**Załącznik nr 1 do SIWZ**

**Opis Przedmiotu Zamówienia**

**Gmina Pokrzywnica**

Spis treści

[1.1 Termin i Harmonogram Wykonania Zamówienia 2](#_Toc509216724)

[1.1.1 Przepisy prawa i Normy 3](#_Toc509216725)

[2 Audyt ochrony danych osobowych wraz z bezpieczeństwem teleinformatycznym 4](#_Toc509216726)

[2.1 Przedmiot usługi: 4](#_Toc509216727)

[2.2 Audyt organizacyjny 5](#_Toc509216728)

[2.3 Audyt fizyczny, teleinformatyczny i środowiskowy 6](#_Toc509216729)

[2.4 Wykonanie i przekazanie Raportów z Audytu, dokumentacji: 11](#_Toc509216730)

[2.5 Szkolenia 12](#_Toc509216731)

[2.6 Pozostałe informacje. 13](#_Toc509216732)

## Termin i Harmonogram Wykonania Zamówienia

Przedmiot umowy musi być zrealizowany zgodnie z Harmonogramem w nieprzekraczalnym terminie **do dnia 31.01.2019 r**.

Tabela 1. Harmonogram realizacji poszczególnych etapów realizacji zamówienia:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa zadania** | **Termin realizacji** |
| Etap I | Podstawowa dokumentacja do wdrożenia RODO między innymi analiza ryzyka, rejestr czynności, zaktualizowana dokumentacja. | **25 maja 2018** |
| Etap II | Zakończenie audytu, aktualizowana dokumentacja, analiza | **31 stycznia 2019** |

Przedmiot umowy będzie realizowany zgodnie z zatwierdzonym przez Zamawiającego Harmonogramem rzeczowo-finansowym. Wykonawca zobowiązany jest przedłożyć Zamawiającemu do zatwierdzenia Harmonogram rzeczowo-finansowy dla wszystkich Zadań w terminie 5 dni kalendarzowych od dnia podpisania umowy. Zamawiający zatwierdzi Harmonogram rzeczowo-finansowy w ciągu 3 dni roboczych od daty jego przedłożenia do zatwierdzenia. Na wniosek każdej ze stron po uzyskaniu wzajemnej akceptacji Harmonogram rzeczowo-finansowy może ulec zmianie pod warunkiem, że terminy końcowe realizacji poszczególnych elementów przedmiotu zamówienia przedstawione w Tabeli 1 – Harmonogram realizacji Etapów Projektu nie ulegną zmianie.

## Przepisy prawa i Normy

1. USTAWA z dnia 6 września 2001 r. o dostępie do informacji publicznej (tj. Dz.U.2016.1764)
2. ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (tj. Dz.U.2007.10.68)
3. USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U.2016.922 z póź zm.
4. ROZPORZĄDZENIE MINISTRA ADMINISTRACJI I CYFRYZACJI z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji Dz.U.2015.745
5. ROZPORZĄDZENIE MINISTRA ADMINISTRACJI I CYFRYZACJI z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych Dz.U.2015.719
6. ROZPORZĄDZENIE MINISTRA ADMINISTRACJI I CYFRYZACJI z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji Dz.U.2014.1934
7. ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych Dz.U.2004.100.1024
8. ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U.2016.1744
9. USTAWA z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz.U.2017.570
10. Dobre praktyki dla administracji publicznej zakresie ochrony danych osobowych jak i informatyzacji. Oraz wytyczne grupy 29
11. Normy: ISO/ICE 27000; ISO/ICE 27001; ISO/ICE 27002; ISO/ICE 27005; ISO/IEC 20000 — zarządzanie usługami IT; ISO/IEC 27017 Kodeks najlepszych praktyk w zakresie zabezpieczeń dla usług w chmurze obliczeniowej; ISO/IEC 27018 Ochrona Danych Osobowych w Chmurze Dbaj o bezpieczeństwo informacji w cyberprzestrzeni; ISO 22301 Zarządzanie Ciągłością Działania; Zarządzanie Ryzykiem ISO 31000; ISO/IEC 19770, Norma PN-ISO/IEC 17799
12. Inne niezbędne przepisy mające wpływ na ochronę informacji i informatyzację administracji publicznej, inwentaryzację sprzętu oprogramowania, ochrona praw autorskich itp.
13. Przedmiot zamówienia musi być zgodny z obowiązującymi przepisami prawa w zakresie Portalów informatycznych wykorzystywanych przez jednostki publiczne, w tym między innymi spełniać wymagania następujących aktów prawnych: Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz. U. 1997, Nr 78 poz. 483 z późn. zm.);
14. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2014, poz. 1182 z późn. zm.);
15. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz.U. L 119 z 4.5.2016
16. Przyszłościowo wydane akty wykonawcze wydane do RODO – nowa ustawa o ochronie danych, rozporządzenia itp.
17. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. 2006, Nr 90, poz. 631 z późn. zm.);
18. Ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (Dz. U. 2011, Nr 123, poz. 698);
19. Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących działania publiczne (Dz. U. z 2014 r. poz. 1114);
20. Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 roku w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz. U. 2005, Nr 217, poz. 1836);
21. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 roku w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006, Nr 206, poz. 1517);
22. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2015 r. poz. 971).
23. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i Portale informatyczne służące do przetwarzania danych osobowych (dz. u. z 2004 r. nr 100, poz. 1024)
24. Ustawa o ochronie baz danych z 27 lipca 2001 roku (Dz. U. z 2001 roku, Nr 128, poz.1402, z 2004 r. Nr 96, poz. 959, z 2007 r. Nr 99, poz. 662, Nr 176, poz. 1238.);
25. Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 z późn. zm.)
26. Inne niezbędne przepisy mające wpływ na ochronę informacji i informatyzację administracji publicznej, inwentaryzację sprzętu oprogramowania, ochrona praw autorskich oraz wszelkie zmiany obecnych przepisów, akty zastępujące itp. obecnie obowiązujące oraz pojawiające się w trakcie realizacji projektu.

