Załącznik nr 1 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Usługa wykonania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz przeprowadzenia audytów KRI niezależnie dla Starostwa Powiatowego w Aleksandrowie Kujawskim oraz jednostek organizacyjnych, w ramach projektu grantowego „Cyberbezpieczny samorząd", zgodnie z zapytaniem ofertowym tj. :

1. Zespołu Szkół Nr 1 w Aleksandrowie Kujawskim
2. Zespołu Szkół Nr 2 w Aleksandrowie Kujawskim
3. Liceum Ogólnokształcącego w Ciechocinku
4. Szkoły Podstawowej Specjalnej w Aleksandrowie Kujawskim
5. Placówki Socjalizacyjnej w Aleksandrowie Kujawskim
6. Domu Pomocy Społecznej w Zakrzewie
7. Poradni Psychologiczno-Pedagogicznej w Aleksandrowie Kujawskim
8. Powiatowego Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim
9. Powiatowego Urzędu Pracy w Aleksandrowie Kujawskim
10. Zarządu Dróg Powiatowych w Aleksandrowie Kujawskim

1. Przedmiotem zamówienia jest wykonanie jednego audytu KRI oraz dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (zwanej dalej SZBI) albo jej dostosowania, według wymagań wskazanych niżej norm i aktów prawnych niezależnie dla Starostwa Powiatowego i każdej z wskazanych wyżej jednostek organizacyjnych. Zamówienie realizowane w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd", Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027".
2. W ramach obecnie funkcjonującego SZBI Zamawiający posiada, w szczególności:
    1. Politykę Bezpieczeństwa Informacji w Starostwie Powiatowym w Aleksandrowie Kujawskim (zawierającą metodykę oraz zapisy dotyczące, m.in., zakresu, celów i zasad Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), organizacji bezpieczeństwa informacji, w tym ról i odpowiedzialności związanych z SZBI),
    2. Politykę Ochrony Danych Osobowych oraz procedurę zarządzania ryzykiem w ochronie danych osobowych oraz oceny skutków dla ochrony danych osobowych
    3. dokumentację bezpieczeństwa informacji - raporty i zestawienia z analizy ryzyk, wykazy zmian w dokumentacji, wykazy aktywów, rejestry incydentów, raporty na przegląd, raporty z audytów wewnętrznych, raporty z audytów zewnętrznych,
    4. dokumentację urządzeń mobilnych i pracy zdalnej - Zasady ochrony danych osobowych podczas pracy zdalnej, Zasady bezpiecznego wykonywania pracy zdalnej
    5. instrukcje dotyczące bezpieczeństwa informatycznego, fizycznego i osobowego
3. W ramach zadania Wykonawca dostosuje obecną albo opracuje nową dokumentację Systemu Zarządzania Bezpieczeństwem Informacji funkcjonującą u Zamawiającego.
4. Wykonawca dokona szczegółowej analizy obecnej dokumentacji SZBI Zamawiającego celem określenia jej zawartości i zakresu. Po przeprowadzonej analizie Wykonawca przestawi Zamawiającemu raport z audytu KRI, którego zakres i przedmiot opisany jest w pkt.6-7 oraz raport, na podstawie którego Wykonawca zdecyduje, czy będzie dostosowywał obecnie funkcjonującą u Zamawiającego dokumentację, czy też opracuje nową dokumentację.

5. Dokumentacja SZBI będzie wykonana w oparciu o wymagania określone w następujących aktach prawnych i normatywnych:
    1. Dyrektywa 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) (Dz.U. UE L 333 z 27.12.2022)
    2. Rozporządzenie 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. U. UE. L 119 z 4.5.2016)
    3. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077).
    4. Rozporządzenie 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. z 2024 r. poz. 773)
    5. PN-EN ISO/IEC 27001:2023-08 (lub równoważnej) Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji - Wymagania
    6. PN-EN ISO/IEC 27701:2021-09 (lub równoważnej) Techniki bezpieczeństwa -- Rozszerzenie do ISO/IEC 27001 i ISO/IEC 27002 (lub równoważnej) w zakresie zarządzania informacjami o ochronie prywatności - Wymagania i wytyczne
    7. PN-EN ISO/IEC 27002:2023-01 (lub równoważnej) Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Zabezpieczenia informacji
    8. PN ISO/IEC 27005:2022-10 (lub równoważnej) Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Wytyczne dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji
    9. PN-EN ISO 22301:2020-04 (lub równoważnej) Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania.
    10. PN-EN ISO/IEC 27017:2021-07 (lub równoważnej) Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 (lub równoważnej) dla usług w chmurze. Ponadto Wykonawca zobowiązany jest uwzględnić zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych tj. Narodowe Standardy Cyberbezpieczeństwa.
    11. Dokumentacja SZBI będzie zawierać zasady/zapisy/wymagania dla następujących obszarów:
        1. Obszar: Zabezpieczeń organizacyjnych
            1. Polityka bezpieczeństwa informacji
            2. Role i obowiązki w zakresie bezpieczeństwa informacji
            3. Podział obowiązków
            4. Odpowiedzialności kierownictwa
            5. Kontakt z organami władzy
            6. Kontakt z grupami szczególnego interesu
            7. Analiza zagrożeń

