

OPIS PRZEDMIOTU ZAMÓWIENIA

SŁOWNIK POJĘĆ I SKRÓTÓW UŻYTYCH W OPZ

Zamawiający	Powiat Ciechanowski.
Projekt	Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1491/ FERC.02.02-CS.01-001/23/2024 "Cyberbezpieczny Samorząd"; Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa
Jednostki Zamawiającego	<p>Wszystkie Jednostki Organizacyjne Powiatu Ciechanowskiego biorące udział w projekcie.</p> <ol style="list-style-type: none"> 1. Starostwo Powiatowe w Ciechanowie 2. Dom Pomocy Społecznej w Ciechanowie 3. Dom Pomocy Społecznej "Kombatant" w Ciechanowie 4. Ośrodek Wsparcia w Ciechanowie 5. Specjalny Ośrodek Szkolno-Wychowawczy w Ciechanowie 6. Placówka Opiekuńczo-Wychowawcza Socjalizacyjna 7. I Liceum Ogólnokształcące im. Zygmunta Krasińskiego w Ciechanowie 8. Zespół Szkół nr 1 im. Gen. Józefa Bema w Ciechanowie 9. Zespół Szkół nr 2 im. Adama Mickiewicza w Ciechanowie 10. Zespół Szkół nr 3 im. Stanisława Staszica w Ciechanowie 11. Zespół Szkół Technicznych Centrum Kształcenia Ustawicznego im. Stanisława Płoskiego w Ciechanowie 12. Powiatowy Zarząd Dróg w Ciechanowie 13. Powiatowe Centrum Pomocy Rodzinie w Ciechanowie 14. Poradnia Psychologiczno- Pedagogiczna w Ciechanowie 15. Powiatowy Urząd Pracy w Ciechanowie 16. Powiatowe Centrum Usług w Wspólnych w Ciechanowie
Zadanie	<ol style="list-style-type: none"> 1. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji na podstawie PN ISO 27001. 2. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji na podstawie PN ISO 27001. 3. Audyt SZBI. 4. Testy socjotechniczne. 5. Testy penetracyjne. 6. Skanowanie podatności.

na Rozwój Cyfrowy

Wykonawca	Wykonawca Zgodnie z definicją zawartą w art. 7 pkt 30) ustawy PZP
OPZ	Opis przedmiotu zamówienia.
SZBI	System Zarządzania Bezpieczeństwem Informacji
Termin w dniach	Oznacza kolejne dni kalendarzowe
PBI	Polityka Bezpieczeństwa Informacji
NSC	Narodowe Standardy Cyberbezpieczeństwa, to zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji. NSC zostały opracowane na podstawie standardów amerykańskiego National Institute of Science and Technology (NIST) oraz przyporządkowane obowiązującym w polskim systemie prawnym normom stosowanym w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.
NIST	National Institute of Science and Technology.
OSSTMM	Open Source Security Testing Methodology Manual.
OWASP	Open Web Application Security Project.
CVSS	Common Vulnerability Scoring System.
Infrastruktura IT	(Information Technology Infrastructure) to zbiór wszystkich zasobów takich jak sprzęt komputerowy, oprogramowanie i sieci.

PRZEPISY PRAWA, NORMY

KSC	Ustawa o krajowym systemie cyberbezpieczeństwa.
KRI	Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
RODO	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) z dnia 27 kwietnia 2016 r. (Dz.Urz.U.E.L Nr 119, str. 1 z późn. zm.)
PN-EN ISO/IEC 27001	Polska norma dotycząca bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony prywatności.
NSC	Narodowe Standardy Cyberbezpieczeństwa.
Ustawy	Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym.
	Ustawa o pracownikach samorządowych.
	Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych.
	Ustawa z dnia 7 września 1991 r. o Systemie oświaty.
	Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe.
	Ustawa o pomocy społecznej z dnia 12 marca 2004 r.
	Ustawa z dnia 20 marca 2025 r. o rynku pracy i służbach zatrudnienia.
	Prawo zamówień publicznych
	Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska
	Ustawa z dnia 7 lipca 1994 r. Prawo budowlane.
	Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne
	Ustawa z dnia 21 marca 1985 r. o drogach publicznych

I. CEL ZADANIA

Celem zadania jest podniesienie poziomu bezpieczeństwa systemów informatycznych Jednostek Zamawiającego poprzez opracowanie dokumentacji Polityki Bezpieczeństwa Informacji oraz wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z wymaganiami normy PN-EN ISO/IEC 27001 oraz zaleceniami norm pokrewnych, jak również RODO.

II. POWODY REALIZACJI:

- brak zbiorczych, jednolitych wytycznych dla Polityki Bezpieczeństwa Informacji w Jednostkach Zamawiającego oraz wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- konieczność ustandaryzowania procedur bezpieczeństwa informacji, wynikających ze stale rosnących zasobów baz danych gromadzonych w Jednostkach Zamawiającego,
- konieczność podniesienia poziomu bezpieczeństwa usług udostępniania informacji, wynikający z faktu znacznego wzrostu zapotrzebowania na takie usługi.

III. DZIĘKI REALIZACJI ZADANIA, SPODZIEWANE JEST OSIĄGNIĘCIE PONIŻSZYCH KORZYŚCI:

- zapewnienie bezpieczeństwa danych i systemów posiadanych przez Jednostki Zamawiającego, jak również danych powierzanych Jednostkom Zamawiającego w oparciu o normy i standardy europejskie takie jak np. PN-EN ISO/IEC 27001;
- ograniczenie czasu niedostępności systemów informatycznych Jednostek Zamawiającego z powodu ich awarii, poprzez opracowanie Planów Ciągłości Działania;
- zmniejszenie skutków działania szkodliwego oprogramowania, włamań i utraty danych;

IV. KONTEKST PRZEDSIĘWZIĘCIA

Zamawiający oczekuje, że Wykonawca zrealizuje usługę polegającą na opracowaniu dokumentacji Polityki Bezpieczeństwa Informacji oraz usługę wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z wymaganiami Krajowych Ram Interoperacyjności, normy PN-EN ISO/IEC 27001 oraz zaleceniami norm pokrewnych, jak również RODO.

OPZ nie będzie obejmował polityki bezpieczeństwa informacji niejawnych określonych w ustawie o ochronie informacji niejawnych.

V. INFORMACJE OGÓLNE O ŚRODOWISKU ZAMAWIAJACEGO

1. Powiat Ciechanowski - ogólnie.

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
980	1102	376	11	88	36

2. Starostwo Powiatowe w Ciechanowie.

ul. 17 Stycznia 7, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
139	120	55	2	12	1

3. Dom Pomocy Społecznej w Ciechanowie.

ul. Krucza 32, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
135	42	28	1	4	5

4. Dom Pomocy Społecznej "Kombatant" w Ciechanowie.

ul. Batalionów Chłopskich 12, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
67	20	21	1	1	1

5. Ośrodek Wsparcia w Ciechanowie.

ul. Świętochowskiego 8, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
11	2 stacjonarne + 1 laptop	2	0	0	1

na Rozwój Cyfrowy

6. Specjalny Ośrodek Szkolno-Wychowawczy w Ciechanowie.

ul. Sienkiewicza 13, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
106	87	29	0	15	6

7. Placówka Opiekuńczo-Wychowawcza Socjalizacyjna.

ul. Krucza 32A, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
11	5 stacjonarnych + 5 laptopów	3	1	0	1

8. I Liceum Ogólnokształcące im. Zygmunta Krasińskiego w Ciechanowie.

ul. 17 Stycznia 66, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
68	128	31	0	2	1

9. Zespół Szkół nr 1 im. Gen. Józefa Bema w Ciechanowie.

ul. Powstańców Warszawskich 24, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
67	224	6	1	11	2

10. Zespół Szkół nr 2 im. Adama Mickiewicza w Ciechanowie.

ul. Orylska 9, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
108	209	116	0	16	7

na Rozwój Cyfrowy

11. Zespół Szkół nr 3 im. Stanisława Staszica w Ciechanowie.

ul. Okrzei 6, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
62	58 stacjonarne + 44 laptopy	8	0	7	6

12. Zespół Szkół Technicznych Centrum Kształcenia Ustawicznego im. Stanisława Płoskiego w Ciechanowie.

ul. Kopernika 7, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
75	62	22	0	8	2

13. Powiatowy Zarząd Dróg w Ciechanowie.

ul. Mazowiecka 7, ul. Sienkiewicza 35, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
25	15	8	1	2	1

14. Powiatowe Centrum Pomocy Rodzinie w Ciechanowie.

ul. 17 Stycznia 7, ul. Kopernika 7, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
22	24	14	0	2	2

15. Poradnia Psychologiczno- Pedagogiczna w Ciechanowie.

ul. Wyzwolenia 10A, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
21	17	10	1	4	1

16. Powiatowy Urząd Pracy w Ciechanowie.

ul. Sygietyńskiego 11, 06-400 Ciechanowie

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
45	45	27	2	3	1

17. Powiatowe Centrum Usług Wspólnych w Ciechanowie.

ul. 17 Stycznia 7, 06-400 Ciechanów

Liczba pracowników	Komputery	Drukarki, kopiarki, skanery itp.	Serwery	Przełączniki	Routery, UTM-y
17	16	9	1	1	1

VI. HARMONOGRAM PRAC

1. Wykonawca zobowiązuje się do wykonania przedmiotu zamówienia w terminie wskazanym w formularzu ofertowym. Termin biegnie od dnia zawarcia umowy do dnia podpisania protokołu końcowego.
2. Wykonawca w terminie do 5 dni od podpisania umowy na wykonanie usługi przeprowadzi szkolenie dla kadry zarządzającej Zamawiającego. Szkolenie będzie obejmowało dwie grupy po około 15 osób każda. Szkolenie zostanie przeprowadzone w trybie stacjonarnym w siedzibie Zamawiającego, czas szkolenia jednej grupy minimum 4 godziny. Szczegółowy zakres szkolenia zostanie ustalony z Zamawiającym, w szczególności ma obejmować System Zarządzania Bezpieczeństwem Informacji (SZBI), Ustawę o krajowym systemie cyberbezpieczeństwa (KSC) oraz Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI).
3. Wykonawca w terminie 7 dni od podpisania umowy na wykonanie usługi przedstawi i przekaże Zamawiającemu wstępny harmonogram prac, który będzie obejmował etapy zadania dla wszystkich Jednostek Zamawiającego.
4. Zamawiający ma prawo do wnoszenia uwag do przedstawionego harmonogramu w terminie 7 dni od daty jego otrzymania. Wykonawca zobowiązany jest do ich uwzględnienia w terminie 7 dni od daty wniesienia.
5. Wstępny harmonogram będzie podlegał akceptacji przez Zamawiającego.
6. Przed przystąpieniem do realizacji każdego kolejnego etapu zadania Wykonawca opracuje szczegółowy harmonogram realizacji danego etapu, dla każdej Jednostki Zamawiającego osobno.

na Rozwój Cyfrowy

7. Przystąpienie Wykonawcy do prac nad poszczególnymi etapami możliwe będzie po zaakceptowaniu przez Zamawiającego harmonogramu szczegółowego, o którym mowa w pkt 6.
8. Harmonogramy, o których mowa w pkt 6 będą zawierały w szczególności terminy wykonania poszczególnych prac w etapie, w tym terminy wnoszenia i akceptacji uwag do produktów prac etapu.
9. Zakończenie prac danego etapu nastąpi po podpisaniu protokołu etapu dla każdej Jednostki Zamawiającego oddzielnie.
10. Prace nad realizacją zadania będą odbywały się równolegle we wszystkich Jednostkach Zamawiającego, zgodnie z harmonogramem wstępnym o którym mowa w pkt 3.
11. Odbiór całości prac nastąpi po podpisaniu protokołu końcowego, który będzie podstawą do wystawienia faktury.
12. Podpisanie protokołu końcowego możliwe będzie jedynie wtedy, gdy będą podpisane wszystkie protokoły etapu.

VII. ETAPY ZADANIA**1. Audyt wstępny - Identyfikacja wstępna stanu faktycznego Jednostek Zamawiającego.****1.1. Zakres prac audytu wstępnego będzie obejmował co najmniej:**

1.1.1. Zapoznanie się ze strukturą organizacyjną Jednostek Zamawiającego.

1.1.2. Analizę i ocenę dokumentacji w zakresie bezpieczeństwa informacji, w tym regulaminów, procedur bezpieczeństwa, zarządzeń, instrukcji oraz innych dokumentów, które Zamawiający udostępni Wykonawcy do analizy.

1.2. Zamawiający na wniosek Wykonawcy prześle mu wszystkie materiały i dokumenty, które zostały wytworzone w ramach zarządzania architekturą Jednostek Zamawiającego, niezbędne do realizacji etapu. Wszystkie prace związane z audytami winny się opierać na przekazanej dokumentacji przez Zamawiającego i nie dublować już zrealizowanych działań.

1.3. Wykonawca przeprowadzi wywiady analityczne z wytypowanymi przez Zamawiającego pracownikami poszczególnych Jednostek Zamawiającego w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa narzucanych normą PN-EN ISO/IEC 27001 oraz wewnętrznymi uregulowaniami Zamawiającego.

1.4. Wykonawca przeprowadzi szkolenie wprowadzające dla pracowników Jednostek Zamawiającego w zakresie celów i zasad funkcjonowania SZBI, ochrony informacji, inwentaryzacji i klasyfikacji aktywów chronionych oraz szacowania ryzyka. Szkoleniem objętych będzie ok. 200 osób (maksymalnie w grupach po ok. 25 osób).

na Rozwój Cyfrowy**1.4.1. Szkolenie musi obejmować:**

- Przedstawienie celów SZBI, harmonogramu oraz oczekiwanych rezultatów na poszczególnych etapach.
- Omówienie wymagań normy PN-EN ISO/IEC 27001.
- Wprowadzenie do zarządzania ryzykiem.
- Omówienie roli i obowiązków zespołów roboczych.
- Omówienie sposobu komunikacji między Wykonawcą a Zamawiającym.

1.4.2. Wykonawca przekaze Zamawiającemu harmonogram szkoleń, materiały szkoleniowe i prezentacje w zakresie szkoleń, najpóźniej na 5 dni przed planowanym terminem rozpoczęcia szkoleń.**1.4.3. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów szkoleniowych oraz harmonogramu szkoleń, w tym do zmiany planowanych terminów szkoleń.****1.4.4. Wykonawca zobowiązany jest do uwzględnienia uwag przekazanych przez Zamawiającego, o których mowa w pkt 1.4.3.****1.4.5. Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:**

- Imiennej listy obecności uczestników szkolenia sporządzanej odrębnie dla każdego dnia szkolenia, zawierającej: informacje o liczbie godzin, obecności danej osoby, podpis uczestnika szkolenia, podpis wykładowcy.
- Ankiety oceny szkolenia wypełnionych przez uczestników szkolenia.

1.4.6. Zamawiający zastrzega sobie prawo do rejestracji audio-wizualnej przebiegu szkoleń. Nagrania będą wykorzystywane w procesie szkoleniowym pracowników Jednostek Zamawiającego. Wykonawca przekaze Zamawiającemu niezbędne licencje do nagrań.**1.4.7. Szkolenie zostanie przeprowadzone w trybie stacjonarnym w siedzibie Zamawiającego.****1.5. Minimalne produkty etapu:**

- Protokoły zakończenia etapu.
- Raport z audytu wstępnego.
- Listy obecności uczestników szkolenia.
- Ankiety oceny szkolenia.

na Rozwój Cyfrowy**2. Audyt zasadniczy.**

2.1. Audyt zostanie przeprowadzony w komórkach organizacyjnych wszystkich Jednostek Zamawiającego.

2.2. Audyt zasadniczy będzie obejmował:

2.2.1. Przegląd kluczowych zbiorów danych.

- Wykonawca dokona przeglądu kluczowych zbiorów informacji przetwarzanych przez Zamawiającego w postaci elektronicznej i papierowej pod kątem ich znaczenia dla osiągnięcia celów Zamawiającego i zgodności z jego strategią.
- Wykonawca zaproponuje przypisanie właścicieli kluczowych zbiorów informacji.
- Wykonawca dokona analizy procedur bezpieczeństwa, które winny być opisane dla zidentyfikowanych zbiorów informacji.
- Zamawiający udostępni na tym etapie wszystkie dostępne materiały, analizy i audyty, które do tej pory były już wykonane.

2.2.2. Klasyfikację zbiorów danych.

- Wykonawca opracuje metody klasyfikowania informacji przetwarzanych w Jednostkach Zamawiającego. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej przez Wykonawcę metodyki klasyfikowania informacji.
- Wykonawca opracuje model podziału informacji przetwarzanych w Jednostkach Zamawiającego w zależności od poziomu ich wrażliwości i przeznaczenia, z wyłączeniem informacji niejawnych.
- Wykonawca przeprowadzi szkolenie dotyczące sposobu klasyfikacji informacji dla pracowników Jednostek Zamawiającego.
- Wykonawca sklasyfikuje wspólnie z pracownikami poszczególnych komórek organizacyjnych przetwarzane informacje w Jednostkach Zamawiającego.
- Wykonawca opracuje raport z procesu klasyfikacji informacji na podstawie danych uzyskanych w trakcie realizacji w/w procesu.
- Najważniejsze wnioski z procesu klasyfikacji informacji Wykonawca zobowiązany jest przedstawić Zamawiającemu w formie prezentacji multimedialnej.
- Opis metodyki klasyfikowania informacji oraz raport z procesu klasyfikowania informacji Wykonawca prześle Zamawiającemu w formie

cyfrowego repozytorium dokumentów (zapewniającego wersjonowanie).
Forma elektroniczna dokumentacji będzie przygotowana w plikach edytowalnych
w formatach: docx, pptx, xlsx.

- Cała dokumentacja, która powstanie w formie elektronicznej w trakcie prac, o których mowa powyżej, będzie zabezpieczona przed nieuprawnionym dostępem oraz podpisana podpisem kwalifikowanym wraz ze znacznikiem czasu i zostanie przekazana Zamawiającemu na nośniku danych CD/DVD.
- Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji, o której mowa powyżej.
- Wykonawca zobowiązany jest do uwzględnienia w raporcie wniesionych przez Zamawiającego uwag.

2.2.3. Przegląd i klasyfikację aktywów przetwarzających dane.

- Wykonawca dokona rozpoznania i klasyfikacji aktywów przetwarzających kluczowe zbiory informacji wykorzystywanych przez Zamawiającego dla informacji w postaci elektronicznej i papierowej.
- Wykonawca zaproponuje przypisanie aktywów do ich właścicieli.
- Wykonawca opracuje procedury bezpieczeństwa, które winny być opisane dla zidentyfikowanych aktywów.

2.2.4. Weryfikację zabezpieczeń organizacyjnych i technicznych na zgodność z wymaganiami normy PN-EN ISO/IEC 27001.

2.2.4.1. Wykonawca przeprowadzi analizę efektywności zabezpieczeń organizacyjnych wykorzystywanych przez Zamawiającego, obejmującą:

- Regulamin bezpieczeństwa.
- Organizację bezpieczeństwa informacji.
- Zarządzanie aktywami.
- Bezpieczeństwo zasobów ludzkich.
- Bezpieczeństwo fizyczne i środowiskowe.
- Zarządzanie systemami i sieciami.
- Kontrolę dostępu.
- Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.

- Zarządzanie incydentami związanymi z bezpieczeństwem informacji.
- Zarządzanie ciągłością działania.

2.2.4.2. Wykonawca przeprowadzi obserwację budynków, pomieszczeń, działań i zachowania pracowników.

2.2.4.3. Wykonawca przeprowadzi analizę bezpieczeństwa systemów teleinformatycznych, w szczególności:

- Ocenę schematu sieci.
- Określenie rodzaju połączeń.
- Określenie segmentów sieci.
- Przeprowadzenie oceny środowiska informatycznego.
- Ocenę sposobu identyfikowania i logowania użytkowników.
- Analizę zarządzania kontami użytkowników.
- Analizę strony WWW pod kątem ochrony danych osobowych.
- Analizę systemu backupów i archiwizacji danych.
- Określenie miejsc redundancji w sieci i w systemach informatycznych.
- Analizę konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
- Analizę konfiguracji zabezpieczeń baz danych.
- Określenie bezpieczeństwa aplikacji i serwerów WWW.
- Analizę konfiguracji urządzeń sieciowych: przełączniki, UTM.
- Ocenę zabezpieczeń dostępu do sieci publicznej.
- Analizę zabezpieczeń stacji roboczych.
- Analizę ochrony danych na komputerach przenośnych.
- Badanie zabezpieczeń nośników zewnętrznych.
- Sprawdzenie procedur zarządzania ciągłością działania.

2.2.5. Zbadanie zgodności działań Zamawiającego ze wszystkimi wskazanymi przez Zamawiającego uregulowaniami prawnymi którym podlega oraz z RODO.

2.2.6. Opracowanie kompletnego raportu z przeprowadzonego audytu.

Wykonawca jest zobowiązany do opracowania kompletnego raportu z audytu, który będzie zawierał w szczególności:

- Cel i zakres audytu.
- Szczegółowy opis przeprowadzonych prac.
- Szczegółowy opis poziomu spełnienia każdego z wymagań normy PN-EN ISO/IEC 27001 opisanych w załączniku A do niniejszej normy.
- Wykaz stwierdzonych niezgodności w odniesieniu do każdego z wymagań normy PN-EN ISO/IEC 27001 zgodnie z załącznikiem A na poziomie opisu poszczególnych zabezpieczeń wraz z przedstawieniem dowodów na istnienie niezgodności.
- Rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności w odniesieniu do każdego z wymagań normy PN-EN ISO/IEC 27001 opisanych w załączniku A do normy.
- Podsumowanie i wnioski.
- Raport, o którym mowa Wykonawca przekaże Zamawiającemu w postaci dokumentacji na CD/DVD. Forma elektroniczna raportu będzie przygotowana w plikach edytowalnych w formatach docx, pptx, xlsx.
- Raport w formie elektronicznej będzie zabezpieczony przed nieuprawnionym dostępem oraz podpisany podpisem kwalifikowanym wraz ze znacznikiem czasu i zostanie przekazany Zamawiającemu na nośniku danych CD/DVD.

2.2.7. Najważniejsze wnioski z audytu Wykonawca jest zobowiązany przedstawić kierownictwu Zamawiającego w formie prezentacji multimedialnej.

2.2.8. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 2.2.6.

2.2.9. Wykonawca zobowiązany jest do uwzględnienia w raporcie wniesionych przez Zamawiającego uwag do raportu, o których mowa w pkt 2.2.8.

2.3. Minimalne produkty etapu:

- Spis kluczowych zbiorów informacji przetwarzanych przez Zamawiającego wraz z oceną ich znaczenia.
- Spis właścicieli zidentyfikowanych zbiorów informacji.
- Spis procedur bezpieczeństwa dla zidentyfikowanych zbiorów informacji.
- Metoda klasyfikacji informacji.

na Rozwój Cyfrowy

- Model podziału informacji przetwarzanych w Jednostkach Zamawiającego w zależności od poziomu ich wrażliwości i przeznaczenia.
- Materiały szkoleniowe dotyczące sposobu klasyfikacji informacji.
- Raport z procesu klasyfikacji informacji.
- Prezentacja multimedialna przedstawiająca najważniejsze wnioski z procesu klasyfikacji informacji w Jednostkach Zamawiającego.
- Wykaz aktywów wykorzystywanych przy przetwarzaniu kluczowych zbiorów informacji wraz z ich właścicielami.
- Klasyfikacja aktywów przetwarzających informacje w Jednostkach Zamawiającego.
- Spis procedur bezpieczeństwa dla zidentyfikowanych aktywów przetwarzających informacje w Jednostkach Zamawiającego.
- Raport z analizy efektywności zabezpieczeń organizacyjnych wykorzystywanych przez Zamawiającego.
- Raport z analizy efektywności zabezpieczeń technicznych wykorzystywanych przez Zamawiającego.
- Raport z analizy zgodności działań Zamawiającego ze wszystkimi wskazanymi przez Zamawiającego uregulowaniami prawnymi, którym podlega w zakresie bezpieczeństwa informacji.
- Robocza wersja raportu z przeprowadzonego audytu do akceptacji Zamawiającego.
- Prezentacja multimedialna wniosków z audytu.
- Zaakceptowana przez Zamawiającego wersja raportu z przeprowadzonego Audytu Zasadniczego będąca podstawą do podpisania protokołu odbioru etapu.

3. Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych.

3.1. W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Jednostkach Zamawiającego, a w szczególności:

- 3.1.1. Opracować metodykę szacowania ryzyka spełniającą wymagania PN-EN ISO/IEC 27005 i Narodowych Standardów Cyberbezpieczeństwa oraz optymalną ze względu na charakter działalności Jednostek Zamawiającego. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej

metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić. Ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z wybraną i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka.

- 3.1.2. Opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyka.
- 3.1.3. Przeszkolić kadrę zarządzającą Jednostki Zamawiającego w zakresie przyjętej metodyki szacowania ryzyka.
- 3.1.4. Przeprowadzić wspólnie z wytypowanymi pracownikami Jednostek Zamawiającego proces szacowania ryzyka, a w szczególności:
 - Zinwentaryzować zasoby na podstawie przekazanej przez Zamawiającego dokumentacji i ewentualnych dodatkowych koniecznych audytów (aktywa informacyjne) oraz ich właścicieli.
 - Określić zagrożenia dla zasobów.
 - Określić podatności dla zasobów.
 - Określić skutki utraty poufności, integralności i dostępności zasobów.
 - Przeanalizować i ocenić zidentyfikowane ryzyka.
- 3.1.5. Opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Jednostek Zamawiającego.
- 3.1.6. Opracować przy współudziale wytypowanych pracowników Jednostek Zamawiającego plan postępowania z ryzykiem.
- 3.1.7. Dokumentację, o której mowa w pkt 3.1. tj. metodykę szacowania ryzyka, raport z procesu szacowania ryzyka oraz plan postępowania z ryzykiem Wykonawca przekaże Zamawiającemu w postaci dokumentacji na CD/DVD. Forma elektroniczna dokumentacji będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx. Pliki wynikowe będą miały spójną strukturę, dzięki temu w przyszłości Zamawiający zaimportuje pliki do Systemu wspierającego analizę ryzyka.
- 3.1.8. Dokumentacja w formie elektronicznej, o której mowa w pkt 3.1.7. będzie zabezpieczona przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i zostanie przekazana Zamawiającemu na nośniku danych CD/DVD.
- 3.1.9. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanej przez Wykonawcę dokumentacji, o której mowa w pkt 3.1.7.

3.1.10. Wykonawca zobowiązany jest do uwzględnienia w dokumentacji wniesionych przez Zamawiającego uwag, o których mowa w pkt 3.1.9.

3.2. Minimalne produkty etapu:

- Metodyka szacowania ryzyka.
- Raport z procesu szacowania ryzyka.
- Plan postępowania z ryzykiem.

4. Opracowanie zaleceń poaudytowych.

4.1. Wykonawca opracuje i przekaże Zamawiającemu dokument zawierający zalecane modyfikacje w zakresie zabezpieczania informacji mających na celu osiągnięcie zgodności z wymaganiami normy PN-EN ISO/IEC 27001.

4.2. Minimalne produkty etapu:

- Dokumentacja zawierająca zalecenia modyfikacji w zakresie zabezpieczania informacji zgodnie z wymaganiami normy PN-EN ISO/IEC 27001.

5. Opracowanie dokumentacji Polityki Bezpieczeństwa Informacji

5.1. Wykonawca na podstawie wyników uzyskanych w trakcie realizacji audytu, procesu klasyfikacji informacji oraz szacowania ryzyka zobowiązany jest opracować i przedstawić koncepcję wdrożenia Polityki Bezpieczeństwa Informacji w Jednostkach Zamawiającego. Dokumentacja ma mieć charakter: klasyczny (jednopoziomowy), hierarchiczny (dwupoziomowy, nadrzędnym dokumentem będzie Polityka Bezpieczeństwa Informacji Powiatu Ciechanowskiego, dla każdej z Jednostek Zamawiającego opracowana zostanie dokumentacja niższego rzędu uwzględniająca indywidualne cechy jednostki) lub hybrydowy (część jednostek korzysta z modelu hierarchicznego reszta z modelu klasycznego). Na etapie wdrożenia Zamawiający zdecyduje, który model dokumentacji wybrać. Koncepcja będzie w szczególności zawierać mapę dokumentów PBI, stanowiącą szczegółowy wykaz dokumentów PBI z zaznaczeniem ich wzajemnych powiązań w tym:

5.1.1. Dokument Główny Polityki Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa w proces zapewnienia bezpieczeństwa informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji. Nie zawiera informacji i powiązań informacji będących przedmiotem ochrony, jest stworzony w taki sposób, aby można było go ujawniać, a wszelkie informacje szczegółowe wskazane były w dokumentach towarzyszących, niejawnych.

5.1.2. Dokument Polityki Zarządzania Bezpieczeństwem Osobowym, w tym:

- Procedura rekrutacji.
- Rozpoczęcie zatrudnienia.
- Nadawanie uprawnień do zasobów.
- Szkolenie wstępne i okresowe.
- Zakończenie zatrudnienia.
- Postępowanie dyscyplinarne.

5.1.3. Dokument Polityki Zarządzania Bezpieczeństwem Fizycznym, w tym:

- Organizacja ochrony fizycznej obiektu.
- Podział obiektu na strefy bezpieczeństwa.
- Zasady organizowania stref.
- Zarządzanie kontrolą dostępu.
- Przyjmowanie gości.

5.1.4. Dokument Polityki Zarządzania Bezpieczeństwem IT.

- Zarządzanie uprawnieniami.
- Zarządzanie zmianą w systemach IT.
- Zarządzanie incydentami.
- Zbywanie i likwidowanie nośników.
- Kryptografia.
- Bezpieczeństwo sieci.
- Bezpieczeństwo urządzeń mobilnych.
- Instrukcja bezpiecznego administrowania systemami teleinformatycznymi.
- Instrukcja bezpiecznego użytkowania systemów teleinformatycznych.

5.1.5. Regulamin Podstawowych Zasad Bezpieczeństwa.

- Polityka czystego biurka i czystego ekranu.
- Zasada prywatności kont w systemach.
- Zasada poufności haseł.
- Zasady bezpiecznego pomieszczenia.
- Zgłaszanie incydentów bezpieczeństwa.

5.1.6. Polityka bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji w organizacji:

- Regulamin Ochrony Danych Osobowych.
- Regulamin Ciągłości Działania.
- Listy wymagań minimalnych dla głównych klas aktywów.
- Procedura okresowych wewnętrznych audytów bezpieczeństwa.
- Plan audytów wewnętrznych i zewnętrznych.
- Instrukcje sporządzania cyklicznych raportów dla właścicieli kluczowych aktywów i kadry zarządzającej.
- Procedury eksploatacyjne dla głównych klas aktywów.
- Szablony rejestrów przewidzianych w regulaminach, instrukcjach i procedurach.

5.1.7. Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

5.1.8. Procedury bezpieczeństwa i instrukcje stanowiące zestaw szczegółowych dokumentów razem z załącznikami i drukami, wynikającymi z regulaminów bezpieczeństwa, o których mowa w pkt 5.1.

5.2. Dla każdego dokumentu, o którym mowa w pkt 5.1. Wykonawca opracuje i przedstawi do akceptacji szczegółowy zakres merytoryczny. W przypadku dokumentów funkcjonujących w Jednostkach Zamawiającego odnoszących się do bezpieczeństwa informacji, których zakres merytoryczny będzie w całości lub częściowo pokrywał się z opracowanymi przez Wykonawcę projektami dokumentów PBI, Wykonawca zaproponuje i uzasadni sposób ich, wyłączenia, zastąpienia lub zintegrowania z zaproponowaną przez Wykonawcę mapą dokumentów. Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego. Uwagi wnoszone przez Zamawiającego muszą zostać uwzględnione przez Wykonawcę w koncepcji wdrożenia PBI.

5.3. Na podstawie zatwierdzonej przez Zamawiającego koncepcji, o której mowa w pkt 5.1., Wykonawca opracuje wszystkie opisane w koncepcji dokumenty Regulaminu Bezpieczeństwa Informacji Jednostek Zamawiającego, uwzględniając wszystkie uwagi Zamawiającego, o których mowa w pkt 5.2.

5.4. Dokumenty PBI, o których mowa w pkt 5.3. muszą być zgodne ze wszystkimi wymaganiami prawnymi, którym podlegają Jednostki Zamawiającego, w szczególności - w zakresie bezpieczeństwa informacji, oraz z wymaganiami normy PN-EN ISO/IEC 27001. Jeżeli w trakcie realizacji umowy wymagania prawne

w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację PBI do zaistniałych zmian.

- 5.5. Wszystkie dokumenty Polityki Bezpieczeństwa Informacji, o których mowa w pkt 5. Wykonawca prześle Zamawiającemu w postaci dokumentacji na CD/DVD. Forma elektroniczna dokumentacji będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx.
- 5.6. Dokumentacja w formie elektronicznej, o której mowa w pkt 5.5. będzie zabezpieczona przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i zostanie przekazana Zamawiającemu na nośniku danych CD/DVD.
- 5.7. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów PBI, o których mowa w pkt 5.5.
- 5.8. Wykonawca jest zobowiązany do wprowadzenia zmian w dokumentach PBI zgodnie z uwagami Zamawiającego, o których mowa w pkt 5.7.
- 5.9. Minimalne produkty etapu:
 - Dokumentacja koncepcyjna Polityki Bezpieczeństwa Informacji wraz z wszystkimi dokumentami towarzyszącymi.
 - Komplet dokumentacji Polityki Bezpieczeństwa Informacji wraz z wszystkimi dokumentami towarzyszącymi.
 - Koncepcja funkcjonowania SZBI, zawierająca szczegółowy opis funkcjonowania SZBI.

6. Szkolenia z powstałej Polityki Bezpieczeństwa Informacji

- 6.1. Wykonawca zobowiązany jest do przygotowania i poprowadzenia szkoleń ze stworzonej i zatwierdzonej przez Zamawiającego Polityki Bezpieczeństwa Informacji dla pracowników Jednostek Zamawiającego.
- 6.2. Wykonawca przygotuje i poprowadzi szkolenia dla pracowników.
 - 6.2.1. Szkolenia dla pracowników będą obejmowały swoim zakresem co najmniej:
 - Omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z PBI.
 - Odpowiedzialność za naruszenie zasad PBI.
 - Zasady zgłaszania i reagowania na incydenty.
 - 6.2.2. Szkolenia dla pracowników zostaną przeprowadzone dla pięciu 20-osobowych grup.

na Rozwój Cyfrowy

- 6.2.3. Szkolenie dla każdej z grup pracowników będzie trwało 6 godzin zegarowych, w tym przerwa 30 minut.
- 6.2.4. Szkolenia dla pracowników będą odbywały się w siedzibie Zamawiającego w dni robocze pomiędzy godziną 8:15 a 15:30.
- 6.3. Wykonawca przygotuje i poprowadzi szkolenia dla audytorów wewnętrznych.
- 6.3.1. Szkolenia dla audytorów wewnętrznych będą obejmowały swoim zakresem co najmniej:
- Zasady audytowania PBI.
 - Monitorowanie skuteczności PBI.
 - Opracowanie wyników z audytu wewnętrznego (działania korygujące, działania zapobiegawcze).
- 6.3.2. Szkolenia dla audytorów wewnętrznych PBI będą przeprowadzone dla grupy szesnastu osób oraz będą trwały minimum 2 dni robocze (7,5 godziny dziennie, w tym przerwa 30 minut).
- 6.3.3. Szkolenia dla audytorów wewnętrznych będą odbywały się w siedzibie Zamawiającego w dni robocze pomiędzy godziną 8:15 a 16:00.
- 6.4. Wykonawca przygotuje i poprowadzi szkolenia dla trenerów PBI.
- 6.4.1. Celem szkoleń dla trenerów będzie zdobycie przez uczestników wiedzy, umożliwiającej w przyszłości prowadzenie szkoleń z PBI dla pracowników Jednostek Zamawiającego.
- 6.4.2. Szkolenia dla trenerów będą przeprowadzone dla grupy szesnastu osób oraz będą trwały minimum 2 dni robocze (7,5 godziny dziennie, w tym przerwa 30 minut).
- 6.4.3. Szkolenia dla trenerów będą odbywały się w siedzibie Zamawiającego w dni robocze pomiędzy godziną 8:15 a 16:00.
- 6.5. Wykonawca prześle do akceptacji Zamawiającemu harmonogram szkoleń, materiały szkoleniowe i prezentacje najpóźniej na 14 dni przed planowanym terminem rozpoczęcia szkoleń.
- 6.6. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę materiałów szkoleniowych i harmonogramu szkoleń, w tym do zmiany planowanych terminów szkoleń.
- 6.7. Wykonawca zobowiązany jest do uwzględnienia uwag, o których mowa w pkt 6.6.
- 6.8. W ramach realizowanej usługi Wykonawca przygotuje szkolenie e-learningowe z Polityki Bezpieczeństwa Informacji, które posłuży jako materiał szkoleniowy dla pracowników Jednostek Zamawiającego.

na Rozwój Cyfrowy

- 6.9. Szkolenie zostanie przygotowane zgodnie ze standardem SCORM. Zamawiający umieści szkolenie e-learningowe na swojej platformie do szkoleń online, w celu przeprowadzania szkoleń pracowników Jednostek Zamawiającego.
- 6.10. Wykonawca przekaze zamawiającemu licencję na wieczyste użytkowanie bez ograniczeń ilościowych (z wyłączeniem zastosowań komercyjnych) na dostarczone szkolenie e-learningowe z Polityki Bezpieczeństwa Informacji.
- 6.11. Zamawiający przedstawi Wykonawcy szczegółowe wymagania odnośnie formy przygotowania szkolenia e-learningowego w terminie 14 dni, liczonym od dnia zaakceptowania prac zrealizowanych w punkcie 5.
- 6.12. Wykonawca jest zobowiązany do opracowania programu szkolenia e-learningowego zgodnie z wymaganiami Zamawiającego.
- 6.13. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę programu szkolenia e-learningowego.
- 6.14. Wykonawca zobowiązany jest do uwzględnienia uwag, o których mowa w pkt 6.13.
- 6.15. Wykonawca zobowiązany jest ponadto do przygotowania i przedłożenia Zamawiającemu:
- 6.15.1. Imiennej listy obecności uczestników szkolenia, sporządzanej odrębnie dla każdego dnia szkolenia, zawierającej: informacje o liczbie godzin, obecności danych osób, podpis uczestników szkolenia, podpis wykładowcy/wykładowców.
- 6.15.2. Ankiety oceny szkolenia wypełnionych i podpisanych przez uczestników szkolenia.
- 6.16. Zamawiający zastrzega sobie prawo do rejestracji audio-wizualnej przebiegu wszystkich szkoleń. Nagrania będą wykorzystywane w procesie szkoleniowym pracowników Jednostek Zamawiającego. Wykonawca przekaze Zamawiającemu niezbędne licencje do nagrań.
- 6.17. Wykonawca zobowiązany jest wystawić wszystkim osobom biorącym udział w szkoleniu imienny certyfikat uczestnictwa w szkoleniu.
- 6.18. Minimalne produkty etapu:
- Harmonogram szkoleń.
 - Materiały szkoleniowe i prezentacje.
 - Materiały e-learningowe zgodnie ze standardem SCORM.
 - Licencje.
 - Listy obecności uczestników szkolenia.
 - Ankiety oceny szkolenia.
 - Imienne certyfikaty uczestników szkolenia.

7. Audyt powdrożeniowy.

- 7.1. Wykonawca zobowiązany jest do przeprowadzenia Audytu powdrożeniowego, który będzie obejmował następujące prace:
 - 7.1.1. Weryfikację poziomu wdrożenia w Jednostkach Zamawiającego zabezpieczeń zgodnie z rekomendacjami, o których mowa w pkt 2.2.6.
 - 7.1.2. Weryfikację stosowania zasad określonych w Polityce Bezpieczeństwa Informacji przez pracowników w Jednostkach Zamawiającego.
 - 7.1.3. Ocenę poziomu spełnienia wymagań normy PN-ISO/IEC 27001 zgodnie z załącznikiem A do niniejszej normy.
- 7.2. Audyt będzie realizowany w wybranych komórkach organizacyjnych Jednostek Zamawiającego.
- 7.3. Wykonawca zobowiązany jest przedstawić Zamawiającemu szczegółowy plan audytu, który będzie podlegał akceptacji przez Zamawiającego.
- 7.4. Wykonawca zobowiązany jest opracować raport z audytu powdrożeniowego zawierający co najmniej:
 - 7.4.1. Cel i zakres przeprowadzonego audytu.
 - 7.4.2. Szczegółowy opis przeprowadzonych prac.
 - 7.4.3. Szczegółowy opis poziomu spełnienia wymagań normy PN-ISO/IEC 27001, w obszarach, w których podczas audytu przedwdrożeniowego stwierdzono niezgodności
 - 7.4.4. Wykaz zaobserwowanych niezgodności w odniesieniu do stosowania przez pracowników Jednostek Zamawiającego zasad Polityki Bezpieczeństwa Informacji.
 - 7.4.5. Szczegółowy opis działań korygujących i naprawczych. Plan doskonalenia.
 - 7.4.6. Ogólną ocenę poziomu spełnienia wymagań normy PN-ISO/IEC 27001 zgodnie z załącznikiem A do niniejszej normy oraz poziomu stosowania przez pracowników Jednostek Zamawiającego zasad Polityki Bezpieczeństwa Informacji.
 - 7.4.7. Podsumowanie i wnioski.
- 7.5. Wykonawca w porozumieniu z Zamawiającym wprowadzi w życie działania korygujące i naprawcze, co zostanie uwzględnione w raporcie.
- 7.6. Najważniejsze wnioski z audytu powdrożeniowego Wykonawca jest zobowiązany przedstawić kierownictwu Zamawiającego w formie prezentacji multimedialnej.

na Rozwój Cyfrowy

- 7.7. Raport, o którym mowa w pkt 7.4. Wykonawca prześle Zamawiającemu w formie elektronicznej w postaci cyfrowego repozytorium dokumentów (zapewniając ich wersjonowanie). Forma elektroniczna raportu będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx.
- 7.8. Raport w formie elektronicznej, o którym mowa w pkt 7.7. będzie zabezpieczony przed nieuprawnionym dostępem oraz podpisany podpisem kwalifikowanym ze znacznikiem czasu i zostanie przekazany Zamawiającemu na nośniku danych CD/DVD.
- 7.9. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 7.7.
- 7.10. Wykonawca zobowiązany jest do uwzględnienia w raporcie, o którym mowa w pkt 7.7. wniesionych przez Zamawiającego uwag.
- 7.11. Minimalne produkty etapu:
- Szczegółowy plan audytu.
 - Raport z audytu powdrożeniowego.

8. Przegląd Systemu Zarządzania Bezpieczeństwem Informacji.

- 8.1. Wykonawca w porozumieniu z wyznaczonymi pracownikami Jednostek Zamawiającego zobowiązany jest do przeprowadzenia przeglądu SZBI, który będzie obejmował następujące prace:
- 8.1.1. Analiza działań podjętych w następstwie wcześniejszych przeglądów SZBI, w tym audytu powdrożeniowego.
- 8.1.2. Sprawdzenie zmian czynników zewnętrznych i wewnętrznych, które są istotne dla SZBI.
- 8.1.3. Sprawdzenie aktualnych potrzeb i oczekiwań zainteresowanych stron, które są istotne dla SZBI.
- 8.1.4. Analiza informacji zwrotnych dotyczących wyników w zakresie bezpieczeństwa informacji, w tym także tendencje w zakresie:
- Niezgodności i działań korygujących.
 - Wyników monitorowania i pomiarów.
 - Wyników audytów.
 - Realizacji celów w zakresie bezpieczeństwa informacji.
- 8.1.5. Sprawdzenie informacji zwrotnych od zainteresowanych stron.

na Rozwój Cyfrowy

- 8.1.6. Analiza wyników oceny ryzyka i stanu realizacji planu postępowania z ryzykiem.
- 8.1.7. Sprawdzenie ciągłości doskonalenia SZBI.
- 8.2. Przegląd będzie realizowany w wybranych komórkach organizacyjnych Jednostek Zamawiającego.
- 8.3. Wykonawca w porozumieniu z wyznaczonymi pracownikami Jednostek Zamawiającego zobowiązany jest przedstawić Zamawiającemu szczegółowy plan przeglądu, który będzie podlegał akceptacji przez Zamawiającego.
- 8.4. Wykonawca w porozumieniu z wyznaczonymi pracownikami Jednostek Zamawiającego zobowiązany jest opracować raport z przeglądu SZBI.
- 8.5. Wyniki przeglądu obejmą decyzje dotyczące możliwości ciągłego doskonalenia oraz wszelkie potrzeby zmian w SZBI.
- 8.6. Wykonawca w porozumieniu z Zamawiającym wprowadzi w życie działania korygujące i naprawcze, co zostanie uwzględnione w raporcie.
- 8.7. Minimalne produkty etapu:
- Raport z Przeglądu Systemu Zarządzania Bezpieczeństwem Informacji.

9. Audyt SZBI.

- 9.1. Wykonawca przeprowadzi audyt SZBI w oparciu o 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 (tj. Dz. U. z 2024 r. poz. 773).
- 9.2. Audyt SZBI należy przeprowadzić dwukrotnie we wszystkich Jednostkach Zamawiającego w dni robocze w godzinach 8:30 — 15:00. Zamawiający nie dopuszcza możliwości realizacji usługi jedynie za pomocą środków zdalnej komunikacji.
- 9.3. Pierwszy audyt SZBI Wykonawca przeprowadzi do 60 dni od podpisania umowy, drugi audyt SZBI odbędzie się na 30 dni przed zakończeniem umowy.
- 9.4. Zakres i przedmiot audytu SZBI obejmuje przegląd Systemów Zarządzania Bezpieczeństwem Informacji w poszczególnych Jednostkach Zamawiającego pod kątem rzeczywistego poziomu bezpieczeństwa informacji z uwzględnieniem w szczególności następujących założeń:
- 9.4.1. Zakres audytu SZBI obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI.

- 9.4.2. Audyt SZBI zostanie przeprowadzony przez audytora posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w szczególności audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001.
- 9.4.3. Wykonawca przygotowuje raport z audytu SZBI w wersji papierowej i elektronicznej. Obie wersje zostaną podpisane przez audytora przeprowadzającego audyt, raport w formie elektronicznej zostanie podpisany przy wykorzystaniu kwalifikowanego podpisu elektronicznego.
- 9.4.4. 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, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. Jeżeli w okresie realizacji zamówienia zostanie przyjęta nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa 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, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) do polskiego systemu prawnego, Wykonawca ma obowiązek uwzględnić wszystkie ich nowe wymagania w trakcie realizacji przedmiotu umowy.
- 9.4.5. Wykonawca przygotowuje wytyczne z zakresu stosowanych zabezpieczeń w oparciu o normy i „najlepsze praktyki”, dostarczy wnioski, zalecenia i rekomendacje w celu dokładnego rozpoznania i redukcji ryzyka, zagrożeń i podatności oraz wskaże adekwatne działania mające na celu jak najszybsze ich wyeliminowanie.
- 9.5. Raport elektroniczny, o którym mowa w punkcie 9.4.3. Wykonawca prześle Zamawiającemu w postaci cyfrowego repozytorium dokumentów (zapewniającego ich wersjonowanie). Forma elektroniczna raportu będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx.
- 9.6. Raport w formie elektronicznej, o którym mowa w pkt 9.5. będzie zabezpieczony przed nieuprawnionym dostępem oraz podpisany podpisem kwalifikowanym ze znacznikiem czasu i zostanie przekazany Zamawiającemu na nośniku danych CD/DVD.

na Rozwój Cyfrowy

- 9.7. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 9.5.
- 9.8. Wykonawca zobowiązany jest do uwzględnienia w raporcie, o którym mowa w pkt 9.5. wniesionych przez Zamawiającego uwag.
- 9.9. Minimalne produkty etapu:
- Raport z Audytu SZBI zgodnego z wymaganiami Rozporządzenia o Krajowych Ramach Interoperacyjności.

10. Testy socjotechniczne.

- 10.1. Test socjotechniczny polega na użyciu odpowiednich metod i technik mających na celu pozyskanie od pracownika hasła dostępowego do systemów informatycznych, danych osobowych, poufnych informacji lub pobranie wirusa.
- 10.2. Wykonawca przygotuje dwie kampanie socjotechniczne wykorzystujące maile wysyłane na skrzynki służbowe pracowników Jednostek Zamawiającego. Każda kampania zostanie przygotowana dla około 600 maili. Pierwsza kampania zostanie przeprowadzona w terminie do 30 dni po podpisaniu umowy, druga kampania zostanie przeprowadzona w październiku 2025 roku. Kampanie będą składać się ze scenariuszy dostosowanych do poszczególnych jednostek.
- 10.3. W ramach kampanii Konsultanci Wykonawcy wyślą spreparowaną wiadomość mail do pracowników Jednostek Zamawiającego z domen przypominających domeny Jednostek. Lista pracowników, do których kierowany będzie atak zostanie stworzona na podstawie informacji dostarczonej przez Zamawiającego. W wiadomości zostanie zawarta treść trudna do zrozumienia dla przeciętnego pracownika, złożona ze zwrotów technicznych i nakłaniająca do natychmiastowego uwierzytelnienia się loginem oraz hasłem na specjalnie przygotowanej do tego celu stronie WWW umieszczonej na domenie łudząco podobnej do oryginalnej domeny Jednostki. Strona zostanie zaprojektowana tak, by odwzorować oryginalną identyfikację graficzną. W treści wiadomości zostanie zawarty również nr telefonu, pod który pracownicy w razie wątpliwości w tej sprawie mogą się zgłosić. W przypadku kontaktu telefonicznego pod podanym numerem, Konsultant Wykonawcy potwierdzi autentyczność wiadomości i konieczność natychmiastowego podania danych uwierzytelniających.
- 10.4. Elementy zawarte w mailu wskazujące na atak:
- 10.4.1. Nieprawidłowa domena.
 - 10.4.2. Nowomowa/skomplikowany język techniczny.
 - 10.4.3. Brak indywidualnego zwrotu do pracownika.

na Rozwój Cyfrowy

- 10.4.4. Błędy językowe/ortograficzne.
- 10.4.5. Nakłanianie do natychmiastowego działania, graficzne przedstawienie uciekającego czasu na wykonanie działania.
- 10.5. Konieczność kliknięcia w link i prośba o podanie hasła. Dokładne scenariusze testu socjotechnicznego zostaną uzgodnione z Zamawiającym.
- 10.6. Przykładowe scenariusze wykorzystywane w badaniach:
 - 10.6.1. Wymagana okresowa zmiana hasła do skrzynki mailowej adresata.
 - 10.6.2. Uzupełnienie danych kadrowych dot. urlopu w związku koniecznością przygotowania planów urlopowych.
 - 10.6.3. Kończy się Twój limit danych w skrzynce mailowej. Jeśli chcesz zwiększyć ilość danych, wypełnij wniosek.
 - 10.6.4. Wyjazd integracyjny - W związku z planowanym wyjazdem integracyjnym prosimy wszystkich pracowników o uzupełnienie formularza informacyjnego.
 - 10.6.5. Zaproszenie na darmowe szkolenie.
 - 10.6.6. Niezapłacona faktura.
- 10.7. Na podstawie zebranych dowodów i zaobserwowanych sytuacji, Konsultanci Wykonawcy opracują raport obrazujący aktualny stan bezpieczeństwa Jednostek Zamawiającego z punktu widzenia zagrożeń socjotechnicznych oraz przedstawia rekomendacje i niezbędne działania, które należy podjąć, aby właściwie chronić się przed opisywanymi zagrożeniami.
- 10.8. Zamawiający ma możliwość odwołania się do zapisów raportu.
- 10.9. Wykonawca w raporcie końcowym uwzględni odwołania Zamawiającego.
- 10.10. Raport testu socjotechnicznego zawiera w szczególności:
 - 10.10.1. Zakres testu.
 - 10.10.2. Podsumowanie dla kierownictwa Zamawiającego, zawierające najważniejsze wnioski oraz wykresy.
 - 10.10.3. Szczegółowy opis wyników ze zidentyfikowanymi zagrożeniami dla badanych maili, z podziałem na: krytyczne, wysokie, średnie oraz niskie.
 - 10.10.4. Opis wyników przeprowadzonego testu z wnioskami oraz rekomendacjami.
- 10.11. Raport, o którym mowa w pkt 10.10. Wykonawca przekaze Zamawiającemu w formie elektronicznej w postaci cyfrowego repozytorium dokumentów

(zapewniającego ich wersjonowanie). Forma elektroniczna raportu będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx.

- 10.12. Raport w formie elektronicznej, o którym mowa w pkt 10.11. będzie zabezpieczony przed nieuprawnionym dostępem oraz podpisany podpisem kwalifikowanym ze znacznikiem czasu i zostanie przekazany Zamawiającemu na nośniku danych CD/DVD.
- 10.13. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 10.11.
- 10.14. Wykonawca zobowiązany jest do uwzględnienia w raporcie, o którym mowa w pkt 10.11. wniesionych przez Zamawiającego uwag.
- 10.15. Minimalne produkty etapu:
 - Raport z testu socjotechnicznego.

11. Testy penetracyjne.

- 11.1. Testy penetracyjne polegają na przeprowadzeniu kontrolowanego ataku na infrastrukturę IT Starostwa Powiatowego w Ciechanowie. Działanie zapewni realną ocenę stanu bezpieczeństwa infrastruktury, wskazując luki bezpieczeństwa, które mogą zostać wykorzystane do skompromitowania zabezpieczeń.
- 11.2. Wykonawca przeprowadzi testy penetracyjne zgodnie z metodyką opracowaną m.in. na zaleceniach opisanych w Narodowych Standardach Cyberbezpieczeństwa, które zostały opracowane na podstawie standardów amerykańskiego National Institute of Science and Technology (NIST), Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP) z uwzględnieniem wewnętrznych doświadczeń Wykonawcy i tzw. najlepszych praktyk.
- 11.3. Testy przeprowadzane zostaną przez zespół posiadający wieloletnie doświadczenie w obszarze bezpieczeństwa systemów teleinformatycznych oraz ciągłości działania.
- 11.4. Zespół testerów dołoży wszelkich starań w trakcie pozyskiwania informacji i testowania w celu zminimalizowania ingerencji w sieć produkcyjną. Jednak działania testerów mogą być obarczone pewnym prawdopodobieństwem destabilizacji niektórych usług, o czym Wykonawca powiadomi Zamawiającego przed wykonaniem danego testu.
- 11.5. Zespół opracuje metodę przeprowadzenia testów penetracyjnych realizującą badanie, w której eksperci zespołu:
 - 11.5.1. Określą wektor ataku.

- 11.5.2. Określą metody prowadzenia audytu.
- 11.5.3. Przygotują dedykowany scenariusz badania z uwzględnioną specyfiką list kontrolnych.
- 11.5.4. Wykonają testy automatyczne oraz ręczne.
- 11.5.5. Zrealizują analitykę zebranych danych oraz przygotują raport.
- 11.6. Wykonawca przedstawi opracowaną metodykę Zamawiającemu oraz omówi potencjalne zagrożenia dla infrastruktury IT Starostwa Powiatowego w Ciechanowie.
- 11.7. Przed rozpoczęciem prac testowych niezbędna będzie zgoda Zamawiającego świadcząca o wiedzy na temat potencjalnych skutków działań testerów.
- 11.8. Zakres testów penetracyjnych:
- 11.8.1. Testy penetracyjne aplikacji webowych i stron www obejmujące:
- Identyfikację i eksploatację luk bezpieczeństwa aplikacji webowych.
 - Testy autoryzacji i uwierzytelniania.
 - Analizę i testy zabezpieczeń danych.
 - Testy kontroli dostępu.
 - Testy podatności na ataki typu SQL Injection, XSS, CSRF, RCE, oraz OWASP TOP 10.
 - Analizę konfiguracji serwerów webowych.
- 11.8.2. Testy penetracyjne infrastruktury sieciowej obejmujące:
- Skanowanie i analiza portów.
 - Identyfikację i eksploatację luk bezpieczeństwa w sieci.
 - Testy odporności na ataki DoS/DDoS wolumetryczne oraz aplikacyjne.
 - Testy zabezpieczeń urządzeń sieciowych (routery, firewalle, przełączniki, punkty dostępowe), wewnętrzne i zewnętrzne.
 - Sprawdzenie polityk zabezpieczeń sieci. (w zakresie podłączania obcych urządzeń, przechodzenia między podsieciami, separacji logicznej sieci itp.).
 - Analizę i testy VPN oraz innych połączeń zdalnych.
 - Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS).
- 11.8.3. Testy penetracyjne infrastruktury serwerowej obejmujące:

- Analizę konfiguracji serwerów pod kątem bezpieczeństwa.
- Analizę bezpieczeństwa Active Directory.
- Identyfikację i eksploatację luk w systemach operacyjnych (Windows, Linux, Unix).
- Testy podatności na ataki typu privilege escalation.
- Sprawdzenie polityk zarządzania użytkownikami i kontrolą dostępu.
- Weryfikacja kont z dostępem administracyjnym i zakresu dostępów.
- Testy zabezpieczeń usług serwerowych (np. FTP, SSH, HTTP/HTTPS, DNS, DHCP).
- Analizę i testy zabezpieczeń baz danych.
- Weryfikację poprawności stosowania aktualizacji i łat bezpieczeństwa.
- Testy systemów kopii zapasowych i odzyskiwania danych.

11.9. Po przeprowadzeniu testów penetracyjnych Wykonawca przygotowuje raport, w którym zawarte są zidentyfikowane podatności w stosunku do każdego z testowanych systemów teleinformatycznych. Dla każdej zidentyfikowanej podatności określono poziom krytyczności zgodnie z modelem Common Vulnerability Scoring System (CVSS). Poziom krytyczności jest elementem wejściowym do analizy ryzyka oraz pozwoli na określenie priorytetów działań minimalizujących wystąpienie podatności. W raporcie zawarte są rekomendacje dot. usunięcia zidentyfikowanych podatności, których wdrożenie pozwoli usunąć zagrożenie.

11.10. Wykonawca zapewni wsparcie techniczne w implementacji zaleceń wynikających z raportu końcowego dla wszystkich urządzeń oraz serwerów, bez naprawy błędów w aplikacjach dedykowanych.

11.11. Raport z testów penetracyjnych będzie zawierał w szczególności:

- 11.11.1. Zakres audytu i listę usług zidentyfikowanych w trakcie testu.
- 11.11.2. Podsumowanie dla kierownictwa, zawierające najważniejsze wnioski oraz wykresy.
- 11.11.3. Szczegółowy opis wyników ze zidentyfikowanymi zagrożeniami w skali: krytyczne, wysokie, średnie oraz niskie, a także prawdopodobieństwem ich wykonania przez osoby atakujące.
- 11.11.4. Opis wyników przeprowadzonego testu bezpieczeństwa, z wnioskami oraz rekomendacjami.

- 11.11.5. Informacje w jaki sposób zostały usunięte zidentyfikowane podatności.
- 11.12. Raport, o którym mowa w pkt 11.11. Wykonawca przekaze Zamawiającemu w formie elektronicznej w postaci cyfrowego repozytorium dokumentów (zapewniającego ich wersjonowanie). Forma elektroniczna raportu będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx.
- 11.13. Raport w formie elektronicznej, o którym mowa w pkt 11.12. będzie zabezpieczony przed nieuprawnionym dostępem oraz podpisany podpisem kwalifikowanym ze znacznikiem czasu i zostanie przekazany Zamawiającemu na nośniku danych CD/DVD.
- 11.14. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu, o którym mowa w pkt 11.12.
- 11.15. Wykonawca zobowiązany jest do uwzględnienia w raporcie, o którym mowa w pkt 11.12. wniesionych przez Zamawiającego uwag.
- 11.16. Minimalne produkty etapu:
- Raport z testu penetracyjnego.