# Audyt ochrony danych osobowych wraz z bezpieczeństwem teleinformatycznym

## Przedmiot usługi:

1. 8 jednostek – Urząd, Biblioteka, Ośrodek Pomocy, Przedszkole, PSP Pobyłkowo Duże, PSP Gzowo, PSP Nowe Niestępowo, PG Dzierżenin oraz 4 Świetlice Wiejskie w Pokrzywnicy, Dzierżeninie, Gzowie, Pobyłkowie Dużym – wszystkie jednostki posiadają połączenia VPN z siecią Urzędu (jedna sieć LAN, każda jednostka posiada swój zakres adresów IP)
2. Świetlice wiejskie tylko pod względem połączeń bezpieczeństwa połączeń VPN z Urzędem i bezpieczeństwa urządzeń UTM, ochrony sprzętu
3. Liczba pracowników około 150
4. Dokładny harmonogram i plan audytu zostanie ustalony w wykonawcą.
5. Sprzęt: (ilość sprzętu może ulec zmianie podczas realizacji projektu)

a) Serwery fizyczne 9 szt., wirtualne około 14 szt., serwery geodety 2 szt.;

b) Komputery około 400 szt. w tym około 250 w pracowniach informatycznych, NAS (Network Attached Storage) - 1 szt.

c) Drukarki – 70 szt.

d) Urządzenie sieciowe: switch zarządzane – 10 szt., UTM - 10 szt., itp. – około 20 szt.

