Załącznik nr 6 do SWZ

Szczegółowy opis przedmiotu zamówienia

1. Przedmiot zamówienia:

Część 1

Doradztwo w zakresie wdrożenia rozwiązań technicznych:

1. **Nadzór nad wdrożeniem rozwiązań technicznych - bieżące monitorowanie i weryfikacja procesów realizowanych przez zespół IT gminy oraz firmy wykonawcze na etapie wdrażania elementów projektu, w tym:**
2. infrastruktura serwerowa i pamięci masowej - nadzór nad wdrożeniem klastra serwerów R450 oraz macierzy ME5024, z uwzględnieniem redundancji, konfiguracji RAID, optymalizacji wydajności i procedur bezpieczeństwa;
3. migracja środowisk wirtualnych (VM → HV) - weryfikacja planu migracji, testów przedprodukcyjnych i minimalizacja przestojów;
4. systemy NAS i backup - kontrola wdrożenia urządzenia QNAP TS-1273AU-RP-8G z pełnym wyposażeniem (12 HDD, 2 SSD), pięcioletnią gwarancją oraz systemu backupu Xopero One dla 35 urządzeń i 8 maszyn wirtualnych;
5. systemy monitoringu i bezpieczeństwa - nadzór nad przedłużeniem i konfiguracją licencji Axence nVision, DA Drive Analyzer oraz wdrożeniem Graylog w roli centralnego systemu logowania i analizy zdarzeń;
6. infrastruktura sieciowa - kontrola montażu i konfiguracji przełączników NETGEAR M4300-12X12F / Aruba 2540 oraz punktów dostępowych Ubiquity AP w celu stworzenia bezpiecznej i wydajnej sieci przewodowej i bezprzewodowej;
7. zasilanie awaryjne - weryfikacja instalacji i testów backupu zasilania UPS EVER POWERLINE RT PRO 3000.
8. **Konsultacje techniczne, w tym:**
9. doradztwo w wyborze optymalnych rozwiązań konfiguracyjnych;
10. wsparcie przy integracji nowych systemów z istniejącą infrastrukturą;
11. pomoc w planowaniu polityk backupu, retencji danych i zabezpieczeń;
12. konsultacje w zakresie cyberbezpieczeństwa, segmentacji sieci oraz monitoringu.
13. **Koordynacja i raportowanie, w tym:**
14. koordynacja i nadzór nad istniejącym harmonogramem.;
15. tworzenie raportów okresowych dokumentujących postęp prac, problemy oraz rekomendowane działania korygujące;
16. koordynacja komunikacji pomiędzy wszystkimi uczestnikami projektu;
17. Weryfikacja zgodności dokumentacji powykonawczej.

Czas realizacji zadania – 66 godzin w siedzibie Zamawiającego w okresie do 120 dni kalendarzowych od dnia zawarcia umowy. Termin, 120 dni kalendarzowych jest odzwierciedleniem maksymalnego terminu wykonania przedmiotu umów dotyczących zakupu sprzętu komputerowego oraz oprogramowania w ramach projektu „Cyberbezpieczny Samorząd”, w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: - Zaawansowane usługi cyfrowe, działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, dofinansowanego ze środków Unii Europejskiej oraz budżetu państwa na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/2189/ FERC.02.02-CS.01- 001/23/2024 zawartej ze Skarbem Państwa, w imieniu którego działa Centrum Projektów Polska Cyfrowa. W przypadku zmiany terminu wykonania przedmiotu umów, o którym mowa wyżej, dopuszcza się zmianę okresu realizacji przedmiotu zamówienia objętego niniejszym postępowaniem.

Część 2:

1. W celu zapewnienia należytego i sprawnego wykonania zamówienia maksymalna odległość siedziby Wykonawcy od siedziby Zamawiającego nie może przekraczać 150 km.
2. Zamawiający posiada do 30 stanowisk komputerowych oraz 1 serwerownię.
3. Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzonej przez siebie dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji przedmiotu zamówienia.
4. Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym koszty swojego ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku, skanu i wysyłki dokumentów.
5. Wykonawca zobowiązany będzie do zachowania poufności wszelkich informacji uzyskanych w trakcie realizacji przedmiotu zamówienia. Przed rozpoczęciem prac podpisana zostanie umowa o zachowaniu poufności.
6. Zamówienie należy wykonać w szczególności w oparciu o:
7. ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t. j. Dz. U. z 2024 r. poz. 1557) (w zakresie dotyczącym bezpieczeństwa informacji),
8. rozporządzenie Rady Ministrów z dnia 21 maja 2024 roku 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) (w zakresie dotyczącym bezpieczeństwa informacji),
9. 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. Urz. UE L 119 z 4.5.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.5.2018, str. 2 i Dz. Urz. UE L 074, 4.3.2021, s. 35)
10. ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781)
11. ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077, z późn. zm.),
12. 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)
13. normy ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27701, ISO/IEC 27017 oraz ISO/IEC 22301, PN-ISO 31000 lub równoważne,
14. wytyczne i poradniki Ministerstwa Cyfryzacji w zakresie bezpieczeństwa informacji oraz ochrony danych osobowych (www.gov.pl) w tym m.in. Poradnik – Cyberbezpieczny Samorząd.

