub równoważnej oraz normą PN-EN ISO 22301:2019 lub równoważną w kontekście ciągłości działania w tym uwzględniające:

- kontekst organizacji;
- polityki bezpieczeństwa informacji;
- organizację bezpieczeństwa informacji;
- postępowanie z ryzykiem w bezpieczeństwie informacji;
- bezpieczeństwo zasobów ludzkich;
- zarządzanie aktywami;
- kontrolę dostępu;
- kryptografię;
- bezpieczeństwo fizyczne i środowiskowe;
- bezpieczną eksploatację;
- bezpieczeństwo komunikacji;
- pozyskiwanie i rozwój systemów;
- relacje z dostawcami;
- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- aspekty bezpieczeństwa informacji w zarzadzaniu ciągłością działania;
- analizę luk w systemach bezpieczeństwa;

3.4.4. obserwację budynków, pomieszczeń, działań i zachowania pracowników Transportowego Dozoru Technicznego w celu weryfikacji przestrzegania przez nich obowiązujących w Transportowym Dozorze Technicznym wewnętrznych procedur z zakresu bezpieczeństwa informacji;

3.5. Wykonawca opracuje i sporządzi raport z przeprowadzonego audytu przedwdrożeniowego,

zawierający w szczególności:

3.5.1. cel i zakres audytu;

3.5.2. szczegółowy opis przeprowadzonych prac;

3.5.3. opis poziomu spełnienia każdego z wymagań bezpieczeństwa określonych w KRI, innych obowiązujących aktach prawnych, o których mowa w pkt 1.4.1-4 i pkt. 1.4.6, normie PN-EN ISO/IEC 27001:2023-08 lub równoważnej oraz wewnętrznych uregulowaniach Transportowego Dozoru Technicznego i normie PN-EN ISO 22301:2019 w zakresie ciągłości działania;

3.5.4. wykaz stwierdzonych niezgodności w odniesieniu do każdego wymagania określonego w KRI, innych obowiązujących aktach prawnych, o których mowa w pkt 1.4.1-4 i pkt. 1.4.6, normie PN-EN ISO/IEC 27001:2023-08 lub równorzędnej, normie PN-EN ISO 22301:2019 w zakresie ciągłości działania oraz wewnętrznych uregulowaniach Transportowego Dozoru Technicznego, normie na poziomie opisu poszczególnych zabezpieczeń wraz z przedstawieniem dowodów na istnienie niezgodności;

3.5.5. rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań określonych w KRI, innych obowiązujących aktach prawnych, o których mowa w pkt 1.4.1-4 i pkt. 1.4.6, normie PN-EN ISO/IEC 27001:2023-08 lub równoważnej, normie PN-EN ISO 22301:2019 w zakresie ciągłości działania oraz wewnętrznych uregulowaniach Transportowego Dozoru Technicznego;

3.5.6. rekomendacje w zakresie wdrożenia środków monitorowania systemów informacyjnych w trybie ciągłym.

3.5.7. rekomendacje w zakresie Zabezpieczenie łańcucha dostaw ICT.

3.5.8. podsumowanie i wnioski.

3.6. Raport, o którym mowa w pkt. 3.5 Wykonawca przekaże Zamawiającemu w formie elektronicznej na adresy email wskazane przez Zamawiającego.

3.7. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do przekazanego przez Wykonawcę raportu. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

3.8. Ostateczną wersję raportu uwzględniającą uwagi zgłoszone przez Zamawiającego, Wykonawca przekaże Zamawiającemu na zakończenie danego etapu.

4. Etap II - Klasyfikacja aktywów informacyjnych

4.1. W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:

4.1.1. opracowania metodyki klasyfikowania aktywów informacyjnych w Transportowym Dozorze Technicznym;

4.1.2. opracowania modelu podziału informacji przetwarzanych w Transportowym Dozorze Technicznym w zależności od poziomu ich wrażliwości i przeznaczenia z uwzględnieniem informacji niejawnych;

4.1.3. przeszkolenia pracowników Transportowego Dozoru Technicznego w zakresie sposobu klasyfikowania informacji na bazie wcześniej opracowanej metodyki;

4.1.4. sklasyfikowania wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych w Transportowym Dozorze Technicznym w tym:

4.1.4.1. identyfikacji aktywów informacyjnych,

4.1.4.2. klasyfikacji informacji,

4.1.4.3. przypisaniu właścicieli aktywów,

4.1.4.4. powiązaniu aktywów z procesami,

4.1.4.5. ocenie krytyczności aktywów,

4.1.4.6. powiązaniu aktywów z ryzykiem.;

4.1.5. opracowania raportu z procesu klasyfikacji informacji.

4.2. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do opracowanej przez Wykonawcę metodyki klasyfikowania informacji. Wykonawca uwzględni przesłane przez Zamawiającego uwagi i przedstawi Zamawiającemu ostateczną wersję metodyki. Zamawiający zatwierdzi ostateczną wersję przesłanej metodyki najpóźniej na 5 dni roboczych przed rozpoczęciem szkoleń.

4.3. Dokumentację, o której mowa w pkt. 4.1, a w szczególności opis metodyki klasyfikowania informacji oraz raport z procesu klasyfikowania informacji Wykonawca przekaże Zamawiającemu w formie elektronicznej na adresy email wskazane przez Zamawiającego.

4.4. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do przekazanej przez Wykonawcę dokumentacji określonej w pkt. 4.1, Wykonawca zobowiązany jest do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

5. Etap III - Wdrożenie systemu analizy ryzyka oraz wsparcie przy jej przeprowadzenie - szacowanie ryzyka.

5.1. W ramach usługi Wykonawca jest zobowiązany przygotować metodykę oraz wesprzeć zamawiającego w procesie szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Transportowym Dozorze Technicznym, a w szczególności:

5.1.1. opracować metodykę szacowania ryzyka spełniającą wymagania KRI/UKSC, norm PN-EN ISO/IEC 27001:2023-08 lub równoważnej, ISO/IEC 27005:2018 lub równoważnej, optymalną ze względu na charakter działalności Transportowego Dozoru Technicznego;

5.1.2. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do opracowanej metodyki szacowania ryzyka, a Wykonawca zobowiązany jest je uwzględnić;

5.1.3. opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;

5.1.4. przeszkolić wybranych pracowników Transportowego Dozoru Technicznego w zakresie przyjętej metodyki szacowania ryzyka;

5.1.5. przeprowadzić wspólnie z wyznaczonymi pracownikami Transportowego Dozoru Technicznego proces szacowania ryzyka zgodnie z wybraną i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka, w tym: zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;

5.1.6. opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Transportowego Dozoru Technicznego;

5.1.7. opracować przy współudziale wyznaczonych pracowników Transportowego Dozoru Technicznego plan postępowania z ryzykiem.

5.1.8. przeprowadzenie integracji procesu szacowania ryzyka o którym mowa w pkt. 5.1.1. z innymi systemami (np. w zakresie ochrony danych osobowych, kontroli zarządczej) przy uwzględnieniu przedłożonej dokumentacji przez Zamawiającego – jeśli Zamawiający tak uzna po konsultacjach z Wykonawcą.

5.2. Dokumentację, o której mowa w pkt. 5.1, tj. metodykę szacowania ryzyka, raport z procesu szacowania ryzyka oraz plan postępowania z ryzykiem Wykonawca przekaże Zamawiającemu w formie elektronicznej na adresy email wskazane przez Zamawiającego.

5.3. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do przekazanej przez Wykonawcę dokumentacji określonej pkt. 5.1, w Wykonawca jest zobowiązany do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.

6. Etap IV - Opracowanie dokumentacji SZBI oraz SZCD

6.1. Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest zaproponować organizację SZBI oraz SZCD oraz opracować i przedstawić koncepcję wdrożenia PBI w Transportowym Dozorze Technicznym spełniającą wymagania UKSC/NIS2.