## Audyt organizacyjny

1. Wytworzenie regulacji wraz z ich wdrożeniem w obszarze zarządzania bezpieczeństwem informacji;
2. Odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
3. Sprawdzenie i aktualizacja dokumentacji bezpieczeństwa informacji w tym danych osobowych zgodnie z wymaganiami KRI oraz jej aktualizacja
4. Szkolenie i wsparcie w przeprowadzaniu analizy ryzyk i stworzenie stosownej dokumentacji do dokonywania dalszych analiz – zgodnie z normami 2700x oraz RODO;
5. KRI, które powinny spełniać systemy IT: utrzymania / zarządzania systemami IT (spełnić wymagania norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2), wymiany danych z innymi systemami i kodowania znaków, dostosowania systemów do standardów WCAG2.0 (kwestia większej dostępności dla osób niepełnosprawnych), wymagania dotyczące bezpieczeństwa, które dominują nad innymi wymaganiami z tego rozdziału.
6. Weryfikacja umów powierzenia, sprawdzenie zawartych oraz analiza, czy nie trzeba zawrzeć innych
7. Analiza formalno-prawna procesów i zbiorów, w których przetwarzane są dane osobowe, prowadzonych w sposób tradycyjny oraz z wykorzystaniem systemów informatycznych pod kątem wymagań Ustawy o Ochronie Danych Osobowych oraz RODO; Przegląd istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania informacji
8. Dokonanie oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji z obowiązującymi aktami prawnymi w szczególności: między innymi § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; wymaganiami technologicznymi w systemach informatycznych zapewniającymi bezpieczeństwo zasobów sprzętowych i informacyjnych.
9. Rozpoznanie wszystkich obszarów przetwarzania danych i ich granic SZBI i ODO.
10. Rozpoznanie wszystkich przetwarzanych zbiorów danych, procesów i danych.
11. Rozpoznanie wszystkich systemów przetwarzających dane i ich konfiguracji, upoważnienia.
12. Przeprowadzenie analizy ochrony punktów krytycznych w obszarach przetwarzania danych.
13. Przeprowadzenie testów socjotechnicznych, w celu ustalenia poziomu świadomości pracowników Zamawiającego z zakresu możliwości utraty informacji, sprzętu na skutek manipulacji i/lub celowego, złośliwego działania osób trzecich. Ze względu na wiarygodność i wrażliwość tego testu jego szczegóły zostaną uzgodnione bezpośrednio między Wykonawcą a upoważnionym przedstawicielem Zamawiającego tuż przed jego wykonaniem. Zamawiający rezerwuje sobie prawo do niewyrażenia zgody na proponowane przez Wykonawcę, w ramach testu, działania oraz do wskazania obszaru i rodzaju działania, który będzie objęty proponowanym przez Wykonawcę testem. Wynik testu nie będzie miał żadnego wpływu na politykę kadrową Zamawiającego. Testy w fizycznej lokalizacji zamawiającego za pośrednictwem telefonu, poczty elektronicznej. Sporządzenie raportu wraz z zaleceniami naprawczymi.
14. Przeprowadzenie analizy wytycznych w zakresie dostępu osób upoważnionych do przetwarzania danych osobowych
15. Przeprowadzenie analizy możliwości dostępu fizycznego do danych przez osoby nieupoważnione.
16. Weryfikacja dokumentów wewnętrznych Zamawiającego regulujących przetwarzanie danych osobowych.
17. Weryfikacja ewidencji osób upoważnionych do przetwarzania danych osobowych.
18. Weryfikacja pracy użytkowników w obszarach, w których przetwarzane są dane osobowe.
19. Weryfikacja sposobu przetwarzania danych osobowych.
20. Weryfikacja kontroli nad przepływem danych osobowych.
21. Weryfikacja przechowywania danych osobowych.
22. Weryfikacja poufności, integralności, dostępności, rozliczalności danych osobowych.
23. Weryfikacja procesu udostępniania danych osobowych
24. Identyfikacja zagrożeń, słabych stron związanych z przetwarzania danych osobowych.
25. Weryfikacja dostępu osób nieupoważnionych do miejsc, gdzie przetwarzane są dane osobowe.
26. Weryfikacja poprawności magazynowania i bieżącej pracy z dokumentacją papierową
27. Sprawdzenie ustalonych zasad bezpieczeństwa pod względem zgodności z obowiązującymi aktami prawnymi.
28. Analiza posiadanej przez Zamawiającego dokumentacji związanej z przetwarzaniem danych w systemach informatycznych.
29. Sprawdzenie czytelności podziału zadań i obowiązków pracowników IT. Sprawdzenie struktury organizacyjnej pod względem IOD.
30. Sprawdzenie zapewnienia niezbędnych szkoleń w zakresie ochrony i bezpieczeństwa danych przetwarzanych w systemach informatycznych dla pracowników.
31. Weryfikacja zgodności nadawania uprawnień do pracy w systemach informatycznych z obowiązującymi procedurami, jeśli procedury nie istnieją bądź są niepełne to ich ustanowienie bądź uzupełnienie.
32. Ocena monitorowania incydentów i problemów w zakresie bezpieczeństwa IT i ochrony danych.
33. Adekwatność i aktualność procedur i instrukcji w zakresie kopii zapasowych.
34. Weryfikacja i ocena procedur i instrukcji w zakresie zapewnienia ciągłości działania systemów informatycznych.
35. Kontrola wewnętrzna przetwarzania danych osobowych,
36. omówienie technik przeprowadzania kontroli systemów informatycznych przez ABI.
37. Zasady dotyczące raportowania stanu bezpieczeństwa.