Etap 1. Przegląd obecnie obowiązującej dokumentacji z zakresu Systemu Zarządzania Bezpieczeństwem Informacji [zwanego dalej, także SZBI] – przeprowadzenie audytu wstępnego (diagnostycznego) jako elementu rozpoznania spełnienia przez Zamawiającego wymagań organizacyjno-technicznych, prawnych, zgodności z normami ISO oraz opracowania założeń do Systemu Zarządzania Bezpieczeństwem Informacji:

* + - * 1. W ramach zadania Wykonawca przeprowadzi przegląd obecnie obowiązującej dokumentacji z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), tj. audyt wstępny (diagnostyczny) funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji w siedzibie Zamawiającego.
        2. Zamawiający wymaga, aby wszystkie prace związane z przeprowadzeniem wywiadów, analiz wśród pracowników Zamawiającego realizowane były przez Wykonawcę w siedzibie Zamawiającego. Zamawiający wyklucza możliwość stosowania ankiet do samodzielnego wypełnienia przez pracowników Zamawiającego. Podstawę audytu wstępnego będą stanowiły, co najmniej:
  + wywiady z pracownikami przeprowadzone w siedzibie Zamawiającego,
  + obserwacje lub wywiady audytora, dotyczące bezpieczeństwa fizycznego i środowiskowego,
  + obserwacje lub wywiady audytora, dotyczące bezpieczeństwa serwerowni Zamawiającego,
  + obserwacje lub wywiady audytora dotyczące bezpieczeństwa wskazanych przez Zamawiającego systemów teleinformatycznych i systemu księgowo-finansowego,
  + zgromadzone materiały audytowe w postaci dokumentacji bezpieczeństwa informacji i organizacyjnej obowiązującej u Zamawiającego.
    - * 1. Wykonawca sporządzi plan audytu wstępnego, zawierający co najmniej listę planowanych działań audytowych, o których mowa w pkt b) oraz dla każdego z działań: termin wykonania działania, komórkę organizacyjną Zamawiającego, listę dowodów do przygotowania.
        2. Przeprowadzany audyt wstępny uwzględniać będzie weryfikację na dzień audytu co najmniej 50% dokumentacji SZBI Zamawiającego, w tym regulaminów, polityk, zasad, wytycznych, procedur i instrukcji bezpieczeństwa informacji oraz analizy środowiska i zasobów teleinformatycznych (m.in badanie ich stosowania. Zamawiający zastrzega sobie prawo do niewysyłania obszernej dokumentacji, polityk, procedur, jeżeli uzna, że czas poświęcony na jej skanowanie będzie niewspółmierny do zamierzonego celu.
        3. Audyt wstępny będzie uwzględniał co najmniej następujące obszary określone w normie ISO/IEC 27001:
* kontekst organizacji,
* polityki bezpieczeństwa informacji i inne dokumenty dotyczące bezpieczeństwa informacji,
* organizacja bezpieczeństwa informacji,
* postępowanie z ryzykiem w bezpieczeństwie informacji,
* bezpieczeństwo zasobów ludzkich,
* zarządzanie aktywami,
* kontrola dostępu,
* kryptografia,
* bezpieczeństwo fizyczne i środowiskowe,
* bezpieczna eksploatacja,
* bezpieczeństwo komunikacji,
* pozyskiwanie, rozwój i utrzymanie systemów,
* relacje z dostawcami,
* zarządzanie incydentami związanymi z bezpieczeństwem informacji,
* zarządzanie ciągłością działania,
* zgodność z obowiązującymi przepisami prawa.
  + - * 1. Efektem realizacji zadania będzie zbiorczy raport z przeprowadzonego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie papierowej i elektronicznej. Raport będzie zawierał co najmniej:
  + podsumowanie zarządcze,
  + opis wykonania planu audytu,
  + opis wykorzystanych standardów,
  + ocenę spełnienia wymagań,
  + wydanie rekomendacji w przypadku stwierdzonych niezgodności i braków, które będą stanowiły podstawę do aktualizacji, dostosowania lub przygotowania i wdrożenia dokumentacji SZBI.
    - * 1. Czas realizacji Zadania – 30 dni kalendarzowych od dnia zawarcia umowy.