8. Bezpieczeństwo informacji w zarządzaniu projektami
9. Rejestr informacji i innych powiązanych zasobów
10. Dopuszczalne wykorzystanie informacji i innych powiązanych zasobów
11. Klasyfikacja informacji
12. Oznakowanie informacji
13. Transfer informacji
14. Kontrola dostępu
15. Zarządzanie tożsamością
16. Informacje uwierzytelniające
17. Prawa dostępu
18. Bezpieczeństwo informacji w relacjach z dostawcami
19. Uwzględnianie bezpieczeństwa informacji w umowach z dostawcami
20. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjnych i komunikacyjnych (ICT)
21. Monitorowanie, przegląd i zarządzanie zmianami w usługach dostawców
22. Bezpieczeństwo informacji przy korzystaniu z usług w chmurze
23. Planowanie i przygotowanie zarządzania incydentami bezpieczeństwa informacji
24. Ocena i decyzje dotyczące zdarzeń związanych z bezpieczeństwem informacji
25. Reagowanie na incydenty związane z bezpieczeństwem informacji
26. Wyciąganie wniosków z incydentów bezpieczeństwa informacji
27. Gromadzenie dowodów z naruszeń/incydentów związanych z bezpieczeństwem informacji
28. Bezpieczeństwo informacji w czasie zakłóceń związanych z bezpieczeństwem informacji
29. Gotowość technologii informacyjno-komunikacyjnych do zapewnienia ciągłości działania z elementami ISO 22301 (lub równoważnej)
30. Wymagania prawne, ustawowe, regulacyjne i umowne związanych z bezpieczeństwem informacji
31. Prawa własności intelektualnej
32. Ochrona zapisów
33. Prywatność i ochrona danych osobowych
34. Niezależny przegląd bezpieczeństwa informacji
35. Zgodność z polityką, zasadami i normami dotyczącymi bezpieczeństwa informacji
36. Udokumentowane procedury operacyjne

2. Obszar: Zabezpieczeń zasobów ludzkich
    1. Screening
    2. Zasady i warunki zatrudnienia
    3. Świadomość, edukacja i szkolenie w zakresie bezpieczeństwa
    4. Postępowanie dyscyplinarne w konsekwencji naruszeń/incydentów związanych z bezpieczeństwem informacji
    5. Obowiązki po rozwiązaniu lub zmianie zatrudnienia

6. Umowy o poufności lub nieujawnianiu informacji
7. Praca zdalna
8. Raportowanie zdarzeń dotyczących bezpieczeństwa informacji

3. Obszar: Zabezpieczeń fizycznych
    1. Strefy bezpieczeństwa fizycznego
    2. Dostęp fizyczny
    3. Zabezpieczanie biur, pomieszczeń i obiektów oraz kontrola dostępu przez wykonawców zewnętrznych
    4. Monitorowanie bezpieczeństwa fizycznego
    5. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
    6. Praca w obszarach chronionych
    7. Czyste biurko i czysty ekran
    8. Rozmieszczenie i ochrona urządzeń
    9. Bezpieczeństwo zasobów poza siedzibą firmy/organizacji
    10. Nośniki danych
    11. Urządzenia wspomagające
    12. Bezpieczeństwo okablowania
    13. Konserwacja sprzętu
    14. Bezpieczna utylizacja lub ponowne wykorzystanie sprzętu
4. Obszar Zabezpieczeń technologicznych
    1. Urządzenia końcowe użytkownika
    2. Prawa uprzywilejowanego dostępu
    3. Ograniczenie dostępu do informacji
    4. Dostęp do kodu źródłowego
    5. Bezpieczne uwierzytelnianie
    6. Zarządzanie wydajnością
    7. Ochrona przed złośliwym oprogramowaniem
    8. Zarządzanie lukami technicznymi
    9. Zarządzanie konfiguracją
    10. Usuwanie informacji
    11. Maskowanie danych
    12. Zapobieganie wyciekom danych
    13. Kopia zapasowa informacji
    14. Nadmiarowość urządzeń do przetwarzania informacji
    15. Rejestrowanie zdarzeń
    16. Monitorowanie działań
    17. Synchronizacja zegarów
    18. Użycie uprzywilejowanych programów narzędziowych
    19. Instalacja oprogramowania na systemach operacyjnych
    20. Bezpieczeństwo sieci
    21. Bezpieczeństwo usług sieciowych
    22. Rozdzielenie sieci
    23. Filtrowanie stron internetowych
    24. Zastosowanie kryptografii
    25. Cykl życia oprogramowania (SDLC)

