

Opis Przedmiotu Zamówienia (zwany „OPZ”)

Usługa polegająca na wykonaniu audytu wstępnego zgodności KRI oraz opracowaniu, przeglądzie, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta i Gminy w Sobkowie i jednostkach podległych: Zakład Wodociągi Gminne w Sobkowie, Miejsko-gminny Ośrodek Pomocy Społecznej w Sobkowie, Zespół Obsługi Ekonomiczno - Administracyjnej Oświaty w Sobkowie w ramach zadania „Projekt Grantowy Cyberbezpieczny Samorząd Etap III” współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Fundusze Europejskie na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa,

I. Ogólne warunki realizacji zamówienia

1. Przedmiotem zamówienia jest wykonanie audytu wstępnego zgodności KRI oraz opracowanie przez Wykonawcę dla Zamawiającego nowego systemu zarządzania bezpieczeństwem informacji, zwanego „nowym SZBI” oraz świadczenie usług asysty wdrożeniowej, zwanych „Usługami asysty” obejmującej wdrożenie, przegląd i aktualizację systemu, zgodnie z Umową, zwane „Przedmiotem Umowy”.
2. Przedmiot Umowy będzie realizowany w czterech etapach:
 - 1) **Etap I** – Audyt wstępny zgodności KRI
 - 2) **Etap II** – analiza działalności Zamawiającego i sporządzenie Sprawozdania, o którym mowa w tyt. III ust. 1 pkt 2;
 - 3) **Etap III** – opracowanie nowego SZBI;
 - 4) **Etap IV** – szkolenia z zakresu SZBI oraz Cyberbezpieczeństwa
 - 5) **Etap V** – świadczenie usług asysty wdrożeniowej, zwanych dalej „**Etapami**”, które szczegółowo określa niniejszy OPZ.
3. Wykonawca zobowiązuje się wykonać Przedmiot Umowy w terminie **do 180 dni kalendarzowych** licząc od dnia następnego po podpisaniu umowy.

II. ETAP I

Wykonawca zobowiązuje się do wykonania audytu wstępnego zgodności KRI/norm PN EN ISO/IEC 27001:2023 (ISO/IEC 27001:2022) zgodnie z przepisami prawa obowiązującymi w tym zakresie. Wyniki audytu będą podstawą do dalszych prac w UMiG, ZWG, MGOPS i ZOEO.

Audyt musi zostać wykonany po odbyciu wizji lokalnej we wszystkich wyżej wymienionych lokalizacjach. Jedynie w przypadku konieczności drobnych uzupełnień, dopuszczalna jest forma zdalna. W szczególności wymagany zakres prac obejmuje: Audyt wstępny bezpieczeństwa informacji i cyberbezpieczeństwa w UMiG, ZWG, MGOPS i ZOEO.

1. sprawdzenie i zrozumienie środowiska UMiG, ZWG, MGOPS i ZOEO., obejmujące aktualną strukturę organizacyjną, system zarządzania realizowanych procesów oraz wymagania prawne funkcjonujące w UMiG, ZWG, MGOPS i ZOEO.,

2. przegląd aktualnej dokumentacji bezpieczeństwa informacji w UMiG, ZWG, MGOPS i ZOEO., w tym polityk, procedur, instrukcji, regulaminów, wytycznych,

3. inwentaryzację i analizę aktywów - zasobów informacyjnych oraz środków służących do gromadzenia i przetwarzania informacji,

Wykonawca deklaruje, iż ocena zgodności z Krajowymi Ramami Interoperacyjności (zwanym dalej: KRI) / Krajowym Systemem Cyberbezpieczeństwa (zwanym dalej: KSC) przebiegać będzie zgodnie z poniższym schematem:

- wyznaczenie osoby do kontaktu - Art. 21 KSC,
- przekazanie danych osoby wyznaczonej - Art. 22 pkt 5) KSC,
- zapewnienie zarządzania incydem - Art. 22 pkt 1) KSC,
- zgłaszanie incydem - Art. 22 pkt 2) Art. 23 KSC,
- zapewnienie obsługi incydem - Art. 22 pkt 3) KSC,
- aktualizowanie regulacji wewnętrznych - Par. 19 ust. 2 pkt 1 KRI,
- inwentaryzacja sprzętu i oprogramowania - Par. 19 ust. 2 pkt 2 KRI,
- postępowanie z ryzykiem - Par. 19 ust. 2 pkt 3 KRI,
- zarządzanie uprawnieniami - Par. 19 ust. 2 pkt 4, 5 KRI,
- szkolenia i uświadamianie - Par. 19 ust. 2 pkt 6 KRI,
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami - Par. 19 ust. 2 pkt 7 KRI,
- ustanowienie zasad bezpiecznej pracy mobilnej, pracy zdalnej - Par. 19 ust. 2 pkt. 8 KRI,
- zabezpieczenie informacji przed nieuprawnionym ujawnieniem - Par. 19 ust. 2 pkt. 9 KRI,
- zawieranie w umowach serwisowych zapisów o bezpieczeństwie - Par. 19 ust. 2 pkt. 10 KRI,
- ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania - Par. 19 ust. 2 pkt. 11 KRI,
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych - Par. 19 ust. 2 pkt 12 KRI,
- zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok - Par. 19 ust. 2 pkt. 14 KRI,
- pozostałe wymogi zgodności KRI, KSC niezbędne do wdrożenia SZBI.

Z przeprowadzonego audytu w UMiG, ZWG, MGOPS i ZOEO. Wykonawca opracuje i przedłoży Zamawiającemu raport w wersji papierowej i elektronicznej (odrębny dla każdej jednostki). Raport musi zawierać również wyniki sprawdzonych zagadnień określonych w ankiecie Dojrzałości Cyberbezpieczeństwa - Załączniku nr 6. Raport z audytu powinien być podpisany przez audytora opracowującego audyt (podpis kwalifikowalny lub własnoręczny w przypadku przedłożenia wersji papierowej). Zamawiający zastrzega prawo do wniesienia uwag do przedłożonej dokumentacji, a Wykonawca zobowiązuje się do jej skorygowania i uwzględnienia wniesionych uwag.

III. ETAP II

1. W ramach Etapu II Wykonawca:

- 1) przeprowadzi analizę, zwaną dalej „Analizą”, której celem jest identyfikacja kontekstu SZBI u Zamawiającego, obejmującą w szczególności:
 - a) identyfikację i ocenę dokumentacji dotyczącej kwestii objętych SZBI funkcjonującej u Zamawiającego.
 - b) obszary działalności Zamawiającego i realizowanych zadań,
 - c) strukturę organizacyjną Zamawiającego,

