|  |  |  |
| --- | --- | --- |
| **OPIS PRZEDMIOTU ZAMÓWIENIA**  Przedmiotem zamówienia jest organizacja i przeprowadzenie szkoleń z zakresu opisanego w poniższej tabeli.  Wymagania wspólne w zakresie szkoleń:   1. Każde szkolenie wchodzące w zakres przedmiotu zamówienia musi zostać zrealizowane najpóźniej do dnia 19 grudnia 2025 r. 2. Termin realizacji poszczególnego szkolenia będzie uzgadniane indywidualnie z Zamawiającym z odpowiednim wyprzedzeniem, nie później niż na 14 dni przed planowanym rozpoczęciem każdego szkolenia. 3. Z uwagi na fakt, iż w poszczególnych szkoleniach biorą udział te same osoby, poszczególne szkolenia nie mogą odbywać się równolegle - w tym samym dniu – każde szkolenie musi zostać zorganizowane w odrębnym terminie, aby zapewnić uczestnictwo odpowiednich grup pracowników oraz możliwość pełnej kontroli realizacji przez Zamawiającego. | | |
| **Wymóg** | | **Minimalne wymaganie Zamawiającego** |
| **Podstawowe szkolenia dla pracowników z cyberbezpieczeństwa** | | |
| **Wymagania ogólne** | Przedmiotem zamówienia jest przeprowadzenie cyklu szkoleń dla pracowników Urzędu Gminy (UG) Zator w zakresie bezpieczeństwa informacji. Szkolenia będą obejmować tematykę z zakresu cyberbezpieczeństwa, regulacji wewnętrznych, wymagań rozporządzenia KRI oraz zasad bezpiecznego korzystania z Internetu. Program szkolenia musi uwzględniać specyfikę jednostki i kłaść nacisk na praktyczne zastosowanie procedur bezpieczeństwa w codziennej pracy.  Szkolenia muszą być prowadzone w formie stacjonarnej w siedzibie Zamawiającego.  Wykonawca zobowiązany jest do zapewnienia wykwalifikowanej kadry szkoleniowej.  Szkolenie dla pracowników (8 godzin), Ilość uczestników: 50 osób.  Zamawiający wymaga przeprowadzenia szkolenia w dwóch turach po 8 godzin, tj. w grupach max. 25 osobowych.  Każdy uczestnik szkolenia musi otrzymać: Imienny certyfikat ukończenia szkolenia, podpisany przez trenera. | |
| **Szczegółowy zakres szkolenia** | 1. Wprowadzenie do cyberbezpieczeństwa - znaczenie ochrony informacji w administracji publicznej. 2. Definicja cyberbezpieczeństwa i jego znaczenie w organizacjach publicznych. 3. Rola ochrony informacji w organizacji oraz zagrożenia związane z nieprzestrzeganiem zasad bezpieczeństwa informacji. 4. Podstawowe pojęcia związane z cyberbezpieczeństwem 5. Omówienie terminologii: dane osobowe, dane wrażliwe, atak hakerski, cyberzagrożenia, phishing, vishing, itp. 6. Definicje, znaczenie i praktyczne zastosowanie pojęć w kontekście bezpieczeństwa informacji w jednostkach publicznych. 7. Największe wycieki danych – przykłady 8. Omówienie realnych przypadków wycieków danych i ich konsekwencji dla organizacji i osób fizycznych. 9. Analiza przypadków dotyczących wycieków w sektorze publicznym. 10. Kary za naruszenia ochrony danych 11. Omówienie przepisów prawnych, w tym RODO, oraz sankcji za nieprzestrzeganie zasad ochrony danych. 12. Szyfrowanie, przechowywanie i udostępnianie danych 13. Zasady bezpiecznego przechowywania danych, szyfrowania oraz metod ich udostępniania zgodnie z przepisami. 14. Zasady korzystania z poczty elektronicznej 15. Bezpieczne korzystanie z poczty elektronicznej, ochronę przed spamem, phishingiem, zagrożeniami związanymi z załącznikami i linkami. 16. Bezpieczeństwo w Internecie 17. Zasady bezpiecznego korzystania z przeglądarek internetowych, rozpoznawanie niebezpiecznych stron i ochrona prywatności. 18. Ochrona danych w chmurze 19. Zasady przechowywania danych w chmurze oraz zabezpieczanie dostępu do nich, w tym szyfrowanie. 20. Bezpieczeństwo pracy zdalnej 21. Zasady pracy zdalnej na sprzęcie służbowym i prywatnym, używanie VPN, zabezpieczenie urządzeń, unikanie publicznych sieci Wi-Fi. 22. Fake news i dezinformacja 23. Jak rozpoznawać i przeciwdziałać dezinformacji oraz fake newsom w środowisku zawodowym. 24. Dokumentacja SZBI w jednostce 25. Przegląd wdrożonej dokumentacji SZBI w jednostkach oraz analiza praktycznych zastosowań. 26. Zalecenia dotyczące szczególnych zagrożeń wynikających z specyfiki urzędów oraz konieczność dostosowania procedur. 27. Podsumowanie 28. Podsumowanie kluczowych zagadnień szkolenia oraz praktyczne wskazówki wdrażania zasad bezpieczeństwa informacji. | |