26. Wymagania dotyczące bezpieczeństwa aplikacji
27. Architektura i zasady inżynierii bezpiecznych systemów
28. Testy bezpieczeństwa w fazie rozwoju i akceptacji
29. Zlecone prace rozwojowe
30. Oddzielenie środowisk rozwojowych, testowych i produkcyjnych
31. Zarządzanie zmianą
32. Dane testowe
33. Ochrona systemów informatycznych podczas audytu

12. W przypadku stwierdzenia w trakcie opracowania wymaganych dokumentów, że zasady/zapisy/wymagania/dane zabezpieczenie z w/w listy nie są stosowane w organizacji, Wykonawca przedstawi dodatkowy dokument w postaci raportu wykluczeń zabezpieczeń z dokładnym i precyzyjnym uzasadnieniem odstąpienia z opracowania wymagań dla takiego zabezpieczenia opisującym źródło takiej decyzji.
13. Zakres zamówienia obejmuje dostosowanie lub przygotowanie dokumentów o charakterze generalnym oraz szczegółowych procedur/instrukcji/zasad dotyczących funkcjonowania SZBI u Zamawiającego.
14. Wykonawca zweryfikuje dokumentację dot. ochrony danych osobowych i dostosuje ją do obowiązujących przepisów prawa, tak aby była spójna z System Zarządzania Bezpieczeństwem Informacji.
15. Wykonawca dokona analizy i identyfikacji procedur i procesów na potrzeby opracowywanej dokumentacji.
16. Wykonawca w ramach dokumentów uzupełniających SZBI przygotuje dokument bazowy SZBI obejmujący listę wszystkich wymagań norm ze wskazaniem:
    1. dokumentu lub dokumentów SZBI odnoszących się do konkretnego wymagania,
    2. opisu dowodów na spełnienie poszczególnych wymagań w tym określenia ich formy (np. plik logów, zdjęcie, dokument papierowy, dokument elektroniczny, plik konfiguracyjny, screenshot, wydruk z rejestru).
17. Wykonawca w ramach dokumentów uzupełniających SZBI przygotuje dokument: Wytyczne do rozwoju i utrzymania SZBI.
18. Wykonawca w ramach dokumentów SZBI dostosuje lub opracuje dokument SZBI związany z zarządzaniem ryzykiem bezpieczeństwa informacji oraz ryzykiem cyberodporności.
19. Wykonawca w ramach dokumentów uzupełniających SZBI przygotuje listę środków technicznych dla zapewnienia bezpieczeństwa informacji oraz cyberbezpieczeństwa z uwzględnieniem środków aktualnie wykorzystywanych przez Zamawiającego jak i planowanych wdrożeń w ramach projektu Cyberbezpieczny Samorząd.
20. Wykonawca w ramach dokumentów uzupełniających SZBI przygotuje listę wymagań związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem, aktualną na dzień odbioru.
21. Wykonawca w opracowanej dokumentacji, w szczególności:
    1. określi i sformalizuje zasady zarządzania, w szczególności poprzez wskazanie ról dla osób odpowiedzialnych oraz poprzez wskazanie podejścia do zapewnienia zasobów niezbędnych do efektywnego zarządzania

bezpieczeństwem informacji oraz cyberbezpieczeństwem i zarządzania usługami,

2. określi i sformalizuje procedury przeprowadzania technicznych audytów bezpieczeństwa, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników,
3. określi i sformalizuje procedury działań korygujących, w przypadku niezgodności z wymaganiami SZBI, z elementami ciągłości działania,
4. określi i sformalizuje procedury wprowadzania działań zapobiegawczych, w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami SZBI,
5. określi i sformalizuje procedury przeglądu SZBI, w szczególności określającej częstotliwość przeglądów, zakres i sposób ich przeprowadzania, materiały źródłowe niezbędne do przeprowadzenia przeglądu, tryb wdrażania wniosków/zaleceń,
6. określi i sformalizuje procedury nadzoru nad dokumentami wchodzącymi w skład SZBI,
7. określi i sformalizuje procedury nadzoru nad zapisami, określające zasady/zapisy/wymagania przechowywania, archiwizowania oraz niszczenia zapisów,
8. określi i sformalizuje procedury zarządzania ryzykiem informacji, oceny i zarządzania ryzykiem cyberodporności, przeprowadzi oceny ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, utraty poufności, integralności i dostępności informacji przetwarzanych przez organizację, wraz z przygotowaniem planu postępowania z ryzykiem zawierającego, m.in.:
    1. zdefiniowanie sposobu pomiaru ryzyka,
    2. zdefiniowanie i opisanie procesu zarządzania ryzykiem,
    3. zdefiniowanie i opisanie inwentaryzacji aktywów informacyjnych lub grup aktywów informacyjnych,
    4. zdefiniowanie i opisanie katalogu zagrożeń i oszacowanie prawdopodobieństw ich występowania na dzień sporządzenia i złożenia katalogu,
    5. zdefiniowanie i opisanie identyfikacji ryzyka, szacowanie ryzyk, rejestr ryzyk,
    6. zdefiniowanie i opisanie planu postępowania z ryzykami
    7. metodykę zarządzania ryzykiem SZBI
9. Wykonawca w dokumentacji uwzględni zmieniającą się infrastrukturę teleinformatyczną Zamawiającego.
10. Zamawiający zastrzega sobie prawo do wniesienia uwag do treści dokumentacji SZBI, zgłaszanych w trakcie procedury odbiorowej.
11. Potwierdzeniem wykonania dokumentacji SZBI będzie podpisany przez obie strony, z wynikiem pozytywnym, Protokół odbioru dokumentacji SZBI.
12. Umowa będzie realizowana w języku polskim.
13. Zadania związane z realizacją przedmiotu Umowy Wykonawca będzie wykonywał z uwzględnieniem określonych w Umowie terminów wykonania.