## Audyt fizyczny, teleinformatyczny i środowiskowy

1. Weryfikacja granic obszaru bezpiecznego;
2. Weryfikacja zabezpieczeń wejścia/wyjścia, polityka kluczy, klucze zapasowe, alarmy i inne zabezpieczenia
3. Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń:
4. Weryfikacja bezpieczeństwa okablowania strukturalnego;
5. Weryfikacja systemów chłodzenia serwerowni;
6. Weryfikacja systemów alarmowych -dostęp, czujki, kody.
7. Ocena zabezpieczeń ochrony i zabezpieczenia danych osobowych (ochrona na poziomie sprzętu i oprogramowania komputerowego oraz infrastruktury przegląd stacji roboczych, serwerów, urządzeń sieciowych (procesy, autoryzacja, zabezpieczenia, analiza systemu zarządzania kopiami zapasowymi, konfiguracja systemu),
8. przegląd konfiguracji oprogramowania, sieci LAN
9. weryfikacja konfiguracji serwerów, zabezpieczeń UTM, stacji, urządzeń sieciowych -wdrożenie działań naprawczych
10. Przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania ciągłości działania;
11. Weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed między innymi możliwością nieautoryzowanych instalacji oprogramowania;
12. Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
13. Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
14. Weryfikacja stosowanych metod kasowanie danych z nośników magnetycznych przeznaczonych do utylizacji - procedury.
15. Inwentaryzacja sprzętu działającego w infrastrukturze informatycznej.
16. Inwentaryzacja usług sieciowych z opisem wzajemnych zależności tych usług oraz wykorzystywanych portów.
17. Inwentaryzacja baz danych ze wskazaniem aplikacji korzystających z tych baz.
18. Inwentaryzacja używanych aplikacji.
19. Zarządzanie aplikacjami (wykaz licencji i aplikacji, zasady dostępu do aplikacji. monitorowanie instalacji oprogramowania oraz osoby nadzorujące).
20. zapewnienia ochrony przed nieautoryzowanym dostępem fizycznym do obiektów lub pomieszczeń zajmowanych przez komórki organizacyjne Zamawiającego, w których są eksploatowane (użytkowane) urządzenia i sprzęt wchodzące w skład systemów i sieci informatycznych Zamawiającego;
21. zapewnienia ochrony przed zdarzeniami i incydentami mogącymi spowodować uszkodzenia lub zakłócenia w prawidłowym funkcjonowaniu systemów i sieci informatycznych;
22. wyznaczenia granic obszarów bezpiecznych dla funkcjonujących systemów i sieci informatycznych oraz wskazanie procedur i mechanizmów kontrolnych zabezpieczających wejścia do tych obszarów.
23. dokonanie identyfikacji zdarzeń, które mogłyby zagrozić bezpieczeństwu informacji przetwarzanych u Zamawiającego oraz ocenę ryzyk związanych z tymi zdarzeniami,
24. Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej
25. Testy styku sieci lokalnej z internetem przeprowadzane ze stacji roboczej podłączonej do sieci internet;
26. Analiza topologii brzegu sieci;
27. Weryfikacja mechanizmów ochronnych;
28. Próba wykrycia usług sieciowych udostępnianych do internetu;
29. Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet;
30. Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci internet;
31. Przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią internet oraz połączeń VPN.
32. Analiza topologi sieci LAN;
33. Weryfikacja mechanizmów ochronnych w sieci;
34. Analiza komunikacji sieciowej;
35. Skanowanie portów TCP/UDP próba wykrycia usług sieciowych;
36. Skanowanie hostów aktywnych w sieci oraz przez VPN;
37. Exploitacja dostępnych urządzeń oraz usług w sieci LAN;
38. Przedstawienie rozwiązań zwiększających bezpieczeństwo w sieci LAN.
39. Kontrola zabezpieczeń obszaru przetwarzania danych osobowych.
40. Kontrola zabezpieczeń pomieszczeń.
41. Kontrola zabezpieczeń zbiorów tradycyjnych.
42. Kontrola zabezpieczeń zbiorów archiwalnych. Dostęp, rejestr itp.
43. Kontrola ochrony przed zdarzeniami losowymi.
44. Kontrola bezpieczeństwa okablowania strukturalnego.
45. Kontrola systemów wspomagających.
46. Kontrola ochrony sprzętu przed kradzieżą.
47. Kontrola działania sytemu monitoringu.
48. Kontrola działania systemu alarmowego.
49. Kontrola działania polityki czystego biurka i czystego ekranu.
50. Audyt stron www i BIP pod względem bezpieczeństwa.
51. Audyt wifi:
    1. Określenie szczelności sieci bezprzewodowej.
    2. Określenie aktualnie stosowanych mechanizmów kryptograficznych zapewniających ochronę w warstwie sieciowej.
    3. Określenie odporności sieci bezprzewodowej na ataki.
    4. Określenie skalowalności sieci pod względem bezpieczeństwa przy wzroście aktywnych klientów (w zakresie bezpieczeństwa i dystrybucji dostępu).
    5. Wykrycie sieci bezprzewodowych (802.11.xx) w kilku wybranych miejscach.
    6. Określenie skalowalności przyjętych rozwiązań (m.in. w zakresie wykorzystania rozwiązań klasy WPA Enterprise)
    7. Określenie typu zabezpieczeń wykrytych sieci (Open System, WEP, WPA, WPA2).
    8. W przypadku wykrycia sieci klasy Open - próba podłączenia się do Access point.
    9. W przypadku wykrycia sieci z zabezpieczeniami - próba złamania klucza szyfrującego i uzyskania dostępu do sieci.
    10. Weryfikacja trybu ogłaszania SSID oraz wartości SSID.
    11. Próba wykrycia producenta urządzenia Access Point.
    12. Określenie wykorzystanych mechanizmów uwierzytelniania stron (na podstawie przekazanych przez Klienta danych dostępowych).
    13. Sprawdzenie wykorzystania mechanizmów uwierzytelniania oferowanych przez standard 802.11.xx
    14. Weryfikacja wykorzystanej klasy protokołu EAP (LEAP, EAP-TLS, PEAP, itd.).
52. Audyt VPN
    1. Zbadanie poziomu bezpieczeństwa ofertowanego przez system klasy VPN.
    2. Weryfikacja możliwości użycia systemów klasy VPN jako punkt pośredni ataku na infrastrukturę IT.
    3. Określenie realnego zabezpieczenia komunikacji sieciowej oferowanej przez wdrożoną u Zamawiającego implementację VPN.
    4. Próba wykrycia aktywności serwera VPN.
    5. Próba wykrycia rodzaju wykorzystywanego rozwiązania VPN (dostawcy sprzętu, protokół).
    6. Próby inicjowania tunelu z różnymi algorytmami kryptograficznymi (szyfry symetryczne, funkcje skrótu, metoda uwierzytelniania, grupa DH).
    7. Skanowanie portów oraz podatności na koncentratorze VPN.
    8. Weryfikacja wykorzystanych trybów połączenia (transport, tunnel, ESP, AH).
    9. Weryfikacja przyjętych metod uwierzytelniania (np. PKI, hasła jednorazowe).
    10. Weryfikacja przyjętych polityk bezpieczeństwa dla urządzeń klienckich korzystających z VPN (pod względem możliwości ataku na infrastrukturę VPN - inicjowanych z urządzeń klienckich).
53. Urządzenia sieciowe
    1. Zbadanie odporności urządzeń na ataki z poziomu Internetu oraz z wewnątrz sieci czynnik ludzki.
    2. Wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności
    3. Wskazanie potencjalnych, dodatkowych metod ochrony sieci.
    4. Analiza podatności na ataki
    5. Skanowanie portów TCP / UDP (kilka typów - prostych oraz zaawansowanych).
    6. Skanowanie hostów aktywnych w danej podsieci także przez VPN
    7. Określenie ścieżki sieciowej do urządzenia (wykorzystanie traceroute).
    8. Próba detekcji typu oraz wersji usług sieciowych działających w systemie.
    9. Próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu.
    10. Po udanej detekcji wersji oprogramowania systemowego / usług - próba lokalizacji znanych podatności w danych wersjach oprogramowania.
    11. Próba komunikacji w obrębie protokołu ICMP (kilka wybranych parametrów type/code).
    12. Próba generacji pakietów o dużym rozmiarze (np. powiększonych pakietów ICMP echo).
54. Audyt LAN
    1. Wskazanie miejsc, które mogą być bezpośrednio zaatakowane w LAN (włamania do wewnętrznych systemów).
    2. Oszacowanie jakości obecnie stosowanych zabezpieczeń w warstwie sieciowej (w tym odporność na ataki techniczne komponentów sieciowych).
    3. Weryfikacja skuteczności procedur zarządzania hasłami (odporność na częste ataki związane z wykorzystaniem domyślnych haseł administracyjnych do urządzeń/usług sieciowych).
    4. Wskazanie ewentualnych dodatkowych metod ochrony.
    5. Wskazanie sposobu naprawy znalezionych luk
    6. Weryfikacja podziału LAN na strefy sieciowe (w tym wykorzystanie firewalli oraz VLAN) – zalecenia konfiguracyjne
    7. Określenie usług działających w LAN
    8. Manualne próby uzyskania dostępu do urządzeń za pomocą domyślnych haseł administracyjnych (przełączniki / serwery )
    9. Sprawdzenie podatności na domyślne hasła producenta oprogramowania w kilku wybranych systemach (przykładowo: detekcja nieaktualnego oprogramowania, możliwość dostępu do wybranych usług z domyślnym hasłem / bez hasła).
    10. Weryfikacja dostępnych mechanizmów uwierzytelniania dostępnych w sieci.
    11. Weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI.
    12. Weryfikacja kilku podstawowych zasad bezpieczeństwa na wybranych 20% stacjach roboczych w danej jednostce (udostępnione usługi, poziom dostępu zapewniany dla użytkowników, dostępność oprogramowania klasy antywirus/antymalware sposoby aktualizacji systemu, itp.)
    13. Weryfikacja dostępu do Internetu z LAN, m. In. pod kątem bezpieczeństwa
    14. Wskazanie potencjalnych, dodatkowych metod ochrony sieci.
55. Identyfikacja tzw. „wąskiego gardła” pojedynczych punktów awarii w infrastrukturze IT
56. Audyt styku z siecią Internet – router brzegowy (między innymi firewall):
57. audyt systemu operacyjnego;
58. Powyższe testy zostaną uzupełnione o testy penetracyjne prowadzone z sieci Internet – zbadanie odporności systemu zabezpieczeń, a także sprawdzenie systemów pod względem wydajności, niezawodności, zgodności z dobrymi praktykami dotyczącymi zasad separacji i kontroli dostępu
59. Weryfikacja w zakresach:
60. Polityki kontroli dostępu do systemów.
61. Zasady odpowiedzialności użytkowników.
62. Procedury dostępu do systemów operacyjnych.
63. Procedury dostępu i kontroli do usług internetowych.
64. Procedury użytkowania Internetu w ramach SZBI
65. Procedury rejestracji błędów.
66. Kontrola postępowania z urządzeniami przenośnymi w szczególności tymi, na których przetwarzane są dane osobowe.
67. Kontrola wytycznych związanych z użytkowaniem sprzętu poza siedzibą.
68. Bezpieczne przekazywanie sprzętu.
69. Analiza procedur backupu (sposób wykonywania kopii bezpieczeństwa, zakres kopiowanych danych, przechowywanie kopii bezpieczeństwa), oraz procesu administracji.
