Znak spraw: OiN.2601.107.2024 Załącznik nr 2 do zapytania ofertowego

**Opis przedmiotu zamówienia**

Przedmiotem zamówieni jest przeprowadzenie audytu KRI, przeglądu, aktualizacji i opracowania kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnej z normą ISO/IEC 27001:2023, wdrożenie SZBI, zbudowanie Planu Ciągłości Działania, przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa oraz przeprowadzenie testów socjotechnicznych.

Wykonawca musi zrealizować usługę polegającą na przeprowadzeniu audytu cyberbezpieczeństwa w urzędzie Starostwa Powiatowego w Żurominie w ramach projektu „Cyberbezpieczny samorząd” zgodnie z zakresem oraz formularzem stanowiącym załącznik do Regulaminu Konkursu Grantowego „Cyberbezpieczny samorząd” zakończonego raportem i diagnozą końcową oraz opracowanie pełnej kompletnej dokumentacji SZBI w oparciu o KRI/KSC i normę ISO27001. Wykonanie i przekazanie Raportu z Audytu oraz diagnozy końcowej (opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów, analiza złożonego zał. nr 6 konkursu grantowego). W ramach niniejszego zapytania ofertowego Wykonawca dodatkowo zobowiązuje się do wypełnienia załącznika nr 6 na zakończenie projektu. W ramach opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Wykonawca wdroży System Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym zgodnie z opisem przedmiotu zamówienia w oparciu o przepisy KRI/KSC i normę ISO 27001. Wykonawca przeprowadzi szkolenia z zakresu cyberbezpieczeństwa dla pracowników urzędu, a także przeprowadzi testy socjotechniczne.

Audyt bezpieczeństwa informacji obejmuje wszystkie obszary funkcjonowania Zamawiającego w tym co najmniej:

1. Audyt organizacyjny:

1. weryfikacja regulacji w obszarze zarządzania bezpieczeństwem informacji;
2. odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
3. dokumentacja, w tym z zakresu ochrony danych osobowych;
4. analiza ryzyka;
5. inwentaryzacja aktywów;
6. plan postępowania z ryzykiem;
7. przeprowadzenie wywiadów z wybranymi pracownikami.

2. Audyt fizyczny i środowiskowy

1. weryfikacja zabezpieczeń wejścia/wyjścia;
2. weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;
3. weryfikacja bezpieczeństwa okablowania strukturalnego;
4. weryfikacja systemów chłodzenia i systemów alarmowych.

3. Audyt teleinformatyczny

1. przeprowadzenie testów penetracyjnych systemu informatycznego wewnętrznie i zewnętrznie, określenie luk, wskazanie rozwiązań naprawczych, opracowanie raportu;
2. weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi;
3. przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania i ciągłości działania;
4. weryfikacja ochrony przed oprogramowaniem szkodliwym;
5. weryfikacja procedur zarządzania kopiami zapasowymi;
6. weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
7. weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
8. weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
9. Analiza i ocena mechanizmów zarządzania aktualizacja.

4. W ramach audytu bezpieczeństwa informacji Wykonawca przeprowadzi wizję lokalną w każdym z budynków Urzędu.

5. Zamawiający nie dopuszcza wykonania audytu bezpieczeństwa informacji w sposób zdalny. Badanie zabezpieczeń, podatności systemów, przeprowadzenie ewentualnych testów penetracyjnych, wykonawca powinien wykonać na miejscu w siedzibie Zamawiającego. Zamawiający dodatkowo wymaga aby w przeprowadzanych czynnościach audytowych brał bezpośrednio udział audytor wskazany w ofercie Wykonawcy.

6. Analiza wyników audytu i możliwości rozwiązania defektów. W wyniku przeprowadzonego audytu i zebranych danych Wykonawca opracuje raport wraz z oceną poziomu realizacji wymagań prawnych w zakresie bezpieczeństwa i ochrony informacji i danych oraz stanu zabezpieczeń technicznych i organizacyjnych. Raport z przeprowadzonego audytu bezpieczeństwa, będzie zawierał co najmniej:

1. podsumowanie zarządcze,
2. opis wykonania planu audytu,
3. opis wykorzystanych standardów,
4. ocenę spełnienia wymagań,
5. rekomendacje, w przypadku stwierdzonych niezgodności i braków, które będą stanowiły podstawę do aktualizacji, dostosowania lub przygotowania dokumentacji związanej z cyberbezpieczeństwem.