Etap 2. Przeprowadzenie audytu zgodności Systemu Zarządzania Bezpieczeństwem Informacji z wymaganiami KRI, w tym:

1. **Opracowanie/aktualizacja i wdrożenie dokumentów Systemu Zarządzania.**

Wykonawca na podstawie sprawozdania z wykonania zadania dotyczącego przeprowadzenia przeglądu obecnie obowiązującej dokumentacji z zakresu SZBI, tj. Audytu wstępnego (diagnostycznego) jako elementu rozpoznania spełnienia przez Zamawiającego wymagań organizacyjno-technicznych, prawnych, zgodności z norami ISO oraz opracowania założeń do Systemu Zarządzania Bezpieczeństwem Informacji:

1. odpowiednio zaktualizuje/opracuje i wdroży dokumentację Systemu Zarządzania Bezpieczeństwem Informacji funkcjonującą w Urzędzie Gminy Dygowo;
2. dokumentacja SZBI uwzględniać będzie dotychczasową dokumentację Zamawiającego, założenia do SZBI przedstawione przez Zamawiającego i rekomendacje opracowane w wyniku przeprowadzenia audytu wstępnego określonego dla etapu 1-go;
3. dokumentacja SZBI będzie wykonana również w oparciu o wymagania ustawy o ochronie danych osobowych, RODO, ustawy o krajowym systemie cyberbezpieczeństwa, dyrektywy NIS2 i norm ISO w tym norm wykorzystanych w dokumentacji Zamawiającego;
4. dokumentacja SZBI musi uwzględniać wymagania wynikające z wyżej wymienionych norm i obejmować, co najmniej poniższe obszary:
   * polityka bezpieczeństwa informacji,
   * organizacja bezpieczeństwa informacji,
   * bezpieczeństwo zasobów ludzkich,
   * zarządzanie aktywami,
   * przekazywanie nośników kontrola dostępu,
   * kryptografia,
   * bezpieczeństwo fizyczne i środowiskowe,
   * bezpieczna eksploatacja,
   * bezpieczeństwo komunikacji,
   * pozyskiwanie, rozwój i utrzymanie systemów,
   * relacje z dostawcami,
   * zarządzanie incydentami związanymi z bezpieczeństwem informacji,
   * bezpieczeństwo informacji w zarządzaniu ciągłością działania,
   * zgodność,
5. wykonawca w ramach dokumentów SZBI:
   * przygotuje dokument bazowy SZBI obejmujący listę wszystkich wymagań z norm ze wskazaniem,
   * przygotuje dokument Wytyczne do rozwoju i utrzymania SZBI,
   * zaktualizuje/opracuje i wdroży dokument SZBI związany z zarządzaniem ryzykiem bezpieczeństwa informacji,
   * przygotuje listę środków technicznych dla zapewnienia bezpieczeństwa informacji z uwzględnieniem środków aktualnie wykorzystywanych i planowanych do zakupu przez Zamawiającego w ramach niniejszego projektu,
   * przygotuje listę środków organizacyjnych dla zapewnienia bezpieczeństwa informacji z uwzględnieniem środków aktualnie wykorzystywanych i planowanych do zakupu przez Zamawiającego w ramach niniejszego projektu.
6. Wykonawca realizując zadanie uwzględni infrastrukturę teleinformatyczną Zamawiającego;
7. Wykonawca przygotuje harmonogram opracowania poszczególnych dokumentów SZBI, o których mowa w pkt. a) – e);
8. harmonogram Wykonawca przekaże Zamawiającemu w terminie do 7 dni kalendarzowych od zakończenia realizacji zadania opisanego w pkt. 1, uzgodnienie harmonogramu realizacji odbywać się będzie drogą elektroniczną poprzez skrzynkę email osoby wskazanej do kontaktu lub adres email: ug@dygowo.pl;
9. Zamawiający zastrzega sobie prawo do wniesienia uwag do treści dokumentacji SZBI, zgłaszanych w trakcie procedury odbiorowej.
10. Wykonawca przygotuje harmonogram wdrożenia SZBI. Uzgodnienie harmonogramu realizacji odbywać się będzie drogą elektroniczną poprzez skrzynkę email osoby wskazanej do kontaktu lub adres email: sekretarz@dygowo.pl.
11. warunkiem odbioru zadania jest wykonanie wszystkich elementów tego zadania oraz akceptacja przez Zamawiającego wytworzonych i przekazanych Zamawiającemu, w ramach realizacji w/w zadania dokumentów;
12. potwierdzeniem wykonania zadania , będzie podpisany z wynikiem pozytywnym przez strony Protokół Odbioru zadania po wykonaniu czynności związanych z wdrożeniem dokumentacji.
13. **Przeprowadzenie szkoleń specjalistycznych dla kadry zarządzającej oraz pracowników w zakresie wdrażanego Systemu Zarządzania Bezpieczeństwem Informacji:**
14. w ramach zadania, pracownicy zostaną przeszkoleni z obszaru Bezpieczeństwa Informacji. Cały program szkolenia będzie opierał się o materiały, które zostały stworzone w poprzednich zadaniach, tak by podnieść świadomość w zakresie zapewnienia bezpieczeństwa w Urzędzie Gminy. Szkoleniem objęta zostanie zarówno kadra zarządzająca jak i pracownicy. Wykonawca podejmie takie działania jak:

* Przygotowanie materiałów szkoleniowych dla pracowników.
* Przeprowadzenie szkoleń pracowników. Szkolenia dedykowane i dostosowane odpowiednio dla każdej z grup (tj. dla kadry zarządzającej i pracowników), z wdrożonymi zasadami i procedurami, jak również z korzyściami wynikającymi ze skutecznego wdrażania SZBI.

1. Wykonawca przygotuje program szkolenia obejmujący m.in. następujące zagadnienia:

* wymogi dla urzędu Gminy wynikające z Krajowych Ram Interoperacyjności (KRI), Ustawy o krajowym systemie cyberbezpieczeństwa (UoKSC), NIS 2 i Ogólnego rozporządzenia o ochronie danych osobowych(RODO),
* zadania pracowników wynikające z KRI, UoKSC, NIS 2, oraz RODO,
* przedstawienie pracownikom wdrożonej/zaktualizowanej dokumentacji SZBI Zamawiającego i wewnętrznych procedur w obszarze bezpieczeństwa informacji w tym danych osobowych,
* System Zarządzania Bezpieczeństwem Informacji w praktyce,
* System Zarządzania Ciągłością Działania – dlaczego jest istotny i jak działa,
* zarządzanie ryzykiem w bezpieczeństwie informacji,
* Identyfikowanie zagrożeń – przestrzeganie zasad bezpieczeństwa,
* naruszenia ochrony danych osobowych i odpowiedzialność pracowników,
* bezpieczne hasła i uwierzytelnienie dwuskładnikowe,
* wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

1. w ramach realizacji zadania Wykonawca zorganizuje i przeprowadzi szkolenia stacjonarne w siedzibie Zamawiającego, w godzinach pracy Urzędu;
2. przeprowadzenie szkoleń z zakresu Systemu Zarządzania Bezpieczeństwem Informacji dla następujących użytkowników:

* szkolenie dla kadry zarządzającej – czas trwania 5 godzin lekcyjnych dla max 15 osób,
* szkolenie dla pracowników – 5 godzin lekcyjnych dla max 30 osób, w dwóch grupach po ok. 15 osób,
* Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników szkoleń w wersji papierowej, które zostaną przekazane Zamawiającemu, nie później niż w dniu rozpoczęcia szkolenia;

1. Wszystkie dokumenty i materiały opracowane przez Wykonawcę winny zostać oznakowane za pomocą:

* znaku Fundusze Europejskie wraz z nazwą Programu,
* barw Rzeczpospolitej Polskiej,
* znaku Unii Europejskiej wraz ze słownym odniesieniem „Dofinansowane przez Unię Europejską”,
* znaku Cyberbezpieczny Samorząd (po linii rozdzielającej).

1. Szczegółowe informacje i przykłady dotyczące zastosowania powyższych wymagań zostały określone w „Podręczniku wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji” oraz w Księdze Tożsamości Wizualnej marki Fundusze Europejskie 2021-2027 - materiały w formie elektronicznej są dostępne w serwisie internetowym pod adresem: www.funduszeeuropejskie.gov.pl;
2. Wykonawca po zakończeniu szkolenia wyda każdemu uczestnikowi imienne zaświadczenie o jego ukończeniu, które będzie zawierało następujące informacje: imię i nazwisko uczestnika, tytuł szkolenia, liczbę godzin, tematykę, datę przeprowadzenia szkolenia, pieczątkę Wykonawcy, identyfikowalny podpis trenera prowadzącego szkolenie. Warunkiem wydania zaświadczenia jest obecność uczestnika na szkoleniu;
3. w ramach zadania Wykonawca zapewni udział w przeprowadzeniu analizy ryzyka w oparciu o metodykę zgodną z ISO 27001, udostępni oprogramowanie służące do przeprowadzenia analizy ryzyka i do zarządzania ryzykiem wraz z co najmniej 2 letnią subskrypcją na użycie tego oprogramowania;
4. czas realizacji zadań opisanych w ust. 2 pkt. 1) i 2) – łącznie 90 dni kalendarzowych od dnia zawarcia umowy.
5. **przeprowadzenie audytu końcowego i sporządzenie raportu:**
6. W audycie końcowym powinny zostać w szczególności uwzględnione (opis celów audytu - wyjaśnienie, jakie cele były do osiągnięcia oraz na jakich obszarach skupiał się audyt):

* zakres audytu - szczegółowy opis zakresu audytu, w tym analizowane systemy, procedury i procesy związane z bezpieczeństwem informacji;
* metodologia - opis metodologii i narzędzi wykorzystanych podczas audytu, w tym techniki testowania i analizy ryzyka;
* wyniki audytu - zestawienie wyników audytu, w tym identyfikowane zagrożenia, słabości i niezgodności z przyjętymi normami i standardami;
* rekomendacje - zalecenia dotyczące działań naprawczych, które należy podjąć w celu poprawy poziomu bezpieczeństwa informacji;
* ocena zgodności - ocena zgodności z obowiązującymi przepisami prawnymi i regulacjami dotyczącymi bezpieczeństwa informacji;
* podsumowanie - krótkie podsumowanie przeprowadzonych działań, głównych ustaleń i rekomendacji;
* załączniki - dokumentacja pomocnicza, takie jak wykresy, tabele, i inne materiały wspierające wyniki audytu;

1. efektem realizacji zadania będzie raport z przeprowadzonego końcowego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie papierowej i elektronicznej, raport będzie zawierał co najmniej:

* ocenę spełnienia wymagań,
* określenie statusu działań: zrealizowane/częściowo zrealizowane/niezrealizowane,
* opis zrealizowanych działań,
* wnioski z audytu (niezgodności, potencjały, uwagi).

1. Zamawiający zastrzega sobie prawo wniesienia uwag do treści raportu z audytu końcowego;
2. po wykonaniu audytu końcowego Wykonawca dokona, przy udziale kadry zarządzającej szczegółowego omówienia wyników audytu;
3. czas realizacji zadania - 120 dni kalendarzowych od dnia zawarcia umowy.

Etap 3. Udział we wdrożeniu zaktualizowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w tym w analizie ryzyka - zapewnienie Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji i wsparcia w przygotowaniu audytów wewnętrznych i przeprowadzania przeglądu zarządzania w oparciu o przygotowaną i wdrożoną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w terminie min. 2 lat od zakończenia Projektu (co zgodnie z zawartą umową o powierzenie grantu nastąpi do dnia 30.06.2026 r.).

Do zadań Pełnomocnika ds. SZBI (osoby posiadającej Certyfikat audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji według normy PN-EN ISO/IEC 27001), należą:

1. nadzorowanie i koordynowanie działań Referatów i samodzielnych stanowisk, związanych z wykonywaniem zadań wynikających z SZBI nadzorowanie realizacji przyjętej Polityki Bezpieczeństwa Informacji,
2. przedstawianie podczas Przeglądów Zarządzania sprawozdań dotyczących funkcjonowania SZBI,
3. opiniowanie klasyfikacji informacji,
4. weryfikowanie realizacji planu minimalizacji ryzyka,
5. inicjowanie działań korygujących i weryfikacja ich realizacji,
6. inicjowanie i nadzorowanie przebiegu audytów wewnętrznych SZBI,
7. prowadzenie i przechowywanie dokumentacji związanej z wdrażaniem i realizacją SZBI,
8. dbanie o aktualność dokumentów opisujących podstawowe elementy funkcjonowania SZBI,
9. monitorowanie i ewidencjonowanie pojawiających się niezgodności z przyjętymi dokumentami dotyczącymi bezpieczeństwa informacji,
10. ocena skuteczności wdrożonego SZBI,
11. promocja zasad bezpieczeństwa informacji.

Czas realizacji zadania – od 01.07.2026r. – 30.06.2028r.