6.2. Koncepcja będzie w szczególności zawierać mapę dokumentów, stanowiącą szczegółowy wykaz dokumentów z zaznaczeniem ich wzajemnych powiązań, w tym:

6.2.1. Dokument Główny PBI definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz aktywów chronionych, role i odpowiedzialności pracowników Transportowego Dozoru Technicznego w zakresie bezpieczeństwa informacji, przeglądy polityk;

6.2.2. Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w Transportowym Dozorze Technicznym w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, ochrony danych osobowych, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;

6.2.3. Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji;

6.2.4. Dokumentację SZCD, w tym zakres systemu, ocenę ryzyka, procedury testowania i ćwiczeń, analizę BIA, analizę wpływu na działalność, identyfikację procesów krytycznych, określenie parametrów RTO/RPO, opracowanie strategii ciągłości działania, planów ciągłości działania lub planów odtworzeniowych oraz scenariuszy testów lub ćwiczeń.

6.3. Dla każdego dokumentu, o którym mowa w pkt. 6.2, Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji szczegółowy zakres merytoryczny.

6.4. W przypadku dokumentów funkcjonujących w Transportowym Dozorze Technicznym, odnoszących się do bezpieczeństwa informacji, których zakres merytoryczny będzie w całości lub częściowo pokrywał się z opracowanymi przez Wykonawcę projektami dokumentów SZBI oraz SZCD, Wykonawca zaproponuje i uzasadni sposób ich, wyłączenia, zastąpienia lub zintegrowania z zaproponowaną przez Wykonawcę mapą dokumentów.

6.5. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wniesione przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia SZBI oraz SZCD.

6.6. Na podstawie zatwierdzonej przez Zamawiającego koncepcji, o której mowa w pkt. 6.1-2, Wykonawca opracuje wszystkie opisane w koncepcji dokumenty. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega Transportowy Dozór Techniczny. Jeżeli w czasie realizacji umowy zostaną uchwalone lub wydane akty prawne prawa powszechnie obowiązującego zmieniające wymagania prawa w zakresie bezpieczeństwa informacji, Wykonawca zobowiązany jest dostosować dokumentację SZBI oraz SZCD do zaistniałych zmian. Na powyższy obowiązek nie wpływa fakt, że ww. akty prawne nie wejdą w życie podczas realizacji umowy.

6.7. Wszystkie dokumenty Wykonawca przekaże Zamawiającemu w formie elektronicznej na adresy email wskazane przez Zamawiającego.

6.8. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

7. Etap V - Szkolenia z zakresu SZBI oraz SZCD

7.1. Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń budujących świadomość cyberzagrożeń oraz sposobów ochrony przed nimi, w tym z zakresu SZBI oraz SZCD dla wszystkich pracowników Transportowego Dozoru Technicznego, obejmujących co najmniej:

7.1.1. omówienie podstawowych zasad bezpieczeństwa informacji,

7.1.2. zagrożenia bezpieczeństwa informacji i ciągłości działania

7.1.3. odpowiedzialność (skutki) za naruszenie zasad wdrożonych SZBI oraz SZCD, w tym Polityk i procedur w tym odpowiedzialność prawna;

7.1.4. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7.1.5. zasady zgłaszania i reagowania na incydenty.

7.2. Wykonawca w ramach realizacji zadania, o którym mowa w pkt. 7.1 zorganizuje szkolenie online (oparte na połączeniu telekonferencyjnym – audio-video), trwające minimum 90 minut.

7.3. Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla kadry zarządzającej Transportowego Dozoru Technicznego oraz osób istotnych z punktu widzenia SZBI oraz SZCD

7.4. Wykonawca w ramach realizacji zadania, o którym mowa w pkt. 7.3 zorganizuje szkolenie online (oparte na połączeniu telekonferencyjnym – audio-video), każde trwające minimum 60 minut.

7.5. Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń dla informatyków z zakresu cyberbezpieczeństwa.

7.6. Wykonawca w ramach realizacji zadania, o którym mowa w pkt. 7.5 Zorganizuje szkolenie online (oparte na połączeniu telekonferencyjnym – audio-video), każde trwające minimum 120 minut.

