**Opis przedmiotu zamówienia**

**część 5: Audyty SZBI/KRI**

Zamawiający wymaga przeprowadzenia audytu SZBI / KRI z wdrożeniem lub aktualizacją w Urzędzie Miejskim w Nowym Tomyślu Polityki Bezpieczeństwa Informacji opisującej SZBI w oparciu o Rozporządzenie KRI, Polską Normę PN ISO/IEC 27001:2023 oraz Dyrektywe NIS2, przeprowadzenia audytu końcowego SZBI i KRI w Urzędzie Miejskim w Nowym Tomyślu oraz przeprowadzenia audytów końcowych KRI dla 7 jednostek podległych.

Przeprowadzane audyty powinny spełniać założenia końcowych audytów wymaganych w programie Cyberbezpieczny Samorząd.

Wykaz jednostek podległych:

1. Szkoła Podstawowa nr 1 im. Tadeusza Kościuszki w Nowym Tomyślu

ul. Wierzbowa 1, 64-300 Nowy Tomyśl;

1. Szkoła Podstawowa nr 2 im. Marii Skłodowskiej – Curie w Nowym Tomyślu

ul. 3 Stycznia 12, 64 - 300 Nowy Tomyśl;

1. Szkoła Podstawowa nr 3 im. Feliksa Szołdrskiego w Nowym Tomyślu

os. Północ 25, 64-300 Nowy Tomyśl;

1. Szkoła Podstawowa im. Marii Kownackiej w Wytomyślu

ul. Szkolna 18, 64-300 Wytomyśl;

1. Szkoła Podstawowa im. Marii Konopnickiej w Borui Kościelnej

ul. Szkolna 14, 64 - 300 Boruja Kościelna;

1. Zespół Przedszkolno - Szkolny w Bukowcu

ul. Kościelna 75, 64 - 300 Nowy Tomyśl;

1. Szkoła Podstawowa im. Leonarda Śliwińskiego w Sątopach

ul. Szkolna 3, 64-300 Sątopy.