- d) specyfikę pracy poszczególnych komórek organizacyjnych Zamawiającego,
 - e) systemy informatyczne użytkowane przez Zamawiającego,
 - f) rejestry publiczne pozostające we właściwości Zamawiającego,
 - g) wstępną identyfikację informacji przetwarzanych u Zamawiającego,
 - h) wstępną identyfikację ryzyk związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego;
- w ramach której Wykonawca dokona oceny ryzyk i szans niezbędnych do zaprojektowania nowego SZBI - również poprzez weryfikację działalności Zamawiającego m.in. w jego siedzibie;
- 2) sporządzi sprawozdanie, zwane dalej „**Sprawozdaniem**”:
- a) podsumowujące przeprowadzoną Analizę, w zakresie, o którym mowa w ust. 1 pkt 1,
 - b) obejmujące propozycje rozwiązań i zmian w zakresie bezpiecznego przetwarzania informacji u Zamawiającego i wprowadzenia u niego nowego SZBI,
 - c) obejmujące wstępną koncepcję nowego SZBI, dostosowaną do potrzeb Zamawiającego, w tym do ryzyk właściwych dla Zamawiającego, zidentyfikowanych w wyniku Analizy, w szczególności wskazującą na główne obszary i rodzaje procedur, które powinny zostać uregulowane nowym SZBI.
2. W celu przeprowadzenia Analizy Zamawiający udostępni Wykonawcy niezbędne, posiadane dokumenty, w szczególności dotyczące aktualnie funkcjonującego SZBI.
3. Sprawozdanie zostanie przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (.doc lub .docx) oraz w formie pisemnej.
4. Celem opracowania przez Wykonawcę wstępnej koncepcji nowego SZBI, Zamawiający wskazuje poniżej ogólny ramowy zarys nowego SZBI:
- Określenie struktury dokumentacji nowego SZBI, która powinna mieć układ hierarchiczny, tj. opisywać nowy SZBI na różnych poziomach szczegółowości oraz określać zagadnienia, które muszą zostać obligatoryjnie uregulowane:
- 1) poziom jednostki (Zamawiający) – nadrzędny dokument „Polityka Bezpieczeństwa Informacji” Zamawiającego, który określa wymagania i zasady bezpieczeństwa informacji obowiązujące u Zamawiającego oraz sposób organizacji nowego SZBI – z tym dokumentem powinny być spójne pozostałe dokumenty składające się na dokumentację nowego SZBI,
 - 2) poziom systemów teleinformatycznych – polityka bezpieczeństwa systemów teleinformatycznych, na którą składają się:
 - a) dokument „Polityka Bezpieczeństwa Systemów Teleinformatycznych”, który opisuje wymagania i zasady bezpieczeństwa dla systemów teleinformatycznych,
 - b) odniesienia co do wymagań dotyczących zakresu dokumentacji poszczególnych systemów teleinformatycznych – np. dokumenty: polityki bezpieczeństwa poszczególnych systemów teleinformatycznych, które opisują w jaki sposób zasady i wymagania bezpieczeństwa zawarte w „Polityce Bezpieczeństwa Informacji” i „Polityce Bezpieczeństwa Systemów Teleinformatycznych” są realizowane w danym systemie teleinformatycznym,
 - 3) poziom procedur, instrukcji i regulaminów – procedury, instrukcje, regulaminy i inne dokumenty SZBI tworzone w celu uszczegółowienia zasad opisanych w ww. politykach, dotyczące w szczególności następujących zagadnień:
 - a) bezpieczeństwo zasobów ludzkich,
 - b) bezpieczeństwo fizyczne,
 - c) bezpieczeństwo cyberprzestrzeni,
 - d) bezpieczeństwo danych osobowych,
 - e) bezpieczeństwo informacji niejawnych,

- f) obsługa incydentów,
 - g) zarządzanie ryzykiem,
 - h) użytkowanie systemów teleinformatycznych,
 - i) użytkowanie urządzeń mobilnych.
5. Ramowy zarys nowego SZBI, o którym mowa w ust. 4, nie ma charakteru bezwzględnie wiążącego i stanowi jedynie propozycję Zamawiającego. W przypadku nieuwzględnienia przez Wykonawcę we wstępnej koncepcji nowego SZBI ramowego zarysu lub jego poszczególnych elementów, Wykonawca uzasadni powyższe Zamawiającemu.

IV. ETAP III

1. W ramach Etapu II Wykonawca, na podstawie wyników Analizy i zaakceptowanego przez Zamawiającego Sprawozdania, opracuje nowy SZBI, dostosowany do potrzeb Zamawiającego.
2. Nowy SZBI, który opracuje Wykonawca, będzie stanowił system zarządzania bezpieczeństwem informacji, o którym mowa w § 19 ust. 1 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. z 2024 roku poz. 773) bądź w zastępujących go, odpowiednich przepisach wykonawczych do ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2024 r. poz.1557) w przypadku ich nowelizacji, zwany „SZBI”.

Rozporządzenie, o którym mowa w zdaniu poprzedzającym, zwane jest dalej „**rozporządzeniem KRI**”.