7.7. Wykonawca uzgodni z Zamawiającym terminy przeprowadzenia szkoleń.

7.8. Wykonawca przygotuje materiały szkoleniowe zgodnie ze standardami dostępności cyfrowej.

7.9. Wykonawca przekaże do akceptacji Zamawiającemu szczegółowy program szkolenia oraz materiały szkoleniowe najpóźniej na 5 dni przed planowanym terminem rozpoczęcia szkolenia.

7.10. Zamawiający zastrzega sobie prawo do rejestracji audiowizualnej przebiegu szkoleń celem dalszego użytkowania w zakresie szkoleń nowych pracowników jak i ponownego wykorzystania w szkoleniach przypominających dla obecnych pracowników.

8. Etap VI - Wykonanie audytu powdrożeniowego SZBI i SZCD na zgodność z KRI i UKSC/NIS2.

8.1. Audyt powdrożeniowy obejmuje następujące prace:

8.1.1. Weryfikację poziomu wdrożenia w Transportowym Dozorze Technicznym zabezpieczeń zgodnie z rekomendacjami, o których mowa w pkt. 3.5.5;

8.1.2. weryfikację stosowania zasad określonych w PBI przez pracowników Transportowego Dozoru Technicznego;

8.1.3. ocenę poziomu spełnienia wymagań Krajowym Ram Interoperacyjności;

8.1.4. ocenę zgodności z przepisami zawartymi w aktach prawnych, wymienionych w pkt. 1.4.1-6 oraz z normami, o której mowa pkt. 1.4.7-8.

8.2. Audyt zostanie przeprowadzony we wskazanych przez Zamawiającego komórkach organizacyjnych Transportowego Dozoru Technicznego uzgodnionych z wykonawcą .

8.3. Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy plan audytu.

8.4. Wykonawca opracuje raport z audytu powdrożeniowego, zawierający co najmniej:

8.4.1. cel i zakres przeprowadzonego audytu;

8.4.2. opis przeprowadzonych prac;

8.4.3. szczegółowy opis poziomu spełnienia wymagań KRI, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz normy PN-EN ISO/IEC 27001:2023-08 lub równoważnej, w których podczas audytu przedwdrożeniowego stwierdzono niezgodności,

8.4.4. potwierdzenie spełnienia wymogów określonych w przepisach zawartych w aktach prawnych wymienionych w pkt. 1.4.1-6 i norm, o których mowa w pkt. 1.4.7-8, w tym potwierdzenie zgodności z przepisami RODO;

8.4.5. wykaz zaobserwowanych niezgodności w odniesieniu do stosowania przez pracowników Transportowego Dozoru Technicznego zasad SZBI;

8.4.6. szczegółowy opis działań korygujących i naprawczych;

8.4.7. ogólną ocenę poziomu spełnienia wymagań KRI oraz normy PN-EN ISO/IEC 27001:2023-08 lub równoważnej zgodnie z załącznikiem A do tej normy oraz poziomu stosowania przez pracowników Transportowego Dozoru Technicznego zasad SZBI;

8.4.8. ogólną ocenę poziomu spełnienia wymagań normy PN-EN ISO 22301:2019 w zakresie ciągłości działania Transportowego Dozoru Technicznego;

8.4.9. podsumowanie i wnioski.

8.5. Raport, o którym mowa w pkt. 8.4, Wykonawca przekaże Zamawiającemu w formie elektronicznej na adresy email wskazane przez Zamawiającego.

8.6. Zamawiający zastrzega sobie prawo do wnoszenia uwag za pomocą poczty elektronicznej do raportu przekazanego przez Wykonawcę. Wykonawca jest zobowiązany do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego.

9. Harmonogram realizacji zamówienia

9.1. Maksymalny termin realizacji - nie później niż do 20.12.2026 r.

9.2. Wykonawca zobowiązany jest zrealizować przedmiot zamówienie zgodnie z przedłożonym i zaakceptowanym harmonogramem.