**Część I:** **Przeprowadzenie trzech audytów zgodności KRI**

1. **Zakres audytu KRI:**
2. Wizja lokalna + skanowanie infrastruktury  **– na miejscu oraz zdalnie.**
3. Wizja lokalna miejsc kluczowych dla działania infrastruktury.
4. Ocena bezpieczeństwa pomieszczenia serwerowego, w tym kontroli dostępu, monitoringu i klimatyzacji.
5. Występowanie pojedynczych punktów awarii.
6. Weryfikacja, czy sprzęt jest chroniony przed nieuprawnionym dostępem oraz czynnikami środowiskowymi.
7. Wywiad techniczny.
8. Skanowanie wewnętrznej infrastruktury. Próba określenia podatności w wykrytych systemach operacyjnych i usługach sieciowych.
9. Bezpieczeństwo danych. Sprawdzenie dobrych praktyk dotyczących wykonywania kopii zapasowych. Przegląd polityk tworzenia kopii.
10. Audyt według wymogów Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773) w zakresie bezpieczeństwa informacji.
11. Raport z audytu zostanie podpisany przez audytora dokonującego audyt i dostarczony do Zamawiającego.
12. Harmonogram poszczególnych audytów:

• Audyt KRI nr 1 – listopad 2024 roku,

• Audyt KRI nr 2 – wrzesień/październik 2025 roku,

• Audyt KRI nr 3 – kwiecień/maj 2026 roku.

**Część II - Opracowanie i wdrożenie SZBI wraz z aktualizacją i audytem zgodności.**

**Zakres audytu SZBI:**

1. Przegląd obejmie następujące obszary:
2. Obszar dot. kwestii organizacyjnych
3. Obszar dot. kwestii prawnych
4. Obszar dot. kwestii informatycznych
5. Obszar dot. kwestii zasobów ludzkich
6. Obszar dot. kwestii bezpieczeństwa fizycznego
7. Wizja lokalna + skanowanie infrastruktury  **– na miejscu oraz zdalnie.**
8. Wizja lokalna miejsc kluczowych dla działania infrastruktury.
9. Ocena bezpieczeństwa pomieszczenia serwerowego, w tym kontroli dostępu, monitoringu i klimatyzacji.
10. Występowanie pojedynczych punktów awarii.
11. Weryfikacja, czy sprzęt jest chroniony przed nieuprawnionym dostępem oraz czynnikami środowiskowymi.
12. Wywiad techniczny.
13. Skanowanie wewnętrznej infrastruktury. Próba określenia podatności w wykrytych systemach operacyjnych i usługach sieciowych.
14. Ocena bezpieczeństwa organizacji z sieci internet – skanowanie z zewnątrz. Ocena urządzeń brzegowych pod kątem: podstawowej konfiguracji, wersji zainstalowanego systemu operacyjnego i możliwych ścieżek aktualizacji, polityk bezpieczeństwa na urządzeniu UTM, podziału sieci fizycznej na sieci logiczne z uwzględnieniem segmentacji sieci oraz izolacji systemów kluczowych.
15. Bezpieczeństwo danych. Sprawdzenie dobrych praktyk dotyczących wykonywania kopii zapasowych. Przegląd polityk tworzenia kopii.
16. Raport z audytu zostanie podpisany przez audytora dokonującego audyt i dostarczony do Zamawiającego.

