**Szczegółowy opis przedmiotu zamówienia**

Celem projektu jest przeprowadzenie audytu z zakresu bezpieczeństwa infrastruktury sieciowej, stanu zarządzania bezpieczeństwem informacji oraz sporządzeniem i wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Łęcznej. Zamawiający podkreśla, że celem nie jest uzyskanie zgodności z normą ISO/IEC 27001 ale podczas audytu i wdrażania SZBI należy kierować się wytycznymi zawartymi w ww. normie.

1. Wykonawca prac wstępnie musi przeprowadzić Audyt 0 polegający na:
	1. Spotkaniu informacyjnym dla kierownictwa nt. zakresu i sposobu przeprowadzenia audytu bezpieczeństwa informacji.
	2. Analizie i ocenie warunków organizacyjnych do spełnienia wymagań PN- ISO/IEC 27001
	3. Analizie dokumentacji ochrony danych osobowych i dokumentacji Polityki Bezpieczeństwa Informacji
	4. Weryfikacji stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji wynikających
	5. Analizie zgodności dokumentacji ochrony informacji
	6. Przygotowanie listy kontrolnej zbudowanej w oparciu o wymagania i wytyczne w zakresie bezpieczeństwa informacji
	7. Ocenie infrastruktury sieciowej Starostwa Powiatowego w Łęcznej polegającej na inwentaryzacji posiadanych urządzeń, analizie istniejącej sieci informatycznej, ocenie poziomu bezpieczeństwa stosowanego w tym zakresie i przedstawienie możliwych rozwiązań w celu ich udoskonalenia.

Ocena poziomu bezpieczeństwa ma opiera się o:

* + 1. Testy bezpieczeństwa wykonywane od strony sieci Internet
		2. Testy serwerów w sieci DMZ
		3. Testach sieci wewnętrznej
		4. Analizie konfiguracji urządzeń sieciowych
		5. Analizie reguł systemu firewall oraz ich optymalizacji pod kątem wydajności i poziomu bezpieczeństwa
		6. Analizie bezpieczeństwa systemów bezpieczeństwa w tym analizę konfiguracji wszystkich komponentów systemu operacyjnego i baz danych.
1. System antywirusowy
2. System IPS/IDS
	* 1. Analizie systemów backupów i archiwizacji danych
		2. Analizie zabezpieczeń oraz zainstalowanego oprogramowania znajdujących się na urządzeniach Zamawiającego
		3. Analizie ryzyka dotyczącego bezpieczeństwa infrastruktury Starostwa Powiatowego w Łęcznej
3. W ramach prac projektowych Wykonawca audytu musi przeprowadzić ocenę faktycznego stanu bezpieczeństwa informacji oraz wykorzystywanych w tym celu metod ochrony w Starostwie Powiatowym w Łęcznej mających odniesienie do przetwarzanych informacji wymagań i wytycznych zawartych w normie ISO/IEC 27001. Na podstawie wyników uzyskany podczas przeprowadzonej analizie Wykonawca opracuje zalecenia jakie należy podjąć w celu podwyższenia poziomu ochrony przetwarzania danych.
4. W zakresie prac projektowych wdrażania i ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji Wykonawca musi wykonać następujące prace:
	1. Ustalić i opisać zakres i granice Systemu Zarządzania Bezpieczeństwem Informacji
	2. Opracować harmonogram projektu wdrożenia SZBI
	3. Przeprowadzić identyfikację aktywów podstawowych i wspierających Starostwo Powiatowe w Łęcznej, i przeprowadzić klasyfikację informacji wraz z opracowaniem dokumentacji określającej sposób klasyfikacji, metody oznaczania oraz sposób postępowania z informacjami zaklasyfikowanymi do danej grupy.
	4. Sporządzić dokument opisujący podejście do szacowania ryzyka w Starostwie Powiatowym w Łęcznej i przeprowadzić badanie szacowania ryzyka w instytucji czego wynikiem będzie raport z szacowania ryzyka przetwarzania informacji oraz plan postępowania z ryzykiem.
	5. Sporządzić dokument opisujący strukturę organizacyjną zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Łęcznej wraz z określeniem ról i zakresów odpowiedzialności osób.
	6. Sporządzić dokumentację bezpieczeństwa, która składać się będzie z:

- Polityki Bezpieczeństwa informacji

- Procesu zarządzania bezpieczeństwem informacji

- zasad bezpieczeństwa informacji

- standardów bezpieczeństwa informacji

- procedur bezpieczeństwa informacji

Dokument polityki bezpieczeństwa informacji powinien zawierać:

1. Cele i definicję polityki bezpieczeństwa
2. Intencje zapewnienia bezpieczeństwa informacji
3. Strategię bezpieczeństwa informacji
4. Podejście do zarządzania bezpieczeństwem informacji
5. Podejście do szacowania ryzyka i postępowania z ryzykiem

Dokument Proces zarządzania bezpieczeństwem powinien zawierać:

1. Opis celów i zakresu procesu zarządzania bezpieczeństwem
2. Opis ról niezbędnych do procesu zarządzania bezpieczeństwem
3. Opis przebiegu zarządzania bezpieczeństwem
4. Definicję polityki i zasad dla procesu zarządzania bezpieczeństwem
5. Definicję mierników skuteczności i efektywności procesu zarządzania bezpieczeństwem
6. Szczegółowe procedury funkcjonowania procesu zarządzania bezpieczeństwem

Dokument zasad bezpieczeństwa informacji powinien odwoływać się do normy ISO/IEC 27001. Dodatkowo powinien zawierać wymagania, zalecenia i wytyczne bezpieczeństwa informacji.

Dokument standardy bezpieczeństwa informacji powinien zawierać uzupełnienie wymagań, zaleceń i wytycznych dokumentu zasad bezpieczeństwa informacji. Dlatego powinny zostać opracowane standardy tj.

1. Stacji roboczych i serwerów
2. Urządzeń sieciowych
3. Kryptograficznej ochrony informacji
4. Aplikacji infrastruktury
5. Autoryzacji i uwierzytelniania
6. Kasowania danych z nośników
7. Środowiska wirtualnego
8. Bezprzewodowej sieci WiFi
9. Polityki systemu DLP

Dokumenty procedur bezpieczeństwa powinny dotyczyć

1. Obsługi incydentów bezpieczeństwa
2. Nadzoru nad dokumentami Systemu Zarządzania Informacją
3. Oceny skuteczności zabezpieczeń
4. Działań zapobiegawczych
5. Audytu wewnętrznego
6. Zarządzania zmianami
	1. Opracować program szkoleń obejmujący zakres, zasady, wymagania dla szkoleń z bezpieczeństwa informacji.
	2. Przeprowadzić szkolenie z zakresu bezpieczeństwa informacji dotyczące zarządzania systemów bezpieczeństwa informacji oraz zarządzania ryzykiem dla pracowników Starostwa Powiatowego w Łęcznej.
7. Wykonawca wraz z Zamawiającym opracuje założenia dla systemu zarządzania ciągłością działania oraz opracuje plan ciągłości działania zawierający zasady postępowania w sytuacjach wystąpienia negatywnych zdarzeń.