| **Szkolenia dla kardy zarządzającej z cyberbezpieczeństwa** | | |
| **Wymagania ogólne** | Przedmiotem zamówienia jest przeprowadzenie cyklu szkoleń dla kadry kierowniczej Urzędu Gminy (UG) Zator w zakresie bezpieczeństwa informacji. Szkolenia będą obejmować tematykę z zakresu cyberbezpieczeństwa, regulacji wewnętrznych, wymagań rozporządzenia KRI oraz zasad bezpiecznego korzystania z Internetu. Program szkolenia musi uwzględniać specyfikę jednostki i kłaść nacisk na praktyczne zastosowanie procedur bezpieczeństwa w codziennej pracy.  Szkolenia muszą być prowadzone w formie stacjonarnej, w siedzibie Zamawiającego.  Wykonawca zobowiązany jest do zapewnienia wykwalifikowanej kadry szkoleniowej.  Szkolenie dla kadry kierowniczej (8 godzin), Ilość uczestników: 10 osób.  Każdy uczestnik szkolenia musi otrzymać: Imienny certyfikat ukończenia szkolenia, podpisany przez trenera. | |
| **Szczegółowy zakres szkolenia** | 1. Omówienie NIS2 i polityki SZBI 2. Przedstawienie wymagań wynikających z dyrektywy NIS2 oraz omówienie wdrożonej polityki SZBI w kontekście organizacyjnym i operacyjnym. 3. Wskazanie odpowiedzialności kadry kierowniczej w zakresie zarządzania bezpieczeństwem informacji. 4. Przedstawienie opracowanych procedur 5. Omówienie zasad postępowania zgodnych z wdrożonym SZBI oraz ich wpływ na funkcjonowanie urzędu. 6. Symulacje rzeczywistych sytuacji i ćwiczenia praktyczne w celu przetestowania skuteczności procedur. 7. Określenie obowiązków wynikających z procedur 8. Wyjaśnienie obowiązków pracowników w zakresie przestrzegania procedur, zarządzania dostępem do danych oraz reagowania na zagrożenia. 9. Wymagania normy ISO/IEC 27001, KRI oraz SZBI 10. Przegląd wymagań normy ISO/IEC 27001 oraz KRI w kontekście organizacyjnym. 11. Omówienie praktycznych aspektów wdrożenia SZBI oraz zarządzania bezpieczeństwem informacji w jednostkach publicznych. 12. Wymagania załącznika A normy ISO27001 13. Szczegółowe omówienie wymagań zawartych w Załączniku A normy ISO 27001, w tym procedur oraz zasad bezpieczeństwa. 14. Szacowanie ryzyka 15. Metody szacowania ryzyka w organizacji, identyfikacja ryzyk i propozycje działań zaradczych. 16. Praktyczne przykłady obliczania ryzyka w kontekście bezpieczeństwa informacji. 17. Symulacje i ćwiczenia 18. Realne przypadki oraz symulacje zagrożeń, które mogą wystąpić w pracy jednostki publicznej. 19. Podsumowanie i zalecenia 20. Podsumowanie kluczowych zagadnień szkolenia, wskazówki dotyczące monitorowania i doskonalenia procedur bezpieczeństwa w jednostkach. | |
| **Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami** | | |
| **Wymagania ogólne** | Przedmiotem zamówienia jest realizacja specjalistycznego szkolenia edukacyjnego w formule „live hacking”, którego celem jest podniesienie świadomości pracowników w zakresie zagrożeń cybernetycznych, ze szczególnym uwzględnieniem metod socjotechnicznych i technicznych wykorzystywanych przez cyberprzestępców.  Szkolenia muszą być prowadzone w formie stacjonarnej, w siedzibie Zamawiającego.  Wykonawca zobowiązany jest do zapewnienia wykwalifikowanej kadry szkoleniowej.  Szkolenie z testami socjotechnicznymi dla urzędników (8 godzin), Ilość uczestników: 50 osób.  Każdy uczestnik szkolenia musi otrzymać: Imienny certyfikat ukończenia szkolenia, podpisany przez trenera. | |