3. Nowy 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:
- a) Polityka Bezpieczeństwa;
 - b) Organizacja bezpieczeństwa informacji;
 - c) Bezpieczeństwo zasobów ludzkich;
 - d) Zarządzanie aktywami;
 - e) Kontrola dostępu;
 - f) Kryptografia;
 - g) Bezpieczeństwo fizyczne i środowiskowe;
 - h) Bezpieczna eksploatacja;
 - i) Bezpieczna komunikacja;
 - j) Pozyskiwanie, rozwój i utrzymanie systemów;
 - k) Relacje z dostawcami;
 - l) Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
 - m) Aspekty bezpieczeństwa w zarządzaniu ciągłością działania;
 - n) Zgodność z wymaganiami prawnymi i własnymi standardami.

Ponadto, nowy SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762.

4. Nowy 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* (Dz. U. z 2024 r., poz. 1557)
 - 5) ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (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* (Dz. U. z 2024 r. poz. 1112);
 - 7) ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2024 r., poz. 632);
 - 8) ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2024 r., poz. 1077);
 - 9) dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z 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 uwzględniać wewnętrzne akty prawne obowiązujące u Zamawiającego.
5. W ramach opracowania nowego SZBI Wykonawca między innymi:
- 1) zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;
 - 2) uwzględni w szczególności następujące zagadnienia:
 - a) określenie organizacji bezpieczeństwa informacji,
 - b) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
 - c) szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
 - d) bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
 - e) kontrola dostępu,
 - f) bezpieczeństwo fizyczne i środowiskowe,
 - g) klasyfikacja informacji,
 - h) odpowiedzialność za zasoby,
 - i) postępowanie z nośnikami informacji,
 - j) użytkowanie urządzeń mobilnych i praca zdalna,
 - k) zarządzanie sprzętem informatycznym,
 - l) instalacja oprogramowania,
 - m) ochrona przed oprogramowaniem złośliwym,
 - n) kopie zapasowe,
 - o) zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
 - p) zarządzanie dokumentacją infrastruktury informatycznej,
 - q) monitorowanie systemów informatycznych,
 - r) zarządzanie pojemnością,
 - s) serwis i konserwacja infrastruktury informatycznej,
 - t) zarządzanie podatnościami technicznymi,
 - u) zarządzanie incydentami bezpieczeństwa,

- v) zabezpieczenia kryptograficzne,
 - w) bezpieczeństwo sieci i transmisji danych,
 - x) ochrona własności intelektualnej,
 - y) bezpieczeństwo informacji w relacjach z dostawcami,
 - z) ciągłość działania,
 - aa) zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
 - bb) weryfikacja zgodności z wymaganiami prawnymi,
 - cc) korzystanie z poczty elektronicznej i Internetu,
 - dd) zarządzanie usługami informatycznymi,
 - ee) utrzymanie i doskonalenie SZBI,
 - ff) przeprowadzanie audytów SZBI.
6. Wykonawca wraz z nowym SZBI przedstawi zestawienie, zwane dalej „**Zestawieniem**”, w którym wykaże spełnienie przez nowy SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, w tym rozporządzenia KRI, a także odpowiednich norm.
7. Nowy SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (.doc lub .docx) oraz w formie pisemnej.
8. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę nowego 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.

V. ETAP IV

1. Wykonawca przeprowadzi szkolenia z pracownikami merytorycznymi oraz kierownictwem na których wyjaśni czym jest SZBI, na podstawie jakich przepisów prawa wdrażane jest SZBI, konsekwencje nieprzestrzegania SZBI, jak klasyfikować informacje oraz na podstawie opracowanej polityki do Analizy Ryzyka przeszkoli pracowników z metodyki szacowania ryzyka. Osób do przeszkolenia jest na moment opublikowania zapytania ofertowego 55 w tym 10 osób z kadry kierowniczej
2. Wykonawca przeprowadzi szkolenia z pracownikami merytorycznymi oraz kierownictwem z zakresu Cyberbezpieczeństwa na którym omówi kwestie: Osintu, phishing, malware, przykład socjotechnik stosowanych przez hakerów, jak rozpoznawać i unikać cyberzagrożenia, dobre praktyki minimalizujące ryzyko cyberataku. Osób do przeszkolenia jest na moment opublikowania zapytania ofertowego 55 w tym 10 osób z kadry kierowniczej