14. Wykonawca będzie zobligowany, do przeprowadzenia spotkań z naczelnikami/kierownikami wydziałów/biur Zamawiającego, w celu dokonania analizy i identyfikacji procedur i procesów na potrzeby opracowywanej dokumentacji - nie dopuszcza się spotkań w formie zdalnej.
15. Na zakończenie realizacji działań, Wykonawca będzie zobligowany do wdrożenia i przeprowadzenia szkoleń z wdrożonego SZBI dla naczelników/kierowników wydziałów/biur i jednostek organizacyjnych Zamawiającego w ilości min. 3h, w grupach dostosowanych do możliwości Wykonawcy w siedzibie Zamawiającego.
16. Na potrzeby opracowania przedmiotu zamówienia Zamawiający udostępni, w formie elektronicznej po podpisaniu Umowy, posiadane materiały i dokumenty SZBI.
17. Wykonawca będzie cyklicznie, co 7 dni, przekazywał Zamawiającemu informację o stanie i stopniu zaawansowania wytwarzanych w ramach realizacji zamówienia dokumentów, podczas spotkań organizowanych on-site lub on-line z pomocą komunikatora internetowego. Z każdego spotkania sporządzona zostanie notatka przez Wykonawcę (podlegająca akceptacji, co do treści przez Zamawiającego) o stanie i stopniu zaawansowania wytwarzanych dokumentów.
18. Zamawiający dopuszcza przesyłanie roboczych dokumentów projektowych drogą elektroniczną
19. W ramach procedury odbiorowej:
    1. Zaakceptowana dokumentacja SZBI zostanie przygotowana w języku polskim i przekazana Zamawiającemu najpóźniej w dniu jej odbioru w formie:
        a. papierowej, w 2 egzemplarzach (format A4, średnia liczba znaków na stronie - 1.900)
        b. oraz formie elektronicznej na adres poczty elektronicznej Zamawiającego wskazany w umowie, w formacie plików do edycji i PDF.
    2. Dokumenty będą zawierać wyłącznie autorskie treści powstałe w wyniku realizacji zamówienia oraz inne autorskie treści Wykonawcy, które nie są publicznie dostępne. Będą opracowaniem kompletnym i wyczerpującym z punktu widzenia celu, któremu mają służyć.

6. Zakres i przedmiot audytu KRI obejmuje przegląd systemów pod kątem zarządzania bezpieczeństwem informacji, umożliwiających realizację i egzekwowanie działań:
    1. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
    2. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
    3. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
    4. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu

adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5. bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
    1. zagrożenia bezpieczeństwa informacji,
    2. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
    3. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
    1. monitorowanie dostępu do informacji,
    2. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
    3. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
    1. dbałości o aktualizację oprogramowania,
    2. minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    3. ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    4. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
    5. zapewnieniu bezpieczeństwa plików systemowych,
    6. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
    7. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
    8. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13. bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
15. rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

7. W ramach realizacji przedmiotu zamówienia audytu KRI Wykonawca zobowiązany będzie do:
    1. dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, zgodnie z § 19 rozporządzeniem Rady Ministrów z dnia 21 maja 2024r. 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),
    2. opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami. Dokumentacja poaudytowa (raport) ma być przygotowana zgodnie z zasadami dostępności cyfrowej dokumentów tekstowych opisanymi na stronie https://www.gov.pl/web/dostepnosc-cyfrowa/jak-zwiekszyc-dostepnosc-cyfrowa-dokumentow-tekstowych oraz oznaczona pełnokolorowym znakiem Funduszy Europejskich, znakiem barw RP i znakiem UE lub znakiem monochromatycznym (zgodnie z Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji).