

Opis Przedmiotu Zamówienia

Spis treści

Słownik	3
1. Organizacja realizacji zamówienia	5
2. Przeprowadzenie audytów KRI	6
2.1. Przeprowadzenie audytów zgodności z Krajowymi Ramami Interoperacyjności	6
2.2. Zakres audytu oraz sposób prowadzenia audytu KRI	7
3. Przeprowadzenie audytu UoKSC dla Urzędu Gminy	10
3.1. Przeprowadzenie testów socjotechnicznych w ramach audytu KSC	11
3.2. Warunki wstępne i sposób realizacji	12
3.3. Szczegółowy opis testów	12
3.3.1. Stworzenie fałszywych stron	12
3.3.2. Wysyłanie wiadomości pocztą elektroniczną	14
4. Przeprowadzenie audytu bezpieczeństwa w obszarze sieci, serwerów oraz oprogramowania serwerowego	15
5. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji	17
5.1. Inwentaryzacja zasobów informacyjnych	17
5.2. Szacowanie ryzyka oraz GAP	17
5.3. Sposób przygotowania dokumentacji SZBI	18
6. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji	22
6.1. Zakres i sposób wdrożenia	22
7. Przeprowadzenie testów penetracyjnych pod kątem wykorzystania znanych podatności	24
7.1. Opis prac objętych pentestami	25
7.2. Przeprowadzenie testów penetracyjnych infrastruktury	26
Testy bezpieczeństwa sieci LAN	26
Testy styku sieci lokalnej z Internetem	26
Testy urządzeń służących do filtrowania ruchu sieciowego	26
7.3. Przeprowadzenie testów penetracyjnych aplikacji	26
7.4. Raport	27
8. Przeprowadzenie szkoleń	27
8.1. Wymagania ogólne dla szkolenia	27
8.2. Szkolenie z ochrony przed wyludzeniem osobowych i informacji	28
8.3. Szkolenie ze stosowania i budowania silnych haseł, wykorzystywania menadżerów haseł oraz szyfrowania danych osobowych	29

8.4.	Szkolenia z zabezpieczenia sprzętu prywatnego wykorzystywanego do celów służbowych	29
8.5.	Przeszkolenie użytkowników z zakresu SZBI	29
8.6.	Szkolenie specjalistyczne dla informatyka	32
9.	Kryteria jakościowe dla odbioru przedmiotu Zamówienia.....	33
9.1.	W zakresie krytycznych systemów teleinformatycznych	33
9.2.	W zakresie krytycznych procesów przetwarzania informacji.....	33
9.3.	Dokumentacji projektowej (w tym SZBI, raportów i innych)	33
9.4.	W zakresie szkoleń	33
9.5.	W zakresie testów penetracyjnych	33
9.6.	W zakresie testów socjotechnicznych	34

Słownik

L.P	Pojęcie	Opis
1.	Zamawiający	Gmina Dobra 34-642 Dobra 233 Reprezentowana przez Urząd Gminy Dobra 34-642 Dobra 233 Zamówienie będzie realizowane w następujących jednostkach: 1. Urząd Gminy Dobra (tel. 18 333-00-20) 2. Gminny Ośrodek Pomocy Społecznej w Dobrej (tel. 18 333-00-60) 3. Dzienny Dom "Senior plus" w Dobrej (tel. 18 333-00-11) 4. Zespół Obsługi Szkół i Przedszkoli w Dobrej (tel. 18 333-00-20) 5. Szkoła Podstawowa im. Leopolda Węgrzynowicza w Dobrej (tel. 18 333-00-09) 6. Zespół Placówek Oświatowych w Jurkowie (tel. 18 334-00-22), w skład którego wchodzi: a) Szkoła Podstawowa im. Władysława Orkana w Jurkowie ze Szkołą Filialną im. Wincentego Pola w Pótrzeczkach, b) Gminne Przedszkole w Jurkowie 7. Zespół Placówek Oświatowych w Skrzydłnej (tel. 18 333-10-06), w skład którego wchodzi: a) Szkoła Podstawowa im. Jana Pawła II w Skrzydłnej b) Gminne Przedszkole w Skrzydłnej 8. Szkoła Podstawowa im. Batalionów Chłopskich w Chyszówkach (tel. 18 333-21-89) 9. Szkoła Podstawowa im. Stanisława Wyspiańskiego w Stróży (tel. 18 333-15-45) 10. Szkoła Podstawowa im. Janusza Korczaka w Wilczycach (tel. 18 333-24-17) 11. Gminne Przedszkole nr 1 w Dobrej (tel. 18 333-00-10) 12. Szkoła Muzyczna I Stopnia w Dobrej (tel. 18 333-04-54).
2.	Test penetracyjny	Znany również jako pentest, to kontrolowany i systematyczny proces symulacji cyberataków na systemy komputerowe, sieci, aplikacje webowe, mobilne, infrastruktury chmurowe lub inne zasoby IT, w celu oceny ich bezpieczeństwa. Celem testu penetracyjnego jest identyfikacja, ocena i wykorzystanie podatności, które mogą być wykorzystane przez atakujących do uzyskania nieautoryzowanego dostępu do zasobów lub danych, naruszenia integralności systemów, lub zakłócenia dostępności usług. Pentestem nie jest identyfikacja znanych podatności przy użyciu narzędzi typu Nessus, Greenbone, Rapid7 czy innych.
3.	Test socjotechniczny	Kontrolowany i systematyczny proces symulacji prób manipulacji ludźmi w celu uzyskania poufnych informacji, dostępu do systemów komputerowych lub wywołania określonych działań, które mogą zagrozić bezpieczeństwu organizacji. Testy socjotechniczne są przeprowadzane w celu oceny świadomości pracowników na temat zagrożeń związanych

		z inżynierią społeczną oraz identyfikacji potencjalnych luk w procesach bezpieczeństwa organizacji.
4.	Środowisko aplikacyjne	Zintegrowane środowisko, które obejmuje wszystkie zasoby, narzędzia, oprogramowanie, usługi i konfiguracje niezbędne do uruchamiania, testowania, wdrażania oraz utrzymania aplikacji w ramach infrastruktury IT. Jest to ekosystem, w którym aplikacja funkcjonuje, obejmujący zarówno komponenty sprzętowe, jak i programowe, które wspierają działanie i rozwój aplikacji. Kluczowe Elementy Środowiska Aplikacyjnego: Sprzęt (Hardware): • Serwery: Maszyny fizyczne lub wirtualne, na których uruchamiane są aplikacje. • Pamięć Masowa: Dyski twarde, SSD, systemy SAN/NAS do przechowywania danych. • Sieć: Urządzenia sieciowe, takie jak routery, przełączniki, firewalles, które umożliwiają komunikację między komponentami systemu. Oprogramowanie (Software): • System Operacyjny: Podstawowe oprogramowanie, które zarządza zasobami sprzętowymi i dostarcza usług dla aplikacji (np. Windows, Linux). • Serwer Aplikacji: Oprogramowanie, które uruchamia aplikacje i zarządza ich działaniem (np. Apache Tomcat, Microsoft IIS). • Baza Danych: System zarządzania bazą danych (DBMS) używany do przechowywania i zarządzania danymi aplikacji (np. MySQL, PostgreSQL, Oracle). • Narzędzia Programistyczne: IDE, frameworki, biblioteki i inne narzędzia używane do tworzenia i testowania aplikacji (np. Eclipse, Visual Studio, Spring, Django). • Usługi i Infrastruktura (Services and Infrastructure): • Chmura: Usługi chmurowe, które oferują skalowalne zasoby obliczeniowe i pamięciowe (np. AWS, Microsoft Azure, Google Cloud Platform). • Usługi Wspomagające: Usługi takie jak serwery DNS, serwery proxy, usługi cache'owania (np. Redis, Memcached). Konfiguracja i Zarządzanie (Configuration and Management): • Konfiguracja Systemu: Ustawienia i parametry konfiguracyjne aplikacji i jej środowiska. • Automatyzacja i Zarządzanie Konfiguracją: Narzędzia do zarządzania konfiguracją i automatyzacji wdrożeń (np. Ansible, Puppet, Chef). • Monitorowanie i Logowanie: Systemy monitorowania wydajności i dostępności aplikacji, oraz logowania błędów i zdarzeń (np. Nagios, Prometheus, ELK Stack). Bezpieczeństwo (Security): • Kontrole Dostępu: Mechanizmy autoryzacji i uwierzytelniania użytkowników. • Ochrona Danych: Szyfrowanie danych, backupy, polityki zarządzania danymi. • Testy Bezpieczeństwa: Regularne audyty i testy penetracyjne w celu identyfikacji i eliminacji podatności. Dla aplikacji webowej, środowisko aplikacyjne może obejmować:

		• Serwer WWW: Apache HTTP Server lub Nginx. • System Operacyjny: Ubuntu Linux. • Baza Danych: MySQL lub PostgreSQL. • Język Programowania: Python z frameworkiem Django. • Usługi Chmurowe: AWS EC2 dla serwerów aplikacji, S3 dla przechowywania danych, RDS dla bazy danych. • Narzędzia Monitorujące: Prometheus dla monitorowania wydajności, Grafana dla wizualizacji danych. • Mechanizmy Bezpieczeństwa: Certyfikaty SSL/TLS dla zabezpieczenia komunikacji, usługi WAF (Web Application Firewall) dla ochrony przed atakami.
5.	2700X	Ilekoć mowa o 27001 Zamawiający ma na myśli normy: PN-EN ISO/IEC 27001:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania, PN-EN ISO/IEC 27002:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji.

1. Organizacja realizacji zamówienia

- 1) Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
- 2) Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiającego lub jednostki objętej zamówieniem nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
- 3) Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
- 4) Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
- 5) Jakiegokolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyko problemów.
- 6) Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z Zamawiającym. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
- 7) Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.

- 8) Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy SWZ i niniejszego OPZ i nie są z nimi sprzeczne.
- 9) Zamawiający we współpracy z Wykonawcą ustali harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
- 10) Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.
- 11) Wykonawca wyznaczy Kierownika Projektu, który stanowi jedyny punkt kontaktu w sprawach organizacyjnych, odpowiada za harmonogram, raportowanie postępu prac oraz udział w spotkaniach statusowych, o których mowa w pkt 9.
- 12) Zamówienie realizuje zespół w składzie zgodnym z wykazem osób złożonym w postępowaniu. Osoby wskazane w wykazie wykonują powierzone im czynności osobiście. Zmiana osoby wymaga uprzedniej zgody Zamawiającego, podania przyczyny zmiany i wskazania osoby o kwalifikacjach i doświadczeniu nie niższych niż wymagane w SWZ. Jeżeli zastępowana osoba była wskazana w kryterium oceny ofert, zastępca musi zachować co najmniej poziom kwalifikacji będący podstawą przyznania punktów, tak aby zmiana nie powodowała obniżenia jakości zadeklarowanej w ofercie. Przed dopuszczeniem do prac Wykonawca okazuje oryginały certyfikatów osób wskazanych w wykazie.
- 13) Kluczowe zadania zastrzeżone do osobistego wykonania przez Wykonawcę, zgodnie z rozdziałem „Podwykonawstwo” SWZ, obejmują: testy penetracyjne i wszelkie czynności wymagające dostępu do systemów produkcyjnych Zamawiającego, testy socjotechniczne, audyt zgodności z KRI oraz audyt zgodności z ustawą o krajowym systemie cyberbezpieczeństwa, a także opracowanie dokumentacji SZBI i analizy ryzyka. Zadania te nie mogą zostać powierzone podwykonawcy.
- 14) Produkty ICT, usługi ICT oraz procesy ICT wykorzystywane przez Wykonawcę do realizacji zamówienia — w tym narzędzia testowe, środowisko testowe i platforma szkoleniowa — nie mogą obejmować rozwiązań wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, ani rozwiązań objętych decyzją w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 tej ustawy. Wykaz wykorzystywanych elementów ICT Wykonawca składa wraz z ofertą na formularzu stanowiącym Załącznik nr 2 do SWZ i aktualizuje go w razie zmiany w trakcie realizacji umowy.
- 15) Wszystkie informacje pozyskane w toku realizacji zamówienia, w szczególności wyniki audytów, raporty z testów penetracyjnych i socjotechnicznych oraz informacje o podatnościach, stanowią informacje poufne. Wykonawca przetwarza je wyłącznie w celu realizacji zamówienia, na zasadach określonych w umowie oraz w umowie powierzenia przetwarzania danych osobowych. Po odbiorze przedmiotu zamówienia Wykonawca usuwa dane pozyskane w toku prac ze środowiska testowego i potwierdza to protokołarnie.
- 16) Terminy realizacji poszczególnych zadań określa harmonogram uzgodniony po zawarciu umowy, w granicach terminu wykonania zamówienia wskazanego w SWZ. Przy sporządzaniu harmonogramu uwzględnia się w szczególności wymóg zachowania co najmniej 5 dni roboczych pomiędzy kolejnymi turami testów socjotechnicznych, o którym mowa w pkt 3.1.

2. Przeprowadzenie audytów KRI

2.1. Przeprowadzenie audytów zgodności z Krajowymi Ramami Interoperacyjności

Lp	Jednostka objęta audytem	Liczba audytów
1.	Urząd Gminy Dobra	1
2.	Gminny Ośrodek Pomocy Społecznej w Dobrej	1

3.	Dzienny Dom "Senior+" w Dobrej	1
4.	Zespół Obsługi Szkół i Przedszkoli w Dobrej	1
5.	Szkoła Podstawowa im. Leopolda Węgrzynowicza w Dobrej wraz z klasami dotychczasowego Publicznego Gimnazjum w Dobrej	1
6.	Zespół Placówek Oświatowych w Jurkowie, w skład którego wchodzi: a) Szkoła Podstawowa im. Władysława Orkana w Jurkowie ze Szkołą Filialną im. Wincentego Pola w Pólrzeczach, b) klasy dotychczasowego Publicznego Gimnazjum w Jurkowie c) Gminne Przedszkole w Jurkowie	1
7.	Zespół Placówek Oświatowych w Skrzydlnej, w skład którego wchodzi: a) Szkoła Podstawowa im. Jana Pawła II w Skrzydlnej b) klasy dotychczasowego Publicznego Gimnazjum w Skrzydlnej c) Gminne Przedszkole w Skrzydlnej	1
8.	Szkoła Podstawowa im. Batalionów Chłopskich w Chyszówkach	1
9.	Szkoła Podstawowa im. Stanisława Wyspiańskiego w Stróży	1
10.	Szkoła Podstawowa im. Janusza Korczaka w Wilczycach	1
11.	Gminne Przedszkole nr 1 w Dobrej	1
12.	Szkoła Muzyczna I Stopnia w Dobrej	1

2.2. Zakres audytu oraz sposób prowadzenia audytu KRI

Przygotowanie do Audytu

a. Zebranie Informacji

- Dokumentacja Organizacji: Zebranie wszelkiej dokumentacji organizacji dotyczącej polityki bezpieczeństwa, procedur, procesów, systemów IT, architektury sieciowej, itp.
- Spotkanie Wstępne: Organizacja spotkania wstępnego z kierownictwem i kluczowymi interesariuszami w celu omówienia zakresu audytu, harmonogramu i oczekiwań.

b. Planowanie Audytu

- Definiowanie Zakresu Audytu: Określenie zakresu audytu zgodnie z wymaganiami KRI, w tym systemów, procesów i jednostek organizacyjnych, które będą objęte audytem. Zakres audytu musi być wynikiem odwołania się do §20 rozporządzenia z dnia 21 maja 2024 r w sprawie Krajowych Ram Interoperacyjności. Wykonawca ma obowiązek przygotować listę szczegółową sprawdzić (tzw. kontrolek), które doprecyzują zakres ogólnie opisany w rozporządzeniu. Lista, o której mowa musi być uzgodniona i zaakceptowana przez Zamawiającego.
- Tworzenie Harmonogramu: Ustalenie szczegółowego harmonogramu audytu, w tym daty przeglądów dokumentacji, wywiadów, inspekcji i analiz technicznych.
- Zespoły Audytowe: Skład zespołów audytowych z przypisaniem ról i odpowiedzialności.

2. Przegląd Dokumentacji

a. Analiza Dokumentów

- Przegląd Polityk i Procedur: Analiza polityk i procedur organizacji w celu sprawdzenia zgodności z wymaganiami KRI.
- Analiza Dokumentacji Technicznej: Przegląd dokumentacji technicznej, w tym konfiguracji systemów, schematów architektury sieciowej, raportów z testów bezpieczeństwa.
- Zgromadzenie Dowodów: Zbieranie dowodów potwierdzających zgodność, takich jak protokoły, logi systemowe, raporty z audytów wewnętrznych, wyniki testów penetracyjnych.

b. Ocena Zgodności

- Ocena Wymagań KRI: Porównanie polityk i procedur organizacji z wymaganiami KRI, identyfikacja obszarów zgodności i niezgodności.
- Dokumentowanie Wyników: Dokumentowanie wyników przeglądu dokumentacji, w tym wykazanie obszarów zgodności oraz wszelkich wykrytych niezgodności.

3. Inspekcje Techniczne i Wywiady

a. Inspekcje Techniczne

- Inspekcje Systemów IT: Przeprowadzanie inspekcji systemów IT w celu weryfikacji ich konfiguracji i zabezpieczeń.
- Testy Bezpieczeństwa: Wykonywanie testów bezpieczeństwa, takich jak skanowanie podatności, testy penetracyjne, analiza logów, weryfikacja ustawień zabezpieczeń.
- Ocena Sieci i Infrastruktur: Analiza topologii sieciowej, konfiguracji firewalli, VPN, systemów wykrywania i zapobiegania włamaniom.

b. Wywiady z Kluczowymi Pracownikami

- Wywiady z Kierownictwem: Rozmowy z kierownictwem IT oraz kierownikami odpowiedzialnymi za bezpieczeństwo informacji w celu oceny ich świadomości i zaangażowania w kwestie zgodności z KRI.
- Wywiady z Pracownikami Technicznymi: Wywiady z pracownikami odpowiedzialnymi za administrację systemów, bezpieczeństwo IT, zarządzanie siecią, w celu zrozumienia ich codziennych praktyk i procedur.

4. Analiza i Ocena Wyników

a. Analiza Zebranych Danych

- Porównanie z Wymaganiami KRI: Analiza zebranych danych i wyników testów w kontekście wymagań KRI.
- Identyfikacja Luk: Identyfikacja wszelkich luk bezpieczeństwa, braków w procedurach, niezgodności z wymaganiami KRI.

b. Opracowanie Raportu z Audytu

- Tworzenie Raportu: Przygotowanie szczegółowego raportu z audytu, zawierającego opis przeprowadzonych działań, wyniki inspekcji, wykryte niezgodności oraz rekomendacje dotyczące poprawy.
- Rekomendacje: Opracowanie konkretnych rekomendacji dotyczących działań korygujących i zapobiegawczych w celu zapewnienia pełnej zgodności z KRI.
- Podsumowanie: Przygotowanie podsumowania wyników audytu dla kierownictwa, zawierającego kluczowe wnioski i zalecenia.

5. Prezentacja i Omówienie Wyników

a. Prezentacja Raportu

- Spotkanie z Kierownictwem: Przedstawienie raportu z audytu kierownictwu organizacji, omówienie kluczowych wyników, niezgodności i rekomendacji.
- Dyskusja i Pytania: Umożliwienie kierownictwu i interesariuszom zadawania pytań, dyskusja nad wynikami audytu i proponowanymi działaniami korygującymi.

b. Plan Działań Korygujących

- Opracowanie Planu Działań: Wspólne opracowanie planu działań korygujących, ustalenie priorytetów, terminów realizacji i odpowiedzialności.
- Monitorowanie Realizacji: Ustalenie mechanizmów monitorowania realizacji działań korygujących i okresowych przeglądów zgodności.

6. Uwagi powdrożeniowe i monitorowanie

a. Wdrożenie Działań Korygujących

- Realizacja Rekomendacji: Wdrożenie zaleceń zawartych w raporcie audytu, zmiany w politykach, procedurach, konfiguracjach systemów.
- Weryfikacja Zgodności: Przeprowadzenie dodatkowych testów i inspekcji w celu weryfikacji skuteczności wdrożonych działań korygujących.

b. Ciągłe Monitorowanie

- Regularne Przeglądy: Organizowanie regularnych przeglądów zgodności z KRI, monitorowanie przestrzegania wprowadzonych zmian i procedur.
- Aktualizacja Polityk: Aktualizacja polityk i procedur w odpowiedzi na zmiany w wymaganiach KRI oraz nowe zagrożenia i technologie.

Produktem audytu będzie szczegółowy raport dla każdej jednostki zawierający:

- Opis przeprowadzonych działań audytowych.
- Wyniki przeglądów dokumentacji i inspekcji technicznych.
- Zidentyfikowane niezgodności i luki bezpieczeństwa.
- Rekomendacje dotyczące działań korygujących i zapobiegawczych.
- Podsumowanie kluczowych wniosków i zaleceń dla kierownictwa organizacji.

3. Przeprowadzenie audytu UoKSC dla Urzędu Gminy

Audyt przeprowadzany jest na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w brzmieniu obowiązującym od 3 kwietnia 2026 r. (Dz. U. z 2026 r. poz. 20 z późn. zm.; zmiana: Dz. U. z 2026 r. poz. 252, wdrażająca dyrektywę 2022/2555 — NIS2). Gmina Dobra jest podmiotem kluczowym w rozumieniu art. 5 ust. 1 ustawy, jako podmiot publiczny wskazany w załączniku nr 1 do ustawy. Audyt obejmuje weryfikację realizacji obowiązków z rozdziału 3 ustawy, w szczególności systemu zarządzania bezpieczeństwem informacji (art. 8), obowiązków kierownika podmiotu (art. 8c–8f), wyznaczenia osób kontaktowych (art. 9), dokumentacji (art. 10) oraz zgłaszania incydentów (art. 11), w zakresie opisanym poniżej.

Nr	Zadanie	Cel	Podstawa prawna / normatywna
1	Identyfikacja aktywów	Sporządzenie listy wszystkich aktywów IT, oprogramowania i danych.	uKSC: art. 8 ust. 1 pkt 2 lit. m; ISO/IEC 27001:2023 — A.5.9
2	Analiza ryzyka	Ocena zagrożeń i podatności wpływających na poufność, integralność i dostępność danych.	uKSC: art. 8 ust. 1 pkt 1 oraz pkt 2 lit. a; ISO/IEC 27001:2023 — 6.1.2
3	Weryfikacja kontroli bezpieczeństwa	Sprawdzenie, czy zastosowane zabezpieczenia (techniczne i organizacyjne) są adekwatne do poziomu ryzyka.	uKSC: art. 8 ust. 1 pkt 2 lit. h; ISO/IEC 27001:2023 — Załącznik A
4	Sprawdzenie zgodności z polityką bezpieczeństwa informacji	Ocena czy w obszarze bezpieczeństwa stosowana jest zatwierdzona polityka bezpieczeństwa, procedury i instrukcje.	uKSC: art. 8 ust. 1 pkt 2 lit. a; ISO/IEC 27001:2023 — A.5.1
5	Ocena zarządzania dostępem	Weryfikacja, czy dostęp do systemu jest przyznawany zgodnie z zasadą najmniejszych uprawnień i jest ewidencjonowany.	uKSC: art. 8 ust. 1 pkt 2 lit. n; ISO/IEC 27001:2023 — A.5.15, A.5.18
6	Ocena mechanizmów uwierzytelniania i autoryzacji	Sprawdzenie stosowania 2FA, zarządzania hasłami, kontroli sesji, logowania działań użytkowników.	uKSC: art. 8 ust. 1 pkt 2 lit. l oraz lit. j; ISO/IEC 27001:2023 — A.5.17, A.8.5
7	Weryfikacja logowania i audytowalności	Upewnienie się, że systemy rejestrują operacje istotne z punktu widzenia bezpieczeństwa i zgodności.	uKSC: art. 8 ust. 1 pkt 2 lit. g; ISO/IEC 27001:2023 — A.8.15, A.8.16

Nr	Zadanie	Cel	Podstawa prawna / normatywna
8	Ocena zabezpieczenia danych osobowych	Sprawdzenie, czy dane osobowe i medyczne są chronione przed nieautoryzowanym dostępem i przetwarzaniem.	uKSC: art. 8 ust. 1 pkt 2 lit. k; RODO art. 32; ISO/IEC 27001:2023 — A.5.34, A.8.24
9	Ocena procedur reagowania na incydenty	Sprawdzenie, czy istnieje skuteczna procedura reagowania na incydenty dotyczące oraz kanały zgłaszania do CSIRT.	uKSC: art. 8 ust. 1 pkt 4 oraz art. 11; ISO/IEC 27001:2023 — A.5.24–A.5.26
10	Ocena zgodności z wymaganiami ciągłości działania	Sprawdzenie, czy istnieją mechanizmy przywracania działania po awarii (backupy, DRP).	uKSC: art. 8 ust. 1 pkt 2 lit. f; ISO/IEC 27001:2023 — A.5.29, A.5.30, A.8.13
11	Sprawdzenie fizycznego bezpieczeństwa dostępu do serwerów	Ocena kontroli dostępu fizycznego (data center, serwerownia) w kontekście ochrony.	uKSC: art. 8 ust. 1 pkt 2 lit. c; ISO/IEC 27001:2023 — A.7
12	Ocena bezpieczeństwa łańcucha dostaw ICT	Weryfikacja zasad doboru i nadzoru nad dostawcami produktów, usług i procesów ICT, w tym uwzględniania podatności dostawcy, jakości dostarczanych rozwiązań oraz decyzji o uznaniu za dostawcę wysokiego ryzyka.	uKSC: art. 8 ust. 1 pkt 2 lit. e oraz art. 8 ust. 2; ISO/IEC 27001:2023 — A.5.19–A.5.22
13	Weryfikacja dokumentacji systemu zarządzania bezpieczeństwem informacji	Sprawdzenie kompletności, aktualności i nadzoru nad dokumentacją SZBI oraz zasad jej udostępniania osobom upoważnionym.	uKSC: art. 10; ISO/IEC 27001:2023 — 7.5
14	Sporządzenie raportu audytowego	Dokumentacja wszystkich ustaleń, rekomendacji i niezgodności w odniesieniu do ISO 27001 i KSC.	uKSC: art. 15 ust. 1; ISO 19011; ISO/IEC 27001:2023 — 9.2
15	Wskazanie niezgodności i działań korygujących	Sformułowanie zaleceń oraz planu działań naprawczych, jeśli stwierdzone zostaną braki w zabezpieczeniach.	uKSC: art. 8 ust. 1 pkt 2 lit. h; ISO/IEC 27001:2023 — 10.2

3.1. Przeprowadzenie testów socjotechnicznych w ramach audytu KSC

Testy socjotechniczne realizowane są w co najmniej dwóch turach. Odstęp pomiędzy kolejnymi turami nie może być krótszy niż 5 dni roboczych, tak aby użytkownicy nie orientowali się, że test jest częścią kampanii phishingowej. Harmonogram i częstotliwość prowadzenia testów muszą być uzgodnione z Zamawiającym.

3.2. Warunki wstępne i sposób realizacji

W celu przeprowadzenia testów muszą zostać spełnione następujące warunki:

Sposób realizacji testów

Testy będą prowadzone w oparciu o konkretne scenariusze. Każdy scenariusz będzie oznaczony jako osobna część, która będzie podlegała oddzielnej weryfikacji względem wyników. Planowane jest dzielenie poszczególnych testów na części oraz grupy docelowe, możliwa będzie zmiana charakterystyki testów w trakcie ich trwania w celu weryfikacji skuteczności. Zmiana będzie możliwa w przypadku gdy nie wpłynie w sposób znaczący na modyfikację scenariusza i nie wymusi przebudowy środowiska testowego.

Środowisko testowe

W celu przeprowadzenia testów Wykonawca przygotuje dedykowane dla celów testów środowisko testów, w którym składowane będą w sposób bezpieczny wszystkie dane pochodzące z testów. W ww. środowisku muszą zostać udostępnione narzędzia umożliwiające przeprowadzenie testów stanowiących przedmiot projektu. Środowisko testowe będzie zbudowane w oparciu o sprzęt i oprogramowanie należące do Wykonawcy.

Zaangażowanie Wykonawcy

Wykonawca musi zapewnić wszystkie komponenty wymagane do przeprowadzenia testów bez ponoszenia przez Zamawiającego dodatkowych kosztów. Ze strony Wykonawcy musi zostać dedykowany zespół co najmniej dwóch osób, które będą odpowiedzialne za przeprowadzenie testów. Tylko wybrane osoby będą komunikowały się z Klientem w celu wymiany informacji pochodzących z testów. Środowisko testów zostanie zabezpieczone w celu ochrony przed nieautoryzowanym dostępem.

Zaangażowanie Zamawiającego

Ze strony Zamawiającego zostaną dedykowane osoby, które będą kompetentne i władne weryfikować przedmiot i wynik poszczególnych faz testów w trakcie ich trwania. Osoby wchodzące w skład zespołu powinny mieć możliwość swobodnego podejmowania decyzji w zakresie realizacji testów.

3.3. Szczegółowy opis testów

W celu przeprowadzenia testów dobór grup oraz zasięg będzie prowadzony wraz z Zamawiającym, tak aby efekt był poparty znajomością struktury organizacyjnej.

Przeprowadzenie testów socjotechnicznych dla pracowników Urzędu Gminy	1
---	---

3.3.1. Stworzenie fałszywych stron

Zadaniem Wykonawcy jest opracowanie trzech fałszywych stron dostępnych pod trzema różnymi domenami, które będą przypominały strony zarządzane przez Urząd. Sposób działania strony Wykonawca przedstawi do akceptacji Zamawiającemu i po akceptacji podłączy strony pod domeny również uzgodnione z Zamawiającym.

Przygotowanie Fałszywych Stron

Wykonawca przygotuje zestaw fałszywych stron internetowych, które będą naśladować wygląd i funkcjonalność autentycznych stron Zamawiającego. Strony te będą analizowane pod kątem ich skuteczności w oszukiwaniu użytkowników oraz zdolności do zbierania poufnych informacji.

Rejestracja Domen (Typosquatting)

Wykonawca przeprowadzi analizę możliwości rejestracji domen, które mogą być wykorzystane do typosquattingu. Zostaną zarejestrowane przykładowe domeny, które różnią się od prawdziwych domen Zamawiającego minimalnymi zmianami w pisowni.

Rejestracja Domen (Punycode)

Wykonawca rejestruje domeny wykorzystujące punycode, które wyglądają podobnie do prawdziwych domen Zamawiającego, ale zawierają znaki specjalne. Celem jest ocena, jak łatwo można przeoczyć te różnice i jak skutecznie mogą być one wykorzystane do ataków phishingowych.

Identyfikacja Zagrożeń

Wykonawca przeprowadzi szczegółową analizę przygotowanych fałszywych stron oraz zarejestrowanych domen, aby zidentyfikować potencjalne zagrożenia i podatności. Analiza obejmie ocenę skuteczności tych stron w oszukiwaniu użytkowników oraz potencjalne skutki wyłudzenia danych.

Raport z Testów

Wyniki testów zostaną przedstawione w szczegółowym raporcie, który obejmie:

- Opis przeprowadzonych działań i zastosowanej metodyki.
- Listę zidentyfikowanych fałszywych stron i domen.
- Analizę ryzyka związanego z typosquattingiem i punycodem.

Rekomendacje

Na podstawie przeprowadzonych testów, Wykonawca przedstawi Zamawiającemu rekomendacje dotyczące:

- Wzmocnienia mechanizmów wykrywania i blokowania fałszywych stron.
- Poprawy procedur weryfikacji domen.
- Szkolenia pracowników w zakresie rozpoznawania phishingu.
- Implementacji dodatkowych środków bezpieczeństwa.

3.3.2. Wysłanie wiadomości pocztą elektroniczną

Celem testów jest sprawdzenie efektywności działania funkcji serwera poczty w zakresie wykrywania i ochrony przed phishingiem. Zamawiający oczekuje, że w tym celu Wykonawca wyśle co najmniej trzy spreparowane wiadomości, które winny być zablokowane przez serwer, bo stanowią phishing.

W celu przeprowadzenia testów phishingu Zamawiający dokona, poprzez dodanie adresu IP serwera Wykonawcy, modyfikacji ustawień poczty w sposób zezwalający Wykonawcy na dostarczenie spreparowanych wiadomości.

Przygotowanie Fałszywych Wiadomości Email

Wykonawca przygotowuje zestaw fałszywych wiadomości email, które będą naśladować wygląd i treść autentycznych wiadomości pochodzących od Zamawiającego. Wiadomości te mogą zawierać:

- Linki do fałszywych stron internetowych.
- Bezpieczne załączniki testowe symulujące cechy złośliwych załączników, bez zdolności do wyrządzenia szkody.
- Prośby o ujawnienie poufnych informacji.

Scenariusze Ataków

Wykonawca przeprowadzi symulowane ataki phishingowe według różnych scenariuszy, które mogą obejmować:

- **Spear Phishing:** Ukierunkowane ataki na konkretne osoby lub grupy pracowników.
- **Whaling:** Ataki skierowane na wysokiego szczebla menedżerów lub decydentów.
- **Clone Phishing:** Tworzenie kopii autentycznych wiadomości email z drobnymi zmianami prowadzącymi do złośliwych zasobów.

Wysyłka Fałszywych Wiadomości Email

Wykonawca przeprowadzi kontrolowaną wysyłkę fałszywych wiadomości email do wybranej grupy pracowników Zamawiającego. Celem jest ocena, jak wielu użytkowników zostanie oszukanych przez te wiadomości i jakie działania podejmą.

Identyfikacja Zagrożeń

Wykonawca przeprowadzi szczegółową analizę reakcji pracowników na fałszywe wiadomości email, w tym:

- Procent użytkowników, którzy kliknęli w złośliwe linki.
- Procent użytkowników, którzy pobrali złośliwe załączniki.
- Procent użytkowników, którzy podjęli próbę ujawnienia informacji w kontrolowanym scenariuszu; rzeczywiste hasła, kody jednorazowe, tokeny MFA, klucze dostępu ani inne dane uwierzytelniające nie mogą być zbierane, przesyłane ani przechowywane.

Raport z Testów

Wyniki testów zostaną przedstawione w szczegółowym raporcie, który obejmie:

- Opis przeprowadzonych działań i zastosowanej metodologii.
- Analizę skuteczności fałszywych wiadomości email.
- Identyfikację podatności i zagrożeń.
- Rekomendacje dotyczące działań korygujących i środków zapobiegawczych.

Rekomendacje

Na podstawie przeprowadzonych testów, Wykonawca przedstawi Zamawiającemu konkretne rekomendacje dotyczące:

- Wzmocnienia mechanizmów wykrywania i blokowania fałszywych wiadomości email.
- Poprawy procedur weryfikacji autentyczności wiadomości email.
- Implementacji dodatkowych środków bezpieczeństwa.

Podsumowanie

Realizacja testów zgodnie z powyższym opisem ma umożliwić Zamawiającemu zidentyfikowanie potencjalnych zagrożeń związanych z phishingiem opartym na fałszywych wiadomościach email, a także na wdrożenie skutecznych środków ochrony, zwiększających bezpieczeństwo informacji i danych osobowych.

4. Przeprowadzenie audytu bezpieczeństwa w obszarze sieci, serwerów oraz oprogramowania serwerowego

Lp	Jednostka	Liczba audytów
1.	Urząd Gminy Dobra	1

Wykonawca przeprowadzi audyt bezpieczeństwa w obszarze sieci, serwerów oraz oprogramowania serwerowego dla Urzędu Gminy Dobra (1 kpl.). Audyt ma na celu weryfikację poprawności konfiguracji, identyfikację podatności oraz ocenę zgodności stosowanych rozwiązań z dobrymi praktykami bezpieczeństwa, niezależnie od testów penetracyjnych opisanych w rozdziale dotyczącym przeprowadzenia testów penetracyjnych.

Audyt zostanie przeprowadzony w siedzibie Zamawiającego, w oparciu o analizę dokumentacji, wywiady z personelem IT oraz przegląd konfiguracji urządzeń i systemów wskazanych przez Zamawiającego.

Sposób prowadzenia audytu:

Audyt zostanie przeprowadzony w następujących etapach:

1. Przygotowanie do audytu – pozyskanie od Zamawiającego dokumentacji sieci, wykazu serwerów i kluczowego oprogramowania serwerowego oraz ustalenie harmonogramu prac.
2. Przegląd dokumentacji – analiza schematów sieci, polityk bezpieczeństwa oraz procedur eksploatacyjnych dotyczących serwerów i sieci.
3. Inspekcja techniczna – przegląd rzeczywistej konfiguracji urządzeń sieciowych i serwerów oraz wywiady z administratorami IT.

4. Analiza i ocena wyników – zestawienie zidentyfikowanych nieprawidłowości i podatności wraz z oceną ich krytyczności.
5. Prezentacja wyników – omówienie ustaleń audytu z Zamawiającym oraz przekazanie raportu końcowego.

W ramach audytu Wykonawca w szczególności:

- Zweryfikuje architekturę sieci lokalnej, w tym segmentację (VLAN), konfigurację urządzeń brzegowych oraz zasady routingu i filtrowania ruchu;
- Dokona przeglądu konfiguracji serwerów fizycznych i wirtualnych pod kątem zgodności z dobrymi praktykami bezpieczeństwa (hardening systemów operacyjnych);
- Zweryfikuje konfigurację oprogramowania serwerowego (systemy operacyjne, usługi katalogowe, bazy danych, usługi sieciowe) pod kątem znanych podatności oraz zbędnie uruchomionych usług;
- Oceni proces zarządzania aktualizacjami i poprawkami bezpieczeństwa (patch management) dla serwerów oraz kluczowego oprogramowania serwerowego;
- Zweryfikuje zasady zarządzania kontami uprzywilejowanymi oraz dostępem administracyjnym do serwerów i urządzeń sieciowych;
- Dokona przeglądu konfiguracji mechanizmów tworzenia kopii zapasowych serwerów oraz procedur ich testowania;
- Zweryfikuje konfigurację mechanizmów rejestrowania zdarzeń (logowania) na serwerach i urządzeniach sieciowych pod kątem możliwości wykrywania incydentów bezpieczeństwa;
- Oceni zgodność zabezpieczeń sieci i serwerów z wymaganiami wynikającymi z Krajowych Ram Interoperacyjności oraz ustawy o krajowym systemie cyberbezpieczeństwa.

Raport z audytu:

Wynikiem audytu będzie raport zawierający co najmniej:

1. Pełny spis i opis przeprowadzonych prac wraz z zakresem objętych audytem urządzeń, serwerów i systemów.
2. Szczegółowy wykaz zidentyfikowanych podatności i nieprawidłowości konfiguracyjnych wraz z oceną ich krytyczności.
3. Rekomendacje działań naprawczych możliwych do wdrożenia przez Zamawiającego, z uwzględnieniem priorytetu wynikającego z krytyczności ustaleń.
4. Podsumowanie zgodności z wymaganiami KRI oraz ustawy o krajowym systemie cyberbezpieczeństwa, możliwe do wykorzystania przy planowaniu dalszych działań w zakresie podnoszenia poziomu cyberbezpieczeństwa Urzędu Gminy Dobra.

5. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

Celem niniejszego zamówienia jest opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej SZBI) dla:

Lp	Jednostka	Liczba SZBI
2.	Urząd Gminy Dobra	1
3.	Gminny Ośrodek Pomocy Społecznej w Dobrej	1
4.	Zespół Obsługi Szkół i Przedszkoli w Dobrej	1

5.1. Inwentaryzacja zasobów informacyjnych

Należy pozyskać informacje na temat:

- Krytycznych systemów teleinformatycznych służących do przetwarzania informacji – należy przez to rozumieć, że Wykonawca wraz z Zamawiającym winien pośród wszystkich systemów teleinformatycznych zidentyfikować systemy krytyczne, które są kluczowe dla prawidłowego funkcjonowania działalności realizowanej przez Zamawiającego. Systemy krytyczne to takie systemy, które w przypadku niedostępności w istotny sposób uniemożliwiają całkowicie i/lub obniżają zdolność Zamawiającego do prowadzenia przez niego podstawowej działalności i/lub informacje przetwarzane w tych systemach stanowią dla Zamawiającego istotną wartość albo generują wysokie ryzyko w przypadku naruszenia przetwarzanych w nich danych. Zamawiający informuje, że samodzielnie zidentyfikował 10 takich systemów, ale podczas prowadzenia prac z Wykonawcą ww. systemów może zostać zidentyfikowanych zdecydowanie więcej.
- Krytycznych procesów przetwarzania informacji – należy przez to rozumieć zidentyfikowanie i opisanie procesów przetwarzania informacji, które są kluczowe dla prawidłowego funkcjonowania działalności realizowanej przez Zamawiającego. Przez proces należy rozumieć zestaw połączonych ze sobą sekwencyjnie czynności, wykonywanych przez osoby przypisane do ról, w określonym czasie oraz przy pomocy określonych systemów teleinformatycznych w tym krytycznych systemów teleinformatycznych. Procesy krytyczne to takie, które w przypadku zakłócenia w istotny sposób ograniczają lub uniemożliwiają prowadzenie działalności podstawowej Zamawiającego i/lub takie, w których informacje przetwarzane w ramach tych procesów stanowią dla Zamawiającego istotną wartość albo generują wysokie ryzyko w przypadku naruszenia przetwarzanych w nich danych. Zamawiający informuje, że w jego ocenie minimalna liczba procesów to 10, ale podczas prowadzenia prac z Wykonawcą ww. systemów może zostać zidentyfikowanych więcej.
- Kluczowych osób dla realizacji procesów przetwarzania informacji – należy przez to rozumieć identyfikację osób, których nieobecność albo niedostępność zakłóci w istotny sposób albo uniemożliwi całkowicie i/lub znacząco obniży zdolność Zamawiającego do prowadzenia przez niego podstawowej działalności.

5.2. Szacowanie ryzyka oraz GAP

Należy przeprowadzić Szacowanie ryzyka, które umożliwi identyfikację ryzyka w obszarze:

- technicznym (systemy, narzędzia i zasoby umożliwiające przetwarzanie informacji),
- organizacyjnym (procesy przetwarzania informacji oraz zapewnienia ciągłości działania),
- zasobów ludzkich (osoby przetwarzające informacje),

Kluczowym dla Zamawiającego jest by precyzyjnie określić sposób minimalizacji ryzyka środkami, który dysponuje przy założeniu, że wynik minimalizacji będzie dla Zamawiającego akceptowalny. W przypadku braku właściwych środków dla celów minimalizacji Wykonawca proponuje środki zastępcze, które mogą od Zamawiającego wymagać inwestycji.

Szacowanie ryzyka należy przeprowadzić w oparciu o kryteria ogólne (generyczne) np.: ryzyko pożaru, zalania, przegrzania, dostępności, umowy wsparcia i serwisu (SLA) ale przede wszystkim winno być prowadzone w oparciu o kryteria rzeczowe, charakterystyczne dla wybranego systemu teleinformatycznego, procesu, osoby. Należy przez to rozumieć, że w zależności od przedmiotu analizy należy np.: analizować dostępność wybranych komponentów teleinformatycznych, teletechnicznych na rynku polskim, potencjał dostawcy/wykonawcy do utrzymania systemu, zdolność do dostosowania się do zmieniającego otoczenia, dostępność kompetencji osób kluczowych na rynku pracy, konkurencję pośrednią i bezpośrednią itp.

5.3. Sposób przygotowania dokumentacji SZBI

Dokumentacja SZBI ma zostać wykonana dla trzech jednostek wskazanych przez Zamawiającego spośród jednostek objętych audytem zgodności z KRI. Wykaz tych jednostek Zamawiający przekaże Wykonawcy najpóźniej w dniu zawarcia umowy. Dla pozostałych jednostek objętych audytem Wykonawca opracowuje wyłącznie rejestr ryzyka oraz analizę GAP. Wykonawca jest zobowiązany zapewnić Zamawiającemu pełne autorskie prawa majątkowe do dokumentacji wytworzonej w ramach zamówienia, na zasadach określonych w umowie, oraz zapewnić odpowiednie upoważnienia i zobowiązania twórców w zakresie wykonywania autorskich praw osobistych. Zabrania się wykorzystywania generatywnej sztucznej inteligencji do tworzenia, redagowania, parafrazowania, streszczania, tłumaczenia lub innego opracowywania dokumentacji SZBI i innych dokumentów stanowiących przedmiot odbioru, a także do przetwarzania w takich systemach danych, dokumentów lub informacji Zamawiającego.

- Zakaz dotyczy publicznych i prywatnych usług generatywnej AI, lokalnych i chmurowych modeli generatywnych oraz funkcji generatywnych wbudowanych w inne aplikacje. Nie obejmuje zwykłych narzędzi niegeneratywnych, takich jak sprawdzanie pisowni, formatowanie, wyszukiwanie tekstu czy mechanizmy obliczeniowe, o ile nie przekazują treści do modelu generatywnego.
- Wykonawca odpowiada za samodzielne opracowanie dokumentacji przez personel posiadający wymagane kompetencje oraz za jej indywidualne dostosowanie do procesów, infrastruktury, ryzyk i wymagań jednostki, dla której dokumentacja jest przygotowywana.
- Na żądanie Zamawiającego Wykonawca składa oświadczenie potwierdzające przestrzeganie zakazu wykorzystywania generatywnej AI oraz posiadanie praw i upoważnień niezbędnych do przeniesienia autorskich praw majątkowych zgodnie z umową.

SZBI ma określać wewnętrzne wymagania dotyczące bezpieczeństwa informacji i zapewni praktyczne rozwiązania w tym zakresie poprzez odpowiednio ustanowione metody, czynności oraz narzędzia. Przez praktyczne rozwiązania Zamawiający rozumie opisanie w ramach dokumentacji SZBI sposobów zapewnienia bezpieczeństwa informacji, które będą minimalizowały ryzyka wystąpienia zdarzeń (incydentów) związanych z bezpieczeństwem informacji, w tym dotyczących naruszenia ochrony danych osobowych. Zamawiający wymaga od Wykonawcy określenia propozycji działań w ramach postępowania ze zidentyfikowanymi ryzykami, w tym dotyczących wdrożenia określonych środków organizacyjnych i technicznych:

- prewencyjnie (poprzez ograniczenie możliwości popełnienia błędu przez człowieka oraz naprawę błędów, które wystąpiły),
- odstraszająco (poprzez zastosowanie środków, które w sposób zrozumiały określą konsekwencje wynikające z niewłaściwego postępowania z informacją),
- reaktywnie (które umożliwią Zamawiającemu prowadzenie analiz po naruszeniach informacji oraz będą stanowiły źródło informacji analitycznych),

Zamawiający wymaga, aby zapisy SZBI były zgodne i kompletne, tj. odnosiły się wprost, do wymagań określonych w normach:

- PN-EN ISO/IEC 27001:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania,
- PN-EN ISO/IEC 27002:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji.
- Dalej obszar opisany w obu normach może być zwany ISO 2700X.

Zamawiający wymaga, żeby zapisy dokumentacji SZBI odnosiły się do wszystkich, i w każdym przypadku do konkretnych, rozdziałów i punktów ww. norm, z literalnym zachowaniem numeracji i nazewnictwa.

Ponadto Zamawiający wymaga, aby dokumentacja SZBI zawierała zapisy dotyczące środków organizacyjnych i technicznych zgodne z rekomendacjami Narodowych Standardów Cyberbezpieczeństwa (NSC), których treść dostępna jest pod adresem <https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber>. Zgodność w tym zakresie ma być osiągnięta poprzez zawarcie w dokumentacji SZBI wymagań NSC w sposób, który umożliwi Zamawiającemu jednoznaczną identyfikację i odniesienie w zapisach SZBI określonych w NSC wymagań dotyczących zabezpieczeń sieci i systemów informatycznych. Wykonawca wraz z Zamawiającym uzgodni przed realizacją zakres NSC, który należy uwzględnić w zadaniach Wykonawcy.

Dokumentacja SZBI musi zostać przygotowana w sposób umożliwiający Zamawiającemu w przyszłości zgłoszenie gotowości do certyfikacji SZBI przez zewnętrzną, akredytowaną przez Polskie Centrum Akredytacji, jednostkę certyfikującą.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji stanowi podstawę dla formalnego rozliczenia się z ochrony informacji. Wykonawca opracuje SZBI bazując na zakresie opisanym w normach ISO 2700X.

Zakres przedmiotowy dokumentacji SZBI musi bezpośrednio pokrywać się z tytułami punktów i podpunktów normy, aby nie było konieczności poszukiwania w dokumentacji zakresu, którego dotyczy wybrana jej część.

Przykład rejestru ryzyka, który docelowo zostanie uzgodniony z Zamawiającym.

Wskaźnik statusu ryzyka	ID Ryzyka	Data identyfikacji ryzyka	Narażony zasób	Kategoria ryzyka	Opis ryzyka	Wpływa na			Wstępna ocena ryzyka					Ocena ryzyka	Statut ryzyka	Właściciel ryzyka	Sposób postępowania z ryzykiem	Opis minimalizacji ryzyka	Szacowany koszt minimalizacji ryzyka w PLN brutto	Koszt minimalizacji ryzyka - dodatkowe informacje	Czy sposób minimalizacji wpływa na prywatność pracowników?	Czy wpływa na prywatność klientów w albo wprowadza ograniczenia?	Wpływa na			Ocena ryzyka szczegółowego					Ocena ryzyka	Statut ryzyka	Ryzyko po minimalizacji	Data kolejnego przeglądu
						Finanse	Wizerunek	Zgodność z prawem	Poufność	Integralność	Dostępność	Prawdopodobieństwo	Wpływ										Finanse	Wizerunek	Zgodność z prawem	Poufność	Integralność	Dostępność	Prawdopodobieństwo	Wpływ				
y	autonumer	19.10.2021	Dane biznesowe	Organizacyjne	Opis ryzyka	T	N	N	T	T	T	1 - 5	1 - 5	1 - 25	Wysokie	Imię Nazwisko	Minimalizować	Opis minimalizacji ryzyka	Czas naszych pracowników		T	N	N	N	N	N	N	4	4	16	Średnie	Poważne	17.04.2022	

6. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

Wdrożenie SZBI musi zostać zrealizowane z uwzględnieniem poniżej opisanych czynności, zadań oraz kryteriów. Kluczowe dla wdrożenia SZBI jest dostosowanie go, do wymagań oraz możliwości jednostki, dla której jest opracowywany. Wdrożeniem objęte są trzy jednostki, dla których przygotowano dokumentację SZBI.

6.1. Zakres i sposób wdrożenia

1. Przygotowanie i Planowanie

Zadania:

- **Zrozumienie Wymagań:** Przeprowadzenie analizy wymagań norm PN-EN ISO/IEC 27001:2023 i PN-EN ISO/IEC 27002:2023.
- **Zakres SZBI:** Określenie zakresu SZBI, czyli zdefiniowanie obszarów organizacji objętych systemem.
- **Polityka Bezpieczeństwa:** Opracowanie i zatwierdzenie polityki bezpieczeństwa informacji, która będzie stanowić fundament SZBI.
- **Zaangażowanie Kierownictwa:** Upewnienie się, że najwyższe kierownictwo jest zaangażowane i wspiera wdrożenie SZBI.

Kryteria jakościowe:

- Polityka bezpieczeństwa informacji jest formalnie zatwierdzona przez kierownictwo.
- Dokumentacja zakresu SZBI jest zgodna z celami organizacji i wymaganiami norm.
- Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
- Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

2. Ocena Ryzyka

Zadania:

- **Identyfikacja Zagrożeń i Wartości:** Przeprowadzenie analizy zagrożeń i identyfikacja wartości informacyjnych.
- **Analiza Ryzyka:** Określenie prawdopodobieństwa wystąpienia zagrożeń oraz potencjalnych skutków zgodnie z opisem zamieszczonym poniżej.
- **Ocena Ryzyka:** Zdefiniowanie poziomu ryzyka dla poszczególnych zagrożeń.
- **Plany Postępowania z Ryzykiem:** Opracowanie i wdrożenie planów redukcji ryzyka, akceptacji, przeniesienia lub unikania ryzyka.

Kryteria jakościowe:

- Analiza i ocena ryzyka.
- Plany postępowania z ryzykiem są zgodne z polityką bezpieczeństwa i zatwierdzone przez kierownictwo.

- Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
- Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

3. Kontrole Bezpieczeństwa

Zadania:

- **Dobór zabezpieczeń:** Na podstawie wyników oceny ryzyka wybór odpowiednich kontroli bezpieczeństwa zgodnie z ISO 27002:2023.
- **Wdrożenie Kontroli:** Implementacja wszystkich wymaganych kontroli technicznych, organizacyjnych i proceduralnych.
- **Dokumentacja Kontroli:** Utworzenie i utrzymanie dokumentacji wszystkich wdrożonych kontroli.

Kryteria jakościowe:

- Kontrole bezpieczeństwa są skutecznie wdrożone i działają zgodnie z założeniami.
- Dokumentacja jest kompletna i odzwierciedla aktualny stan wdrożonych kontroli.
- Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
- Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

4. Monitorowanie i Przegląd

Zadania:

- **Monitorowanie Efektywności:** Ciągłe monitorowanie efektywności wdrożonych kontroli bezpieczeństwa.
- **Przeglądy Wewnętrzne:** Regularne przeprowadzanie audytów wewnętrznych SZBI.
- **Przeglądy Zarządzania:** Okresowe przeglądy SZBI przez najwyższe kierownictwo.

Kryteria jakościowe:

- Raporty z monitorowania i przeglądów są regularnie generowane i analizowane.
- Audyty wewnętrzne są przeprowadzane zgodnie z harmonogramem i normami.
- Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
- Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

5. Doskonalenie

Zadania:

- **Zarządzanie Incydentami:** Ustanowienie procedur zarządzania incydentami bezpieczeństwa informacji.

- **Działania Korygujące:** Identyfikowanie i wdrażanie działań korygujących oraz zapobiegawczych.
- **Ciągłe Doskonalenie:** Regularne przeglądy i aktualizacje polityki, procedur oraz kontrolek SZBI.

Kryteria jakościowe:

- Wszystkie incydenty są rejestrowane, analizowane i odpowiednio zarządzane.
- Działania korygujące i zapobiegawcze są dokumentowane i śledzone pod kątem efektywności.
- Regularne aktualizacje SZBI w odpowiedzi na zmieniające się zagrożenia i wymagania.
- Wszyscy pracownicy są przeszkoleni w siedzibie Zamawiającego przez Wykonawcę.
- Wszyscy pracownicy zdali test wiedzy w zakresie właściwym dla Zadań, który potwierdza umiejętność stosowania SZBI.

7. Przeprowadzenie testów penetracyjnych pod kątem wykorzystania znanych podatności

Testy penetracyjne mają zostać przeprowadzone wyłącznie w Urzędzie Gminy.

Celem Zamawiającego jest sprawdzenie, czy wytworzone oraz dostarczone przez wykonawców, podwykonawców i dostawców elementy infrastruktury oraz aplikacje są bezpieczne do użytkowania.

W ramach zamówienia należy przeprowadzić testy penetracyjne, których celem jest między innymi wykrycie:

- luk i podatności związanych z zastosowaną architekturą aplikacji,
- luk i podatności wynikających z zastosowanych wzorców projektowych,
- luk i podatności związanych z zastosowanymi technologiami na poziomie warstwy prezentacji danych,
- luk i podatności związanych z zastosowanymi technologiami na poziomie warstwy aplikacji,
- luk i podatności związanych z zastosowanymi serwerami WWW lub ich niewłaściwej konfiguracji,
- luk i podatności związanych z zastosowanym środowiskiem aplikacyjnym lub jego niewłaściwą konfiguracją,
- luk i podatności związanych z niewłaściwą walidacją danych wejściowych,
- luk i podatności związanych z zaimplementowanymi mechanizmami uwierzytelniania i autoryzacji.

Zamawiający informuje, że pod pojęciem testów penetracyjnych należy rozumieć przeprowadzenie ręcznych czynności przez audytorów bezpieczeństwa technicznego wchodzących w skład zespołu Wykonawcy, co oznacza, że wyklucza się wykorzystanie narzędzi np. typu Nessus, Greenbone (Open VAS), Acunetix i podobnych do prowadzenia audytu. Zamawiający wyklucza możliwość wskazania badania na występowanie znanych podatności jako potwierdzenie wykonania audytu technicznego. Jednocześnie Zamawiający wskazuje, że przedmiot zamówienia obejmuje również skanowanie i identyfikację znanych podatności, do których Wykonawca może użyć wyżej wymienionych narzędzi.

Wykonywane przez Wykonawcę testy mają być uzgodnione z Zamawiającym przez co należy rozumieć uzgodnienie daty i czasu wykonania oraz wpływu testu na infrastrukturę Zamawiającego. O ile

wykonanie testu może wpłynąć negatywnie na dostępność testowanego elementu Wykonawca musi o tym poinformować Zamawiającego. Wykonawca zobowiązany jest bezpośrednio kontaktować się z dostawcami systemów teleinformatycznych, które testuje i później w których wykrył podatności albo zidentyfikował ryzyka celem wskazania sposobu postępowania.

Wykonawca zobowiązany jest do wykonania retestów celem weryfikacji poprawnego postąpienia z odnalezionymi ryzykami.

Testy wskazanych przez Zamawiającego aplikacji muszą zostać wykonane zgodnie z metodologią OWASP Application Security Verification Standard 4.0.3 Level 2.

Testy muszą zostać wykonane zgodnie z Penetration Testing Execution Standard.

Wykonawca w celu przeprowadzenia testów ma obowiązek przeprowadzić je zgodnie z Penetration Testing Framework w najnowszej dostępnej wersji.

7.1. Opis prac objętych pentestami

1. Ocena zagrożeń, wynikających ze zidentyfikowanych podatności, oraz opisanie sposobu minimalizacji zidentyfikowanych zagrożeń w celu podjęcia przez Zamawiającego czynności mających na celu zwiększenie odporności na wszelkie, znane na dzień audytu, formy zagrożeń.
2. Oceny wpływu podatności muszą zostać ocenione w skali CVSS wersji 4.0.
3. Analiza i wykazanie potencjalnego nieautoryzowanego dostępu do danych i zasobów w obrębie badanego systemu.
4. Na podstawie wyników przeprowadzonego audytu przygotować zalecenia w zakresie tzw. hardeningu aplikacji, systemów operacyjnych, usług serwerowych oraz infrastruktury sprzętowej (serwerów, przełączników, routerów oraz innych urządzeń aktywnych) w postaci gotowych do implementacji zaleceń, które może wykonać Zamawiający, wykonawca kluczowych komponentów platformy, wyłoniony w ramach postępowań, o których mowa wyżej, lub inna firma trzecia, posiadająca wiedzę i doświadczenie w zakresie wybranych technologii.
5. Przygotować inwentaryzację komponentów, na które składa się środowisko Zamawiającego.
6. Przygotować ocenę ryzyka wykorzystania, utrzymania, rozwoju każdego ze zidentyfikowanych w toku wykonywanych testów komponentów. Przygotować analizę ryzyk dotyczącą wyników i wniosków przeprowadzanych testów penetracyjnych i bezpieczeństwa, oraz dodatkowo:
 - a. występowania pojedynczych punktów awarii krytycznych, skutkującej całkowitym brakiem możliwości korzystania przez użytkowników;
 - b. występowania pojedynczych punktów usterek, skutkujących czasowym lub ograniczonym funkcjonowaniem konkretnych komponentów;
 - c. wpływu na systemy Zamawiającego ataków typu DoS;
7. Wykonawca ma podjąć próbę przełamania lub ominięcia zabezpieczeń WAF (z ang. Web Application Firewall), urządzeń UTM (z ang. Unified Threat Management), VPN.
8. O ile Wykonawca z powodzeniem przełamie zabezpieczenia i uzyska dostęp do sieci wewnętrznej Zamawiającego winien podjąć próbę przełamania zabezpieczeń sieci wewnętrznej w zakresie opisanym poniżej.
9. Wykonawca ma przeprowadzić testy penetracyjne wewnątrz sieci Zamawiającego w tym:
 - Wykonać rekonesans celem identyfikacji słabych punktów,
 - Podjąć próby przełamania zabezpieczeń urządzeń sieciowych,
 - Podjąć próby przełamania urządzeń podłączonych do sieci w tym komputerów, serwerów oraz innych urządzeń aktywnych,
 - Podjąć próbę przełamania sieci bezprzewodowej,
 - Podjąć próbę instalacji złośliwego oprogramowania oraz sprzętu,

- Podjąć próbę podsłuchiwania ruchu sieciowego

10. Wykonawca zobowiązany jest do przeprowadzenia analizy stacji roboczych pod kątem wykazania błędów konfiguracyjnych oraz opisanie sposobu ich naprawy.

7.2. Przeprowadzenie testów penetracyjnych infrastruktury

Wykonawca powinien przeprowadzić testy penetracyjne infrastruktury, których celem jest odnalezienie podatności wynikających z błędnej konfiguracji urządzeń sieciowych, urządzeń podłączonych do sieci przewodowej oraz bezprzewodowej oraz konfiguracji tych sieci. Testy penetracyjne infrastruktury mają być przeprowadzone lokalnie, w siedzibie Zamawiającego.

Testy bezpieczeństwa sieci LAN

- Próby oszukania działania przełącznika;
- Ataki Man-in-the-Middle: podsłuchiwanie, przechwytywanie sesji;
- Określenie producenta urządzeń sieciowych;
- Próba uzyskania dostępu do wydzielonych VLAN-ów;
- Uzyskanie informacji z protokołów routingu;
- Test zabezpieczeń protokołu SNMP na urządzeniach sieciowych: próba odczytu informacji, próba zmiany ustawień;
- Weryfikacja stosowanych kluczy SSL;
- Sprawdzenie restrykcji i ich skuteczności w komunikacji do sieci Internet;
- Analiza architektury pod względem optymalnego działania.

Testy styku sieci lokalnej z Internetem

- Skanowanie urządzenia w celu określenia działających usług;
- Identyfikacja wersji uruchomionych usług;
- Pogrupowanie odnalezionych usług do poszczególnych systemów, które je udostępniają;
- Próba wykonania nadużyć działających usług;
- Weryfikacja czy znalezione usługi i systemy posiadają znane błędy i podatności;
- Test wykrywalności ataków przez urządzenie brzegowe;
- Analiza architektury pod względem optymalnego działania;
- Określenie nazwy producenta;
- Weryfikacja stosowanych kluczy SSL;

Testy urządzeń służących do filtrowania ruchu sieciowego

- Generowanie złośliwego ruchu: w warstwie sieci, w warstwie aplikacji, na aplikacje webowe, ataki wychodzące;
- Przesyłanie malware'u poprzez użycie próbki przynajmniej 30 złośliwych programów;
- Generowanie ruchu o nietypowych godzinach;
- Próba wejścia na serwisy www zablokowane przez urządzenia;
- Próba nawiązania połączenia z podejrzanymi domenami;
- Nawiązanie połączenia do sieci Tor;
- Przeprowadzanie skanowania portów różnymi technikami, łącznie z obniżającymi wykrycie;
- Generowanie błędnego ruchu.

7.3. Przeprowadzenie testów penetracyjnych aplikacji

Wykonawca powinien przeprowadzić testy penetracyjne zgodnie z zestawieniem kategorii określonych na stronie <https://owasp.org/www-project-top-ten/> „Top 10 Web Application Security Risks”. Należy

przez to rozumieć, że Wykonawca w ramach testów wykona czynności sprawdzające każdy obszar podatności wskazanych w Top 10.

Testom będzie podlegała strona główna Urzędu oraz strona Biuletynu Informacji Publicznej oraz pozostałe strony wskazane przez zamawiającego w ilości określonej w zestawieniu.

Przez testy penetracyjne należy rozumieć ręczne poszukiwanie podatności:

- w konfiguracji serwerów baz danych oraz www, które pozostają w dyspozycji Zamawiającego,
- w kodzie źródłowym aplikacji podlegających testom,
- przeprowadzenie kontrolowanego testu odporności aplikacji na zwiększone obciążenie lub ruch, bez prowadzenia rozproszonego ataku DDoS; parametry testu wymagają uprzedniej pisemnej zgody Zamawiającego i nie mogą powodować niedostępności usług,
- w sposobie wykonywania się aplikacji.

7.4. Raport

Na potwierdzenie wykonania powyższego zakresu prac Wykonawca sporządzi raport zawierający minimum:

1. Pełny spis i opis przeprowadzonych prac,
2. Szczegółowy wykaz wykrytych podatności, wraz z pełnymi dowodami ich występowania,
3. Każda znana podatność zostanie oznaczona odpowiednim kodem ze słownika CVE (Common Vulnerabilities and Exposures),
4. Opisowe rekomendacje w zakresie sposobu postępowania z wykrytymi podatnościami wraz z podaniem zaleceń i instrukcji do wprowadzenia zmian konfiguracyjnych lub czynności naprawczych w celu właściwego postępowania z ryzykiem,

8. Przeprowadzenie szkoleń

Szkolenia opisane winny być przeprowadzone dla 80 pracowników wyznaczonych przez Zamawiającego.

Szkolenie specjalistyczne opisane w punkcie 8.6 ma zostać przeprowadzone dla wskazanego pracownika Urzędu Gminy.

8.1. Wymagania ogólne dla szkolenia

- 8.1.1. Szkolenie musi odbyć się w siedzibie Zamawiającego ale Wykonawca powinien również dostarczyć platformę umożliwiającą prowadzenie szkoleń i być gotowym do organizacji szkolenia online.
- 8.1.2. Wykonawca przygotowuje również szkolenie dla użytkowników końcowych (wszystkich pracowników oraz współpracowników Zamawiającego), które będzie dotyczyło dokumentów sklasyfikowanych jako wewnętrzne. W ramach szkolenia Wykonawca omówi zakres opisany w tych dokumentach oraz przygotowuje w postaci elektronicznej test wiedzy użytkowników.
- 8.1.3. Zamawiający udostępni bezpłatnie pomieszczenie wyposażone w rzutnik oraz dostęp do Internetu, na potrzeby szkolenia stacjonarnego.
- 8.1.4. Każde szkolenie powinno trwać od 3 do 6 godzin szkoleniowych dla 1 grupy szkoleniowej w ciągu dnia.
- 8.1.5. Liczba osób uczestniczących w szkoleniu nie przekroczy 20 osób na grupę.
- 8.1.6. Szkolenia będą odbywać się w dni robocze od poniedziałku do piątku w godzinach 7.30 – 15.30 w siedzibie Zamawiającego albo każdej jednostki w zależności od wyboru Zamawiającego.

8.1.7.W przypadku szkolenia prowadzonego dla szkół Wykonawca musi się liczyć z możliwością prowadzenia szkoleń w godzinach pomiędzy 14:00 a 19:00.

8.1.8.W celu maksymalizacji czasu nie przewiduje się przerw podczas szkolenia.

8.1.9.W ramach organizacji szkoleń Wykonawca zapewni:

8.1.9.1. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.

8.1.9.2. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:

8.1.9.2.1. Lista obecności Uczestników szkolenia (dienne, wypełniane oddzielnie każdego dnia szkolenia).

8.1.9.2.2. Lista odbioru zaświadczeń o ukończeniu szkolenia.

8.1.9.2.3. Ankieta satysfakcji ze szkolenia.

8.2. Szkolenie z ochrony przed wyłudzeniem osobowych i informacji

- Wprowadzenie do Bezpieczeństwa Informacji
 - Cel i znaczenie szkolenia
 - Przegląd zagrożeń cybernetycznych
 - Podstawowe zasady bezpieczeństwa informacji
- Wykrywanie Phishingu oraz Jego Odmian
 - Definicja i rodzaje phishingu (email, SMS, spear phishing, whaling)
 - Metody rozpoznawania phishingu
 - Przykłady ataków phishingowych
 - Praktyczne ćwiczenia w wykrywaniu phishingu
- Wykorzystywanie Mechanizmów Podwójnego Uwierzytelnienia (2FA)
 - Co to jest podwójne uwierzytelnienie (2FA) i dlaczego jest ważne
 - Rodzaje 2FA (SMS, aplikacje uwierzytelniające, tokeny sprzętowe)
 - Konfiguracja 2FA na popularnych platformach
 - Ćwiczenia praktyczne: wdrażanie i używanie 2FA
- Stosowanie VPN
 - Co to jest VPN i jak działa
 - Korzyści z używania VPN
 - Przegląd popularnych usług VPN
 - Praktyczne ćwiczenia: konfiguracja i korzystanie z VPN
- Stosowanie SSL/TLS
 - Podstawy SSL/TLS: co to jest i jak działa
 - Rola certyfikatów SSL/TLS
 - Jak sprawdzić poprawność certyfikatów SSL/TLS na stronach internetowych
 - Praktyczne ćwiczenia: konfiguracja SSL/TLS na serwerze
- Rozpoznawanie Fałszywych Stron i Domen (Typosquatting, Punycode i ich Odmiany)
 - Co to jest typosquatting i punycode
 - Techniki rozpoznawania fałszywych stron i domen
 - Narzędzia do weryfikacji domen i URL
 - Praktyczne ćwiczenia: identyfikacja fałszywych stron
- Obrona przed Fałszywymi Sieciami WiFi
 - Zagrożenia związane z fałszywymi sieciami WiFi (evil twin, rogue AP)
 - Jak rozpoznać i unikać fałszywych sieci WiFi
 - Narzędzia i techniki zabezpieczania się przed fałszywymi sieciami
- Bezpieczeństwo w Użytkowaniu Sztucznej Inteligencji
 - Wprowadzenie do sztucznej inteligencji i jej zastosowań

- Zagrożenia związane z wykorzystaniem AI (deepfake, automatyzacja ataków)
- Najlepsze praktyki w bezpiecznym używaniu AI
- Przykłady narzędzi i rozwiązań wspierających bezpieczeństwo AI

8.3. Szkolenie ze stosowania i budowania silnych haseł, wykorzystywania menedżerów haseł oraz szyfrowania danych osobowych.

- Skuteczne Tworzenie Haseł
 - Zasady tworzenia silnych haseł
 - Częste błędy przy tworzeniu haseł
 - Narzędzia do generowania silnych haseł
 - Praktyczne ćwiczenia: tworzenie i ocena haseł
- Skuteczne Szyfrowanie Danych
 - Podstawy szyfrowania danych: symetryczne i asymetryczne
 - Najlepsze praktyki szyfrowania danych w spoczynku i w tranzycie
 - Przykłady narzędzi do szyfrowania danych (VeraCrypt, BitLocker, PGP)
 - Ćwiczenia praktyczne: szyfrowanie i deszyfrowanie plików
- Wykorzystywanie Menedżerów Haseł
 - Dlaczego menedżery haseł są ważne
 - Przegląd popularnych menedżerów haseł (LastPass, 1Password, Bitwarden)
 - Jak bezpiecznie korzystać z menedżerów haseł
 - Praktyczne ćwiczenia: zakładanie kont i korzystanie z menedżerów haseł

8.4. Szkolenia z zabezpieczenia sprzętu prywatnego wykorzystywanego do celów służbowych

- Wprowadzenie: znaczenie bezpieczeństwa sprzętu prywatnego w pracy zdalnej i hybrydowej
 - Podstawowe zasady ochrony urządzeń prywatnych
 - Aktualizacje systemu i oprogramowania — dlaczego są kluczowe
 - Uwierzytelnianie i zarządzanie hasłami
 - Szyfrowanie danych na urządzeniu
 - Bezpieczne korzystanie z sieci Wi-Fi i VPN
 - Antywirus i ochrona przed malware czy wystarczy?
 - Backup danych i przywracanie systemu
 - Bezpieczne korzystanie z aplikacji służbowych i chmurowych
 - Ochrona prywatności i zapobieganie wyciekom danych
 - Zasady bezpiecznego korzystania z nośników zewnętrznych
 - Świadomość zagrożeń — phishing, ransomware i socjotechnika
 - Procedury postępowania w przypadku podejrzenia incydentu bezpieczeństwa
 - Podsumowanie i najlepsze praktyki ochrony sprzętu prywatnego

8.5. Przeszkolenie użytkowników z zakresu SZBI

Wykonawca musi przeszkolić użytkowników w zakresie gwarantującym nabycie umiejętności umożliwiających utrzymanie SZBI w kolejnych latach co oznacza, że Wykonawca winien przeprowadzić szkolenia we właściwym zakresie. Termin szkolenia musi zostać uzgodniony pomiędzy wykonawcą a jednostką, która będzie szkolona. Przeszkoleni muszą zostać wszyscy pracownicy jednostki. Wykonawca prócz przeprowadzenia szkoleń w jednostce przygotuje

szkolenia e-learning wzbogacone o test wiedzy, do których prawa autorskie i majątkowe przekaże każdej jednostce.

Wykonawca musi przygotować szkolenia dedykowane dla dwóch grup użytkowników:

Liderów – którzy będą odpowiedzialni za skuteczne doskonalenie oraz utrzymanie SZBI

Pozostałych użytkowników SZBI – którzy będą odpowiedzialni za skuteczne stosowania SZBI

Agenda Szkolenia z Zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Dla Liderów SZBI

1. Wprowadzenie do SZBI

- Wprowadzenie do ISO 27001 i ISO 27002
- Znaczenie SZBI dla organizacji

2. Rola Liderów w Utrzymaniu SZBI

- Obowiązki i odpowiedzialności liderów SZBI
- Kształtowanie kultury bezpieczeństwa informacji

3. Zarządzanie Ryzykiem

- Identyfikacja i ocena ryzyka
- Implementacja planów zarządzania ryzykiem
- Przykłady skutecznego zarządzania ryzykiem

4. Polityki i Procedury Bezpieczeństwa Informacji

- Tworzenie i aktualizacja polityk bezpieczeństwa
- Procedury operacyjne i techniczne
- Zarządzanie dokumentacją SZBI

5. Kontrole Bezpieczeństwa

- Wybór i implementacja odpowiednich kontroli bezpieczeństwa
- Monitorowanie i przegląd efektywności kontroli
- Studium przypadku z wdrożenia kontroli bezpieczeństwa

6. Audyt i Przeglądy SZBI

- Przygotowanie do audytów wewnętrznych i zewnętrznych
- Proces audytu i dokumentacja
- Analiza wyników audytu i wdrażanie działań korygujących

7. Zarządzanie Incydentami Bezpieczeństwa

- Identyfikacja i klasyfikacja incydentów
- Procedury reagowania na incydenty
- Dokumentacja i analiza incydentów

8. Ciągłe Doskonalenie SZBI

- Procesy ciągłego doskonalenia
- Rola liderów w inicjowaniu zmian

- Narzędzia i techniki doskonalenia SZBI
9. **Szkolenia i Podnoszenie Świadomości**
 - Programy szkoleniowe dla pracowników
 - Metody podnoszenia świadomości bezpieczeństwa
 - Testowanie i ocena skuteczności szkoleń
 10. **Zarządzanie Zgodnością**
 - Przegląd kluczowych regulacji dotyczących bezpieczeństwa informacji
 - Utrzymywanie zgodności z przepisami i normami
 - Dokumentowanie zgodności

Agenda Szkolenia z Zakresu SZBI

Dla Pozostałych Pracowników

1. **Wprowadzenie do SZBI**
 - Podstawy bezpieczeństwa informacji
 - Znaczenie SZBI dla organizacji
2. **Podstawowe Polityki i Procedury Bezpieczeństwa Informacji**
 - Kluczowe polityki bezpieczeństwa
 - Zasady i procedury, których należy przestrzegać
3. **Rozpoznawanie i Reagowanie na Zagrożenia**
 - Najczęstsze zagrożenia bezpieczeństwa informacji
 - Jak rozpoznawać i zgłaszać podejrzane działania
4. **Bezpieczne Praktyki Pracy z Danymi**
 - Bezpieczne korzystanie z systemów informatycznych
 - Ochrona danych osobowych i wrażliwych
 - Praktyki bezpiecznego zarządzania hasłami
5. **Zarządzanie Dostępem i Autoryzacją**
 - Zasady zarządzania dostępem do informacji
 - Procedury uzyskiwania i zmiany uprawnień
6. **Reagowanie na Incydenty Bezpieczeństwa**
 - Co robić w przypadku wykrycia incydentu bezpieczeństwa
 - Procedury zgłaszania incydentów
7. **Ochrona Przed Złośliwym Oprogramowaniem**
 - Rozpoznawanie i unikanie złośliwego oprogramowania
 - Zasady korzystania z programów antywirusowych
8. **Bezpieczne Korzystanie z Internetu i Poczty E-mail**

- Zasady bezpiecznego korzystania z Internetu
- Jak unikać phishingu i innych oszustw online

9. Znaczenie Szkolenia i Podnoszenia Świadomości

- Rola każdego pracownika w utrzymaniu bezpieczeństwa informacji
- Dostępne programy szkoleniowe i zasoby edukacyjne

10. Podsumowanie i Q&A

- Kluczowe wnioski ze szkolenia
- Sesja pytań i odpowiedzi

8.6. Szkolenie specjalistyczne dla informatyka

Szkolenie specjalistyczne dla informatyka ma zostać przeprowadzone dla wskazanego przez Zamawiającego pracownika odpowiedzialnego za obszar IT w Urzędzie Gminy Dobra (1 osoba). Szkolenie ma charakter techniczny i uzupełnia szkolenia z zakresu SZBI opisane w punkcie 8.5, koncentrując się na praktycznych aspektach zabezpieczenia infrastruktury IT, reagowania na incydenty oraz bieżącej obsługi narzędzi bezpieczeństwa.

Szkolenie powinno trwać nie mniej niż 16 godzin szkoleniowych (2 dni szkoleniowe) i powinno być prowadzone w formie uzgodnionej z Zamawiającym.

Zakres tematyczny szkolenia obejmuje co najmniej:

- Bieżące zagrożenia cyberbezpieczeństwa i wektory ataków (phishing, ransomware, malware, ataki socjotechniczne) z perspektywy administratora IT;
- Zasady bezpiecznej konfiguracji i utwardzania (hardening) systemów operacyjnych, serwerów oraz stacji roboczych;
- Zarządzanie podatnościami: identyfikacja, ocena ryzyka oraz proces wdrażania poprawek bezpieczeństwa (patch management);
- Podstawy bezpieczeństwa sieci: segmentacja, konfiguracja firewalli, VPN oraz monitorowanie ruchu sieciowego;
- Zasady tworzenia i testowania kopii zapasowych oraz procedury odtwarzania danych po incydencie;
- Rozpoznawanie i wstępna obsługa incydentów bezpieczeństwa zgodnie z procedurami wynikającymi z SZBI oraz ustawy o KSC;
- Zarządzanie uprawnieniami i kontami uprzywilejowanymi (w tym zasada najmniejszych uprawnień);
- Bezpieczeństwo urządzeń mobilnych oraz pracy zdalnej administratora;
- Podstawy analizy logów systemowych oraz korzystania z narzędzi klasy SIEM/EDR w zakresie wykrywania anomalii.

Wykonawca zapewni materiały szkoleniowe w formie elektronicznej oraz wyda uczestnikowi zaświadczenie o ukończeniu szkolenia. Szkolenie zakończy się sesją pytań i odpowiedzi oraz krótkim podsumowaniem kluczowych wniosków.

9. Kryteria jakościowe dla odbioru przedmiotu Zamówienia

9.1. W zakresie krytycznych systemów teleinformatycznych

- Zidentyfikowane wszystkie systemy krytyczne w kontekście zapewniania ciągłości działania Zamawiającego.
- Dla każdego zidentyfikowanego systemu krytycznego zidentyfikowano i przygotowano plan postępowania z ryzykiem.
- Przygotowano propozycje postępowania z oszacowanym ryzykiem, ze wskazaniem możliwych do wdrożenia środków technicznych i organizacyjnych.
- Zweryfikowano kompletność zapisów wymagań SZBI pod kątem zgodności pokrycia z zakresem wymagań określonych w normach 2700X.

9.2. W zakresie krytycznych procesów przetwarzania informacji

- Zidentyfikowano wszystkie procesy krytyczne w kontekście zapewniania ciągłości działania Zamawiającego.
- Dla każdego zidentyfikowanego procesu krytycznego przeprowadzono szacowanie i przygotowano plan postępowania z ryzykiem.

9.3. W zakresie audytu bezpieczeństwa sieci, serwerów oraz oprogramowania serwerowego

- Zidentyfikowano wszystkie serwery, urządzenia sieciowe oraz kluczowe oprogramowanie serwerowe objęte audytem.
- Dla każdej zidentyfikowanej podatności lub nieprawidłowości przygotowano rekomendację działania naprawczego.
- Raport z audytu został omówiony z Zamawiającym i przekazany w formie pisemnej.

9.4. Dokumentacji projektowej (w tym SZBI, raportów i innych)

- Pokrywa pełny zakres norm ISO 2700X.
- Każdy punkt normy zawiera opis środków organizacyjnych oraz technicznych zapewniających ochronę informacji. Należy przez to rozumieć, że obowiązkiem Wykonawcy jest opisanie środków ochrony informacji, którymi dysponuje lub które może / powinien wdrożyć Zamawiający w ramach przygotowanej dokumentacji.
- Dokumentacja jest przygotowana poprzez użycie funkcji automatyzujących formatowanie (punktatory, listy, formatowania i inne) w formacie DOCX.
- Istnieje możliwość demonstracji pełnego pokrycia przygotowanej dokumentacji na zgodność z ISO 2700X.

9.5. W zakresie szkoleń

- Wszyscy użytkownicy zostali przeszkoleni w zakresie opisanym w niniejszym zamówieniu.
- Wszyscy użytkownicy zdali testy wiedzy potwierdzające nabycie umiejętności w wybranym zakresie.
- Wszyscy użytkownicy posiadają dostęp do szkoleń e-Learning.

9.6. W zakresie testów penetracyjnych

- Testy zostały wykonane w oparciu o metodykę PTES albo OSSTMM.
- Testy zostały wykonane przez osoby posiadające kwalifikacje opisane w zamówieniu.
- Dla wszystkich testów zostały opracowane raporty.
- Wykonano retesty potwierdzające usunięcie zgłoszonych podatności/ryzyk.

9.7. W zakresie testów socjotechnicznych

- Przeprowadzono testy zgodnie z harmonogramem: przed i po szkoleniach użytkowników z obszaru phishingu.
- Przygotowano i wykonano scenariusze testów zgodnie z wymaganiami Zamawiającego.
- Testy zostały wykonane przez osoby posiadające kwalifikacje opisane w zamówieniu.
- Dla wszystkich testów zostały opracowane raporty.