ETAP V

1. W ramach Etapu III Wykonawca będzie świadczył Usługi wdrożeniowe w następującym zakresie:
 - 1) przeprowadzenie procesów:
 - a) identyfikacji aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,

- b) szacowania ryzyka oraz postępowania z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
 - z udziałem wyznaczonych w tym celu pracowników Zamawiającego;
 - 2) wyjaśnianie zagadnień ujętych w nowym SZBI i proponowanie rozwiązań w zakresie jego wdrażania;
 - 3) pomoc w rozwiązywaniu bieżących problemów, które mogą pojawić się w toku funkcjonowania nowego SZBI;
 - 4) pomoc w modyfikacji dokumentacji Zamawiającego związanej z bezpieczeństwem informacji, w szczególności nowego SZBI (np. poprzez zmianę poszczególnych elementów składowych lub opracowanie nowych elementów).
2. Usługi asysty świadczone będą zdalnie (w szczególności za pośrednictwem poczty elektronicznej lub telefonu) lub w siedzibie Zamawiającego. Decyzja o formie świadczenia Usług asysty zależeć będzie od ich charakteru i każdorazowo należy do Zamawiającego.
3. Wykonawca zobowiązany jest uwzględnić w ofercie **40 godz.** doradztwa wdrożeniowego.

VI. Organizacja realizacji przedmiotu zamówienia

1. Wykonawca wyznaczy, spośród pracowników jednostek oddelegowanych do realizacji zamówienia, zespół do realizacji i współpracy.
2. Zespół Projektu będzie posiadał pełną wiedzę o realizowanym projekcie oraz będzie odpowiedzialny za komunikację w projekcie i podpisywanie raportów częściowych z etapów realizacji prac, przedstawianie harmonogramów oraz ewentualnych zmian.
3. W ramach każdego etapu Wykonawca przeprowadzi przynajmniej jedno spotkanie inicjujące, na którym poinformuje w szczególności o harmonogramie pracy, sposobie realizacji, celach, produktach częściowych, kamieniach milowych.
4. W ramach etapów II-III Wykonawca powinien przewidzieć konsultacje w siedzibie Zamawiającego oraz jednostce podległej.
5. Wykonawca wymaga informowania w formie pisemnej o przebiegu realizacji prac z uwzględnieniem każdego etapu.
6. Każdy etap prac uznaje się za zakończony po przyjęciu przez obie strony raportu z zakończenia prac danego etapu.
7. Informacje, które będą przekazywane w celu realizacji niniejszego projektu, stanowią informacje chronione, w związku z tym realizacja projektu będzie wymagała akceptacji zapisów o zachowaniu poufności i zapewnieniu stosownej ochrony, w tym również dla danych osobowych.
8. Wszystkie dokumenty sporządzone będą w formie pisemnej w języku polskim, w formie papierowej oraz formie elektronicznej w formacie danych .pdf oraz jednym z formatów edytowalnych: .doc, .rtf, .xlsx.
9. Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty niniejszego zamówienia.
10. Wykonawca w ramach 24-miesięcznej gwarancji, liczonej od dnia zakończenia ostatniego etapu, zobowiązany będzie do poprawy błędów w przekazanej dokumentacji niezależnie od formy jej wytworzenia, w terminie nie dłuższym niż 30 dni od daty zgłoszenia błędu przez Zamawiającego. Z uwagi na zapisy konkursowe Wykonawca oświadcza, że usługi gwarancyjne świadczone po dniu zakończenia projektu przez Zamawiającego, są usługami świadczonymi nieodpłatnie.

VII. Wymagania dodatkowe:

1. Dokumentacja:

- a. Dokumentacja związana z realizacją usługi powinna zostać przygotowana zgodnie z wymogami Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027.
- b. Dokumenty należy oznaczyć logotypami Programu, zgodnie z wytycznymi projektu „Cyberbezpieczny Samorząd”.
- c. dla uczestników szkolenia wykonawca przygotowuje certyfikaty potwierdzające uczestnictwo w szkoleniu