70. Identyfikację podatności systemów i sieci na ataki typu: DoS, DDoS, Sniffing, Spoffing, XSS, Hijacking, Backdoor, Flooding, Password, Guessing i inne.
71. W szczególności w ramach audytu przeskanowane zostaną aktywne urządzenia sieci komputerowej, w tym routery, zapory (firewall), przełączniki, serwery i stacje robocze na występowanie luk/podatności w tych urządzeniach oraz błędów w konfiguracji zmniejszających poziom bezpieczeństwa systemów, zgodnie z następującymi wytycznymi:
72. W pierwszym kroku zostanie sporządzona mapa aktywnych urządzeń sieci zarówno w postaci graficznej jak i listy adresów IP, z przypisanymi do nich systemami operacyjnymi urządzeń.
73. Spośród listy urządzeń aktywnych audytor wyselekcjonuje najważniejsze urządzenia z punktu widzenia bezpieczeństwa całej sieci, które zostaną poddane szczegółowej analizie podatności.
74. Wykryte zostaną podatności i błędy w konfiguracji systemów będących w posiadaniu urzędu, z uwzględnieniem poziomu ważności ze względu na bezpieczeństwo.
75. W celu wykrycia luk w systemach, nie będą przeprowadzane ataki destrukcyjne, które zakłócą pracę systemów.
76. Wykonane zostanie skanowanie z autentykacją w celu potwierdzenia podatności systemu operacyjnego oraz oprogramowania pakietów biurowych i systemu poczty elektronicznej.
77. W procesie skanowania luk wykorzystywane będą najnowsze bazy podatności publikowane w serwisach CVE, Bagtraq oraz producentów sprzętu i systemów operacyjnych.
78. Skanowanie podatności na komputerach i serwerach powinno się odbyć bez instalacji jakiegokolwiek oprogramowania na urządzeniach badanych.
79. Po przeskanowaniu sieci zostaną sporządzone szczegółowe raporty dotyczące wykrytych podatności.
80. Do wszystkich wykrytych podatności lub błędnych konfiguracji zostanie przygotowana lista poprawek do zainstalowania lub instrukcje w jaki sposób je wyeliminować.
81. Lista poprawek lub instrukcji będzie sporządzona w postaci przejrzystego raportu, w którym urządzenia będą podzielone na grupy zasobów, w zależności od: lokalizacji, przynależności do komórki organizacyjnej lub rodzaju systemu operacyjnego.
82. Zostanie przygotowany raport poprawek, które należy zaaplikować do poszczególnych systemów, z linkami do stron producentów w celu ich pobrania oraz informacją, kiedy dana poprawka powstała; dla każdej z poprawek wylistowane zostaną podatności, które powinny być załatane po jej aplikacji.
83. Zostanie przygotowana lista urządzeń posiadających przestarzałe oprogramowanie z linkami do stron producentów.
84. Dla wybranych serwerów i stacji roboczych, zostanie zweryfikowana zgodność na poziomie technologicznym konfiguracji systemów operacyjnych z wytycznymi wynikającymi z polityki bezpieczeństwa.
85. Dla poszczególnych grup badanych urządzeń zostanie przeprowadzona ocena ryzyka systemów IT na poziomie technologicznym w ramach przeprowadzonej oceny ryzyka SZBI.
86. Dla publicznych adresów IP po skanowaniu audytowym odbędą się jeszcze 3 skanowania kontrolne w odstępie 3 miesięcy, a po ich wykonaniu zostanie sporządzony raport trendu podatności i poziomu ryzyka systemów.
87. Infokioski powinny te być objęte testami i badaniem bezpieczeństwa.
88. Badanie AD i DNS poprawność konfiguracji serwera i synchronizacji klientów.
89. Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi:
90. Sprawdzenie serwisów internetowych wszystkie w domenie pokrzywnica.pl lub udostępnione z poniższych zakresów adresów IP 79.187.204.207 -214, 94.246.181.146; 194.181.20.5; 46.171.5.125; 94.246.181.142; 94.246.181.144; 194.181.20.9; 194.181.20.10; 194.181.20.11; 83.3.152.122; 94.246.181.145; pokrzywnica.eboi.pl i ESP innych jednostek, pokrzywnica.wliczbach.pl, pokrzywnica.ankietaoceny.eu; portale geodety udostępnione w Projekcie EA
91. Inwentaryzacja wszystkich usług, aplikacji ich sprawdzenie niezbędne do dokumentacji i późniejszym nadawaniu uprawnień.
92. testami penetracyjnymi ma być objęta infrastruktura, systemy użytkowane przez Zamawiającego np. systemy użytkowe, biurowe, poczta elektroniczna, dedykowane
93. Opis zakresu przeprowadzonych prac audytowych.
94. Analizę informacji zebranych podczas audytów.
95. Wnioski i zalecenia audytora.
96. Ocenę poziomu bezpieczeństwa danych osobowych i systemu informatycznego.
97. Analizę wyników testów penetracyjnych pod kątem oceny zagrożenia integralności systemu oraz możliwości dostępu do danych przez osoby nieupoważnione.
98. Zalecenia w przypadku wymiany infrastruktury sprzętowej oraz systemów operacyjnych na okres 5 lat od dnia wykonania audytu.
99. Poprawności doboru topologii sieci.
100. Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych.
101. Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego zdalnego (przez WWW) dostępu do paneli administracyjnych.
102. Weryfikacja poprawności aktualizacji zabezpieczeń antywirusowych.
103. Weryfikacja zasilania awaryjnego
104. Sprawdzenie wyposażenia i zabezpieczenia pomieszczeń serwerowni.
105. Dokumentowanie konfiguracji systemów służących przetwarzaniu danych osobowych.
106. Zasady zarządzania oprogramowaniem.
107. Zapewnienie bezpieczeństwa danych przy dokonywaniu napraw sprzętu i oprogramowania.
108. Wyznaczenie osób uprawnionych do dokonywania napraw sprzętu i oprogramowania.