7. Raport powinien zostać omówiony na spotkaniu Najwyższym Kierownictwem Urzędu, Służbami Informatycznymi, Inspektorem Ochrony Danych i innymi wskazanymi osobami przez Zamawiającego. Wyniki raportu powinna wskazywać możliwości rozwiązania odkrytych defektów i nakreślić plan działań naprawczych.

1. Opracowanie dokumentacji SZBI:

Zamawiający posiada wytworzoną we własnym zakresie dokumentację wymaganą innymi aktami prawnymi. Dokumentacja ta wymaga aktualizacji i dostosowania do aktualnych norm. Wykonawca zaktualizuje lub w przypadku braku opracuje wspólnie z pracownikami zamawiającego, dokumenty z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa zgodnie z następującymi aktami prawnymi oraz normami:

1. ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557, z późn. zm.) (w zakresie dotyczącym bezpieczeństwa informacji),
2. rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymian informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773, z późn. zm.)(w zakresie dotyczącym bezpieczeństwa informacji),
3. rozporządzeniem 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),
4. ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077)
5. aktualnymi normami PN-ISO/IEC 27001, PN-ISO/IEC 27002,
6. Wykonawca przeprowadzi testy penetracyjne metodą black-box. Zamawiający oczekuje po wykonaniu testów penetracyjnych przekazania raportu zawierającego wykryte nieprawidłowości, a także korzystne rozwiązania, których celem będzie wyeliminowanie bądź ograniczenie słabości zabezpieczeń.
7. W ramach dokumentacji SZBI Wykonawca powinien zapewnić dostęp do wzorcowych szablonów dokumentów szacowania ryzyka, które wraz z Zamawiającym dostosuje do wymagań Urzędu.
8. Wykonawca zapewni dobór odpowiedniej dla organizacji metody oceny ryzyka,
9. Wykonawca udzieli wsparcie dla organizacji w zakresie inwentaryzacji i klasyfikacji aktywów informacyjnych oraz określenia ich podatności,
10. Wykonawca zapewni dobór odpowiedniej dla organizacji metody oceny ryzyka,
11. Wykonawca przygotuje wypełniony formularz szacowania ryzyka dla aktywów Zamawiającego oraz udzieli wsparcia w zakresie szacowania ryzyka i weryfikacji uzyskanych, udokumentowanych wyników,
12. W ramach dokumentacji SZBI Wykonawca powinien zapewnić dostęp do wzorcowych szablonów dokumentów planów ciągłości działania
13. Wykonawca udzieli wsparcia dla organizacji w zakresie wdrożenia planów ciągłości działania jego założeń i celów.
14. Wykonawca udzieli wsparcia w identyfikacji krytycznych procesów, zasobów i usług dostarczanych przez Urząd i jednostki podległe.
15. Wykonawca udzieli wsparcia w procesie budowy scenariuszy postępowania i określenia sposobów wznowienia krytycznych procesów i zasobów w sytuacjach awaryjnych, kryzysowych.
16. Wykonawca przeprowadzi szkolenia z zakresu cyberbezpieczeństwa dla pracowników urzędu. Szacowana liczba pracowników 65 osób. Wykonawca przeprowadzi szkolenia dla użytkowników w grupach 5-10 osób. Wielkość grup będzie uzależniona od liczby osób, które w tym samym czasie będą mogły opuścić stanowisko pracy bez zakłócania ciągłości działania Starostwa. Szkolenia odbędą się w formie wykładów połączonych z ćwiczeniami praktycznymi. Zamawiający udostępni Wykonawcy salę szkoleniową. Wszelkie niezbędne do przeprowadzenia szkoleń urządzenia wykonawca zapewni we własnym zakresie.