12. Skanowanie podatności.

- 12.1. Celem skanowania podatności jest identyfikacja, analiza oraz dokumentacja luk bezpieczeństwa w systemach IT. Skanowanie podatności będzie dotyczyć wszystkich Jednostek Zamawiającego, w celu zwiększenia ich poziomu ochrony danych, aplikacji i usług.
- 12.2. Wykonawca przygotuje szkolenie oraz materiały szkoleniowe dla wyznaczonych pracowników Jednostek Zamawiającego z zakresu przeprowadzanych skanów podatności.
- 12.3. Procedury skanowania podatności, opracowywanie wniosków oraz wszystkie pozostałe czynności związane ze skanowaniem podatności w Starostwie Powiatowym w Ciechanowie zostaną przeprowadzone z udziałem pracowników Starostwa.
- 12.4. Zakres Skanowania podatności:
- 12.4.1. Zakres adresów IP, sieci oraz aplikacji zostanie ustalony przez Wykonawcę z przedstawicielami Jednostek Zamawiającego.
- 12.4.2. Testy obejmą skanowanie systemów operacyjnych, aplikacji webowych, serwerów, urządzeń sieciowych.
- 12.4.3. Prace obejmą zarówno skanowanie zewnętrzne (od strony Internetu), jak i wewnętrzne (jeśli dostęp zostanie zapewniony).

na Rozwój Cyfrowy

- 12.4.4. Skanowanie nieinwazyjne – bez ingerencji w dane, konfigurację, ani bez przerywania pracy systemów.
- 12.4.5. Możliwość wykonania testów inwazyjnych (np. prób eksploatacji podatności) po uzyskaniu pisemnej zgody.
- 12.5. Przykładowe narzędzia: Nmap, Nessus, OpenVAS, Nikto, Burp Suite, OWASP ZAP, Qualys, TestSSL.sh, inne.
- 12.6. Ograniczenia zastosowania testów:
- 12.6.1. Testy nie obejmą elementów wymagających testów socjotechnicznych lub inżynierii społecznej, są one ujęte w innym punkcie.
- 12.6.2. Brak zmian konfiguracyjnych i brak modyfikacji danych produkcyjnych.
- 12.7. Przed rozpoczęciem testów wymagana jest akceptacja przedstawiciela Jednostki Zamawiającego dla następujących elementów:
- 12.7.1. Zakres prac i testowanych systemów, adresy IP, aplikacje, czas testów.
- 12.7.2. Zgoda na wykonanie testów w środowisku produkcyjnym (jeśli dotyczy).
- 12.7.3. Zgoda na ewentualne testy inwazyjne (np. próba wykorzystania wykrytej podatności).
- 12.7.4. Udzielenie wymaganych dostępów (np. VPN, konta testowe do skanów uwierzytelnionych).
- 12.7.5. Wyznaczenie osoby kontaktowej po stronie Jednostek Zamawiającego.
- 12.8. Opis zadań wykonywanych podczas skanowania podatności.
- 12.8.1. Odkrywanie aktywnych hostów:
- Wykrywanie aktywnych urządzeń i systemów w sieci.
 - Techniki: Ping sweep, TCP/UDP scan.
 - Narzędzia: Nmap, Masscan.
- 12.8.2. Identyfikacja systemów i usług:
- Ustalanie systemu operacyjnego, uruchomionych usług, portów i wersji oprogramowania.
 - Umożliwia dopasowanie znanych podatności do wykrytych komponentów.
- 12.8.3. Skanowanie podatności:
- Porównanie zidentyfikowanych systemów z bazami podatności (np. CVE).

- Detekcja luk typu RCE, SQLi, XSS, błędnych konfiguracji, niezłaatanych komponentów.
- Klasyfikacja według poziomu ryzyka.

12.8.4. Skany uwierzytelnione:

- Dokładniejsza analiza przy wykorzystaniu kont testowych.
- Weryfikacja uprawnień, konfiguracji, zainstalowanego oprogramowania.

12.8.5. Testy aplikacji webowych:

- Analiza błędów aplikacyjnych wg OWASP Top 10.
- Testy podatności: XSS, CSRF, IDOR, brak nagłówek bezpieczeństwa, błędne sesje.
- Narzędzia: OWASP ZAP, Burp Suite, Nikto.

12.8.6. Raportowanie:

- Szczegółowe wyniki testów z klasyfikacją podatności.
- Rekomendacje działań naprawczych.
- Podsumowanie dla IT i w wersji nietechnicznej dla kadry zarządzającej.

12.9. Po zakończeniu pierwszego etapu skanowania podatności zostanie przedstawiony raport wstępny, zawierający:

12.9.1. Listę wykrytych podatności (z podziałem na: krytyczne, wysokie, średnie, niskie).

12.9.2. Szczegółowe informacje techniczne – opisy, poziomy ryzyka, ścieżki dojścia.

12.9.3. Rekomendacje działań naprawczych – zarówno natychmiastowych, jak i długoterminowych.

12.9.4. Załączniki: logi, zrzuty ekranu, pliki wyjściowe ze skanów.

12.9.5. Raport zostanie przekazany osobiście – z omówieniem wyników i sesją pytań i odpowiedzi z przedstawicielami Jednostek Zamawiającego.

12.10. Po przedstawieniu wstępnego raportu Wykonawca przedstawi plan naprawczy oraz udzieli wsparcia Jednostkom Zamawiającego we wprowadzeniu działań naprawczych dla wykrytych podatności.

12.11. Po wdrożeniu planu naprawczego przez Jednostki Zamawiającego wykonane zostanie ponowne skanowanie i wygenerowany raport końcowy, który zawiera:

na Rozwój Cyfrowy

- 12.11.1. Porównanie stanu przed i po wdrożeniu poprawek.
 - 12.11.2. Potwierdzenie usunięcia podatności (lub wskazanie nadal istniejących).
 - 12.11.3. Ostateczna ocena bezpieczeństwa.
 - 12.11.4. Dalsze rekomendacje (np. cykliczne testy, wdrożenie WAF, segmentacja sieci).
 - 12.11.5. Możliwość przygotowania osobnego raportu dla kierownictwa w wersji uproszczonej/nietechnicznej.
 - 12.11.6. Informacje na temat w jaki sposób zostały usunięte zidentyfikowane podatności.
- 12.12. Raporty, o których mowa w pkt 12.9 i 12.11. Wykonawca przekaże Zamawiającemu w formie elektronicznej w postaci cyfrowego repozytorium dokumentów (zapewniającego ich wersjonowanie). Forma elektroniczna raportów będzie przygotowana w plikach edytowalnych w formatach: docx, pptx, xlsx.
- 12.13. Raporty w formie elektronicznej, o których mowa w pkt 12.12. będą zabezpieczone przed nieuprawnionym dostępem oraz podpisane podpisem kwalifikowanym ze znacznikiem czasu i zostaną przekazane Zamawiającemu na nośniku danych CD/DVD.
- 12.14. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę raportów, o których mowa w pkt 12.9. i 12.11.
- 12.15. Wykonawca zobowiązany jest do uwzględnienia w raportach, o których mowa w pkt 12.9. i 12.11. wniesionych przez Zamawiającego uwag.
- 12.16. Minimalne produkty etapu:
- Raport wstępny ze skanowania podatności.
 - Raport końcowy ze skanowania podatności.
 - Materiały szkoleniowe z zakresu przeprowadzanych skanów podatności.

13. Ankieta Dojrzałości.

- 13.1. Wykonawca opracuje i wypełni Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego stanowiące załącznik nr 6 do Regulaminu Konkursu Grantowego pn. "Cyberbezpieczny Samorząd".
- 13.2. Ankietę dojrzałości należy opracować dla wszystkich Jednostek Zamawiającego w dni robocze w godzinach 8:30 — 15:00. Zamawiający nie dopuszcza możliwości realizacji usługi jedynie za pomocą środków zdalnej komunikacji.

na Rozwój Cyfrowy

- 13.3. Wykonawca prześle wypełnione Ankiety Dojrzałości wszystkich Jednostek na 30 dni przed zakończeniem umowy.
- 13.4. Ankiety dojrzałości zostaną opracowane przez audytora posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) w szczególności audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001.
- 13.5. Ankiety dojrzałości, o których mowa w pkt 13.1. Wykonawca prześle Zamawiającemu w postaci cyfrowej. Forma elektroniczna raportu będzie przygotowana w plikach edytowalnych w formacie xls.
- 13.6. Ankiety dojrzałości w formie elektronicznej, o którym mowa w pkt 13.5. będą zabezpieczone przed nieuprawnionym dostępem oraz podpisane podpisem kwalifikowanym ze znacznikiem czasu i zostaną przekazane Zamawiającemu na nośniku danych CD/DVD.
- 13.7. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanych przez Wykonawcę Ankiety dojrzałości, o których mowa w pkt 13.5.
- 13.8. Wykonawca zobowiązany jest do uwzględnienia w Ankiecie dojrzałości, o których mowa w pkt 13.5. wniesionych przez Zamawiającego uwag.
- 13.9. Minimalne produkty etapu:
- Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego stanowiące załącznik nr 6 do Regulaminu Konkursu Grantowego pn. "Cyberbezpieczny Samorząd".