1. **Wymagania minimalne**
2. Wykonawca zapewni audytora/audytorów do przeprowadzenia audytów KRI/SZBI, którzy dokonają oceny funkcjonowania SZBI zgodnie z Rozporządzeniem KRI, Normą PN-EN ISO/IEC 27001-203 oraz Dyrektywą NIS2 i przedstawią wyniki w postaci raportów z audytów.
3. Wykonawca zrealizuje audyty:
   1. początkowy SZBI (audyt zgodności z Rozporządzeniem KRI, Normą PN-EN ISO/IEC 27001-203 oraz Dyrektywą NIS2) w Urzędzie Miejskim w Nowym Tomyślu w terminie do 30 dni od dnia podpisania umowy.
   2. końcowy SZBI/KRI w standardzie NIS 2 w Urzędzie Miejskim w Nowym Tomyślu w terminie 9 miesięcy od dnia podpisania umowy (nie wcześniej niż od dnia poinformowania przez Zamawiającego o zakończeniu wdrożenia zakupionego sprzętu i zakończenia projektu w zakresie dostaw – Zamawiający przewiduje zakończenie dostaw do dnia **01.10.2025 r.**).
   3. końcowy KRI (audyt zgodności z Rozporządzeniem KRI, Normą PN-EN ISO/IEC 27001-2023 oraz Dyrektywą NIS2) w 7 jednostkach podległych w terminie 7 miesięcy od dnia podpisania umowy (nie wcześniej niż od dnia poinformowania przez Zamawiającego o zakończeniu wdrożenia zakupionego sprzętu i zakończenia projektu w zakresie dostaw – Zamawiający przewiduje zakończenie dostaw do dnia **02.08.2025 r.**).
4. Wykonawca dokona aktualizacji/sporządzenia dokumentacji SZBI z uwzględnieniem (Rozporządzenia KRI, Polskiej Normy PN-EN ISO/IEC 27001-2023, Dyrektywy NIS2 oraz obowiązującej ustawy o Krajowym Systemie Cyberbezpieczeństwa) dla Urzędu Miejskiego w Nowym Tomyślu. Efekt: Polityka Bezpieczeństwa Informacji Urzędu Miejskiego w Nowym Tomyślu opisująca system zarządzania bezpieczeństwem informacji, sporządzona w oparciu o normę wskazane powyżej normę i przepisy krajowe i dyrektywy unijne i z nimi zgodna.
5. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
6. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.
7. Wykonawca po wykonaniu ostatniego audytu KRI jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
8. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
9. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
10. Na wszystkie usługi Wykonawca udzieli 12-miesięcznej gwarancji polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji dokumentacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.
11. Wykonawca zapewnia o zgodności przeprowadzonych audytów końcowych z wytycznymi i wymaganiami zawartymi w projekcie Cyberbezpieczny Samorząd.
12. **Wymagania audytów SZBI / KRI**
13. Przeprowadzany audyt SZBI powinien sprawdzać zgodność z Rozporządzeniem KRI oraz zgodność z normami PN-ISO/IEC 27001-2023, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO- 22301, Dyrektywą NIS 2 i obowiązującą ustawą o Krajowym systemie cyberbezpieczeństwa.
14. W tym m.in. czy w Polityce bezpieczeństwa informacji opisującej system zarządzania bezpieczeństwem informacji ujęto zagadnienia opisujące:
    1. Kierunki bezpieczeństwa informacji określone przez kierownictwo;
    2. Organizacje bezpieczeństwa informacji:
       * organizację wewnętrzną;
       * sposób zarządzania urządzeniami mobilnymi i zarządzanie telepracą;
    3. Bezpieczeństwo zasobów Ludzkich:
       * przed zatrudnieniem;
       * podczas zatrudnienia;
       * zakończenia i zmiany zatrudnienia;
    4. Zarządzanie aktywami:
       * odpowiedzialność za aktywa;
       * klasyfikacje informacji;
       * postępowanie z nośnikami;
    5. Kontrole dostępu:
       * wymagania biznesowe wobec kontroli dostępu;
       * zarządzanie dostępem użytkowników;
       * odpowiedzialność użytkowników;
       * kontrolę dostępu do systemów i aplikacji;
    6. Kryptografię:
       * zabezpieczenia kryptograficzne;
    7. Bezpieczeństwo fizyczne i środowiskowe:
       * obszary bezpieczne;
       * sprzęt;
    8. Bezpieczną eksploatację:
       * procedury eksploatacyjne;
       * ochrona przed szkodliwym oprogramowaniem;
       * kopie zapasowe;
       * rejestrowanie zdarzeń i monitorowanie;
       * zarządzanie podatnościami technicznymi;
       * informacje o zasadach prowadzenia audytów informatycznych;
    9. Bezpieczeństwo komunikacji:
       * zarządzanie bezpieczeństwem sieci;
       * przesyłanie informacji;
    10. Pozyskiwanie i utrzymywanie systemów informatycznych:
        * wymagania związane z bezpieczeństwem systemów informatycznych;
        * bezpieczeństwo w procesach wsparcia;
        * dane testowe;
    11. Relacje z dostawcami;
    12. Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
    13. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania:
        * ciągłość bezpieczeństwa informacji;
        * nadmiarowość;
    14. Zgodność:
        * zgodność z wymaganiami prawnymi i umownymi;
        * przeglądy bezpieczeństwa informacji;
    15. Analiza ryzyka w systemach informatycznych
15. **Wymagania odnośnie wdrożenia lub aktualizacji SZBI**
16. Wykonawca **w terminie 5 miesięcy** od dnia zawarcia umowy dokona aktualizacji i/lub sporządzenia dokumentacji SZBI w oparciu o Rozporządzenie KRI, normę PN-ISO/IEC 27001-2023 z uwzględnieniem Dyrektywy NIS 2 dla Urzędu Miejskiego w Nowym Tomyślu.

Efekt: Polityka bezpieczeństwa informacji Urzędu Miejskiego w Nowym Tomyślu opisująca system zarządzania bezpieczeństwem informacji, sporządzona w oparciu o Rozporządzenie KRI, normę PN-ISO/IEC 27001-2023 i z nią zgodna. Polityka Bezpieczeństwa Informacji UM w Nowym Tomyślu ma także uwzględniać wymogi zawarte w Dyrektywie NIS 2 oraz obowiązującej ustawie o Krajowym systemie cyberbezpieczeństwa.

1. **Wymagania odnośnie audytorów**
2. Posiada przynajmniej następujące kwalifikacje do przeprowadzania audytu:
   1. jeden z certyfikatów:

Certified Internal Auditor (CIA);

Certified Information System Auditor (CISA);

Certyfikat Audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami; Ustawy z dnia 13.04. 2016 r. o systemach zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338). W zakresie certyfikacji osób;

Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN-ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13.04.2016 r. o systemach; Oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

Certified Information Security Manager (CISM);

Certified in Risk and Information System Control (CRISC);

Certified in the Governance of Enterprisce IT (CGEIT);

Certified Information System Security Professional (CISSP);

System Security Certified Practicioner (SSCP);

Certified Reliability Professional;

Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

* 1. Audytor musi posiadać dwuletnie doświadczenie w przeprowadzaniu Audytów bezpieczeństwa.

Załącznik nr 1 - Szacunkowe dane do audytu