## Wykonanie i przekazanie Raportów z Audytu, dokumentacji:

1. Audyt winien być zakończony opracowaniem i przekazaniem raportu o stosownym poziomie poufności wraz z projektami niezbędnej zaktualizowanej dokumentacji dla każdej jednostki z ochrony danych osobowych, zaś ze względu na połączenia i powiazania między jednostkami dokumentacja SZABI będzie stworzona jedna dla wszystkich jednostek.
2. Opracowanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji do zaimplementowania u zamawiającego wg aktualnego stanu prawnego oraz wymagań normy PN ISO/IEC 27001:2014-12: Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym wraz ze wszystkimi niezbędnymi procedurami uzupełniającymi oraz analizą ryzyka. Opracowana dokumentacja ma zapewnić możliwość zaimplementowania zmian określonych w Rozporządzeniu ogólnym o ochronie danych osobowych /RODO/, KRI
3. stopnia spełnienia wymogów wymienionych w § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
4. spełnienia skuteczności stosowanych zabezpieczeń;
5. wskazanie obszarów wymagających doskonalenia;
6. określenie zakresu i priorytetu działań naprawczych dla wszystkich wykrytych uchybień we wszystkich aspektach jednostek.
7. Wszystkie dokumenty związane z przeprowadzonym audytem Wykonawca dostarczy Zamawiającemu w postaci wydruku i w postaci elektronicznej. Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował jako poufne i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego, z wyłączeniem organów występujących o to z mocy prawa po uprzednim powiadomieniu o tym wystąpieniu Zamawiającego.
8. Sporządzeniem przez Wykonawcę raportu pokontrolnego zawierającego: Opis aktualnego stanu bezpieczeństwa danych, ze szczególnym uwzględnieniem danych osobowych. Wskazanie stwierdzonych uchybień i zagrożeń. Zalecenia i opisy dotyczących sposobów, metod i środków usunięcia stwierdzonych uchybień i zagrożeń związanych z bezpieczeństwem przetwarzania danych, ze szczególnym uwzględnieniem danych osobowych, dla osiągnięcia zgodności z wymienionymi wyżej aktami prawnymi i dokumentami.
9. Opracować harmonogram projektu wdrożenia SZBI
10. Sporządzić dokument opisujący podejście do szacowania ryzyka w i przeprowadzić badanie szacowania ryzyka w instytucji czego wynikiem będzie raport z szacowania ryzyka przetwarzania informacji oraz plan postępowania z ryzykiem.
11. Sporządzić dokument opisujący strukturę organizacyjną zarządzania bezpieczeństwem informacji w wraz z określeniem ról i zakresów odpowiedzialności osób.
12. Zapisy odnośnie dokumentacji nie dotyczą Świetlic Wiejskich.
13. Dokument Proces zarządzania bezpieczeństwem powinien zawierać:
14. Opis celów i zakresu procesu zarządzania bezpieczeństwem
15. Opis ról niezbędnych do procesu zarządzania bezpieczeństwem
16. Opis przebiegu zarządzania bezpieczeństwem
17. Definicję polityki i zasad dla procesu zarządzania bezpieczeństwem
18. Definicję mierników skuteczności i efektywności procesu zarządzania bezpieczeństwem
19. Szczegółowe procedury funkcjonowania procesu zarządzania bezpieczeństwem
20. Dokument standardy bezpieczeństwa informacji powinien zawierać uzupełnienie wymagań, zaleceń i wytycznych dokumentu zasad bezpieczeństwa informacji. Dlatego powinny zostać opracowane standardy tj. Stacji roboczych i serwerów, Urządzeń sieciowych, Kryptograficznej ochrony informacji, Aplikacji infrastruktury, Autoryzacji i uwierzytelniania, Kasowania danych z nośników, Środowiska wirtualnego, Bezprzewodowej sieci WiFi, Polityki systemu DLP
21. Dokumenty procedur bezpieczeństwa powinny dotyczyć Obsługi incydentów bezpieczeństwa, Nadzoru nad dokumentami Systemu Zarządzania Informacją, Oceny skuteczności zabezpieczeń, Działań korygujących, Audytu wewnętrznego, Zarządzania zmianami
22. Wykonawca sporządzi sprawozdanie audytowe, które będzie zawierać: Szczegółowy opis i ocenę stanu wszystkich obszarów podlegających audytowi. Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń (prawdopodobieństwo wystąpienia i mechanizm zminimalizowania/eliminacji skutków). Zobrazowanie połączeń logicznych, sieci lokalnej oraz styku sieci lokalnej z siecią Internet, z uwzględnieniem wszystkich urządzeń ich adresacji i działających usług, używanych portów i protokołów. Szczegółową, elektroniczną inwentaryzację sprzętu i oprogramowania działającego w infrastrukturze informatycznej Zamawiającego. Zalecenia dotyczące sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyk. Lista poprawek do zainstalowania oraz szczegółowy opis zalecanych zmian konfiguracji. Przygotowaną przez Wykonawcę listę proponowanych nowelizacji wewnętrznych regulacji Zamawiającego w zakresie przetwarzania danych w systemach informatycznych dotyczących elementów tej dokumentacji, gdzie zdiagnozowano potrzebę nowelizacji, w szczególności: Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym. Propozycje te Wykonawca przygotuje w porozumieniu z Zamawiającym, uwzględniając specyfikę działania i organizację pracy Zamawiającego. Wykonawca nie jest zobowiązany do przygotowania nowych kompletnych tekstów jednolitych regulacji wewnętrznych Zamawiającego ww. zakresie.
23. Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował jako poufne i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego

**Zapewnienie opieki doradczej po zakończeniu audytu** – między innymi konsultacje, zapytania itp. zamawiającego z wykonawcą zaleceń zawartych w raportach przez okres 4 miesięcy od daty podpisania protokołu odbiorczego.

## Szkolenia

1. Po zakończeniu audytów Wykonawca przeprowadzi szkolenie dla pracowników zakończone dokumentem potwierdzającym wiedzę dotyczącą zagrożeń przy przetwarzaniu danych osobowych i informacji. Tematyka szkolenia musi omawiać przynajmniej niżej wymienione zagadnienia (Możliwość stworzenia szkolenia e-lerningowego obejmującego poniższe zagadnienia oraz KIR i zakresu bezpieczeństwa pracy w systemach teleinformatycznych na platformie Zamawiającego wraz z testem po szkoleniu i automatycznym wydaniem certyfikatów – przekazanie pełni praw autorskich do szkolenia) ):
2. Czym są dane osobowe.
3. Zagrożenia bezpieczeństwa danych osobowych.
4. Możliwości e-kradzieży danych.
5. Sposoby wyłudzenia informacji.
6. Sposoby wycieku informacji.
7. Utrata danych na skutek sytuacji losowych.
8. Sposoby utraty poufności, dostępności i integralności danych.
9. Zasady stosowania zabezpieczeń ochrony fizycznej.
10. Zasady korzystania z bezpiecznego hasła.
11. Zasady bezpiecznego użytkowania komputera.
12. Zasady czystego ekranu i czystego biurka.
13. Zasady bezpiecznego transportu informacji.
14. Zasady obiegu informacji w organizacji.
15. Odpowiedzialność karna, cywilna i administracyjna przy przetwarzaniu danych osobowych.
16. Zagadnienia z nowo wprowadzonej polityki bezpieczeństwa informacji.
17. Przeprowadzić szkolenie z zakresu bezpieczeństwa informacji dotyczące zarządzania systemów bezpieczeństwa informacji oraz zarządzania ryzykiem dla wybranych pracowników do 10 osób.
18. Szkolenie przygotowujące do roli audytora wewnętrznego w zakresie bezpieczeństwa informacji dal 1 osoby

## Pozostałe informacje.

Wykonawca przed przystąpieniem do realizacji audytu jest zobowiązany do podpisania klauzuli poufności i jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych.

Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań audytowych i jest bezterminowe.

KLAUZULA POUFNOŚCI

w związku z realizacją zamówienia na „…………………….”

Ja, niżej podpisany(a):

………………………………………..(imię i nazwisko), legitymujący się dowodem osobistym nr ……………………… jako upoważniony przedstawiciel Wykonawcy …………………………………….. z siedzibą w ………………………………. wraz ze wszystkimi osobami uczestniczącymi w realizacji przedmiotowego zamówienia po stronie Wykonawcy zobowiązuję się do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych.

Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań audytowych i jest bezterminowe.