Minimalny zakres szkolenia:

Obszar 1: Wprowadzenie

* Czy w cyfrowym świecie naprawdę jest niebezpiecznie?
* Czym ryzykujemy zaniedbując bezpieczeństwo?
* Co zrobić, gdy popełniliśmy błąd w security?
* Co można stracić

Obszar 2: Wiedza podstawowa

* Jak dbać o swoje stanowisko pracy
* Unikanie ryzykownego sprzętu elektronicznego
* Podstawowe oprogramowanie zabezpieczające
* Wewnętrzne szkolenia z bezpieczeństwa

Obszar 3: Jak nas podejść, popularne techniki ataków

* Socjotechnika
* Phishing
* Ransomware

Obszar 4: Jak się bronić

* Hasła
* jako korzystać i chronić
* zabezpieczenie wieloczynnikowe
* antywirus
* kopie zapasowe
* aktualizacja oprogramowania
* zaufanie, a właściwie jego brak
* szyfrowanie danych

Obszar 5: Co chronimy

* Twoje dane
* Email -dlaczego należy chronić
* Przeglądarka
* Telefon
* Karty
* Komputer

Obszar 6: użyteczne oprogramowanie

* Samodzielne rozwijanie wiedzy o bezpieczeństwie
* Jeśli wyjdziesz z zamku, jego mury Cię nie obronią - dyscyplina
* Polityka prywatności, RODO i prawidłowe przetwarzanie danych wrażliwych
* Jak to jest z zasłanianiem kamerki, odłączaniem mikrofonu...?

Obszar 7: Bezpieczne hasła

* Jakie hasła są naprawdę bezpieczne?
* Korzyści ze sprawdzonego narzędzia - KeePass
* Instalacja i konfiguracja KeePass
* Dodawanie i używanie własnych haseł w KeePass
* Jak współdzielić hasła firmowe za pomocą KeePass

Obszar 8: Uwierzytelnianie dwuskładnikowe

* Obrona przed wyciekiem haseł
* Czym jest uwierzytelnianie dwuskładnikowe?
* Jakie rodzaje dodatkowych poświadczeń możemy wykorzystać?
* Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Google
* Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Facebook
* Do jakich usług zaleca się koniecznie korzystać z uwierzytelnienia dwuskładnikowego?

Obszar 9: Email oraz przeglądarka internetowa

* Co robimy, a co nie w przeglądarce
* Jak bezpiecznie używać poczty elektronicznej

Obszar 10: Smartfony i tablety

* Może lepiej nie korzystać ze wzoru bezpieczeństwa?
* Ile zajmuje włamywaczowi zainstalowanie szkodliwego programu na smartfonie?
* Czy można instalować aplikacje spoza sklepu google play?
* Ogranicz zaufanie do osób kontaktujących się telefonicznie

Obszar 11: Zagrożenia w pracy zdalnej

* Domownicy i własne dzieci mogą niecelowo Ci zaszkodzić
* Jak nie dać sobie ukraść danych osobowych
* Przechwycenie tożsamości i oszuści na portalach społecznościowych
* Okazje, zaskakująco dobre oferty i wygrane w konkursach

Obszar 12: Szkodliwe oprogramowanie, "robaki"

* Czym jest Bloatware i jak można się go pozbyć
* Jak sprawdzić czy jakiś plik jest bezpieczny
* Jak poznać się, że program spowalnia komputer

1. Wykonawca przeprowadzi testy socjotechniczne.

Wykonawca przeprowadzi testy socjotechniczne wobec pracowników Zamawiającego. Zamawiający wymaga przeprowadzenia testów socjotechnicznych opartych co najmniej o 4 różne scenariusze. Zakres testów zostanie uzgodniony z Zamawiającym. Szczegółowe scenariusze testów socjotechnicznych Wykonawca przekaże Zamawiającemu w terminie do **20** dni od dnia zawarcia umowy**.** Materiał zgromadzony w czasie testów zostanie opracowywany i przekazany Zamawiającemu i musi zawierać informację o osiągniętych rezultatach, zalecenia odnośnie podniesienia bezpieczeństwa procesów i systemów oraz uzupełnienia wiedzy użytkowników. Przeprowadzone testy mają na celu:

1. Identyfikację podatności na ataki socjotechniczne
2. Ocenę świadomości bezpieczeństwa wśród pracowników
3. Sprawdzenie skuteczności polityk i procedur bezpieczeństwa
4. Zwiększenie świadomości zagrożeń związanych z socjotechniką
5. Poprawa ogólnej strategii bezpieczeństwa u Zamawiającego