**OPRACOWANIE I WDROŻENIE SZBI**

1. W ramach Etapu II Wykonawca, na podstawie wyników Audytu Zgodności SZBI opracuje dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI) dostosowany do potrzeb Zamawiającego.
2. SZBI, który opracuje Wykonawca, będzie stanowił system zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2021 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773), bądź w zastępujących go, odpowiednich przepisach wykonawczych do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307).
3. SZBI powinien być zgodny z rozporządzeniem KRI i spełniać wymagania normy PN-ISO/IEC 27001, w tym obejmować czternaście następujących obszarów mających wpływ na bezpieczeństwo w organizacji Zamawiającego:
4. Polityka Bezpieczeństwa;
5. Organizacja bezpieczeństwa informacji;
6. Bezpieczeństwo zasobów ludzkich;
7. Zarządzanie aktywami;
8. Kontrola dostępu;
9. Kryptografia;
10. Bezpieczeństwo fizyczne i środowiskowe;
11. Bezpieczna eksploatacja;
12. Bezpieczna komunikacja;
13. Pozyskiwanie, rozwój i utrzymanie systemów
14. Relacje z dostawcami;
15. Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
16. Aspekty bezpieczeństwa w zarządzaniu ciągłością działania;
17. Zgodność z wymaganiami prawnymi i własnymi standardami.

Ponadto SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762. 4. SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:

1. rozporządzenia KRI;
2. rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);
3. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
4. ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307);
5. ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902);
6. ustawy z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowiska (t.j. Dz. U. z 2024 r. poz. 1112);
7. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 632));
8. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077);

oraz uwzględniać wewnętrzne akty prawne obowiązujące u Zamawiającego.

1. W ramach opracowania SZBI Wykonawca między innymi:
2. zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;
3. uwzględni w szczególności następujące zagadnienia:
4. określenie organizacji bezpieczeństwa informacji,
5. identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
6. szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
7. bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
8. szkolenia z zakresu bezpieczeństwa informacji,
9. kontrola dostępu,
10. bezpieczeństwo fizyczne i środowiskowe,
11. klasyfikacja informacji,
12. odpowiedzialność za zasoby,
13. postępowanie z nośnikami informacji,
14. użytkowanie urządzeń mobilnych i praca zdalna,
15. zarządzanie sprzętem informatycznym,
16. instalacja oprogramowania,
17. ochrona przed oprogramowaniem złośliwym,
18. kopie zapasowe,
19. zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
20. zarządzanie dokumentacją infrastruktury informatycznej,
21. monitorowanie systemów informatycznych,
22. zarządzanie pojemnością,
23. serwis i konserwacja infrastruktury informatycznej,
24. zarządzanie podatnościami technicznymi,
25. zarządzanie incydentami bezpieczeństwa,
26. zabezpieczenia kryptograficzne,
27. bezpieczeństwo sieci i transmisji danych,
28. ochrona własności intelektualnej,
29. bezpieczeństwo informacji w relacjach z dostawcami,
30. ciągłość działania,
31. zasady bezpieczństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
32. weryfikacja zgodności z wymaganiami prawnymi,
33. korzystanie z poczty elektronicznej i Internetu,
34. zarządzanie usługami informatycznymi,
35. utrzymanie i doskonalenie SZBI,
36. przeprowadzanie audytów SZBI.
37. Wykonawca wraz z SZBI przedstawi zestawienie, zwane „Zestawieniem, w którym wykaże spełnienie przez SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, w tym rozporządzenia KRI, a także odpowiednich norm.
38. SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.
39. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę SZBI, w tym do rodzaju dokumentów, ich liczby, nazewnictwa, zakresu merytorycznego. Uwagi Zamawiającego powinny być każdorazowo uwzględnione przez Wykonawcę. W przypadku, gdyby proponowane przez Zamawiającego zmiany mogły powodować niezgodność dokumentacji z Umową, Wykonawca poinformuje o tym wcześniej Zamawiającego, uzasadniając swoje stanowisko – w takim przypadku Zamawiający podejmie ostateczną decyzję w zakresie konieczności uwzględnienia jego uwag przez Wykonawcę.
40. Aktualizacja dokumentacji SZBI – po wykonaniu drugiego audytu zgodności KRI (termin drugiego audytu KRI u Zamawiającego - wrzesień/październik 2025).
41. Harmonogram poszczególnych części zadania:

• Audyt SZBI – listopad 2024 roku,

• Opracowanie i wdrożenie SZBI – styczeń/luty 2025 roku,

• Aktualizacja SZBI – listopad 2025 roku.