| **Szczegółowy zakres szkolenia** | 1. Szkolenie podzielone musi być na moduły tematyczne, z których każdy musi zawierać: 2. Krótkie wprowadzenie teoretyczne (z kontekstem i statystykami), 3. Pokaz ataku w czasie rzeczywistym („live demo”), 4. Analizę przebiegu ataku i identyfikację błędów użytkownika, 5. Omówienie środków zaradczych (technicznych i organizacyjnych). 6. Moduł 1: Wprowadzenie do cyberzagrożeń 7. Najczęstsze zagrożenia w organizacjach publicznych i ochrony zdrowia. 8. Statystyki skuteczności ataków socjotechnicznych (phishing, spear-phishing, smishing, vishing). 9. Cele atakujących: kradzież danych, dostęp do systemów, szantaż (ransomware), dezinformacja. 10. Przegląd najgłośniejszych incydentów z ostatnich lat (z Polski i świata). 11. Moduł 2: Phishing – najbardziej popularna broń hakera   Pokaz na żywo:   1. Utworzenie fałszywego maila od działu IT (np. prośba o zmianę hasła). 2. Zbudowanie strony phishingowej przypominającej portal logowania (np. Microsoft 365). 3. Demonstracja, jak ofiara wprowadza dane i jak trafiają one do atakującego.   Uczestnicy muszą dowiedź się:   1. Jak rozpoznać fałszywego maila (analiza nagłówków, linków, języka wiadomości). 2. Czym różni się phishing masowy od spear-phishingu (spersonalizowanego). 3. Jakie są konsekwencje kliknięcia w podejrzany link i jak reagować. 4. Moduł 3: Złośliwe oprogramowanie w akcji (malware, keyloggery, RAT)   Pokaz na żywo:   1. Przykład e-maila z załącznikiem (np. faktura, CV), który zawiera makro uruchamiające złośliwy kod. 2. Symulacja działania keyloggera – rejestrowanie wszystkiego, co wpisuje użytkownik. 3. Demonstracja zdalnego dostępu do komputera (RAT – Remote Access Trojan).   Uczestnicy muszą dowiedź się:   1. Jakie pliki są szczególnie niebezpieczne (np. .docm, .exe, .zip). 2. Dlaczego makra w dokumentach Office są ryzykowne. 3. Jakie są objawy infekcji i kiedy należy reagować. 4. Moduł 4: Przejęcie konta – jak łatwo ukraść tożsamość użytkownika   Pokaz na żywo:   1. Przejęcie loginu i hasła z fałszywej strony logowania. 2. Próba logowania do rzeczywistej usługi przy użyciu zdobytych danych (symulacja).   Uczestnicy muszą dowiedź się:   1. Dlaczego unikalne i silne hasła są kluczowe. 2. Jak działa uwierzytelnianie wieloskładnikowe (MFA) i dlaczego warto je włączyć. 3. Jakie są najczęstsze błędy związane z przechowywaniem danych dostępowych. 4. Moduł 5: Ataki w sieci lokalnej – sniffing, man-in-the-middle   Pokaz na żywo:   1. Podłączenie się do tej samej sieci Wi-Fi co ofiara. 2. Przechwytywanie ruchu sieciowego (np. dane logowania, zapytania HTTP). 3. Przykład ataku MITM (Man-in-the-Middle) – modyfikacja komunikacji użytkownika.   Uczestnicy muszą dowiedź się:   1. Dlaczego nie należy korzystać z otwartych sieci Wi-Fi. 2. Czym są certyfikaty SSL/TLS i jak chronią komunikację. 3. Jakie są podstawowe środki ochrony w sieciach lokalnych. 4. Moduł 6: Spoofing i pretexting – socjotechnika głosem i słowem   Pokaz na żywo:   1. Symulacja rozmowy telefonicznej z podszyciem się pod dział IT lub administratora. 2. Tworzenie przekonującej narracji – „pretext”, czyli historia mająca na celu zmanipulowanie pracownika.   Uczestnicy muszą dowiedź się:   1. Jakie techniki manipulacyjne stosują atakujący. 2. Jak rozpoznać nieautoryzowany kontakt. 3. Jakie zasady obowiązują przy weryfikacji tożsamości rozmówcy. 4. Moduł 7: Ataki fizyczne i psychologiczne – tailgating, baiting   Omówienie i pokaz:   1. Jak osoba nieuprawniona może wejść na teren organizacji (tailgating). 2. Przykład „niewinnego” pendrive’a pozostawionego na recepcji (baiting). 3. Co może się wydarzyć po jego podłączeniu do komputera.   Uczestnicy muszą dowiedź się:   1. Jak rozpoznawać i reagować na próby manipulacji w świecie fizycznym. 2. Dlaczego polityka czystego biurka (clean desk policy) ma znaczenie. 3. Jakie są procedury reagowania na incydenty fizyczne. 4. Moduł 8: Podsumowanie i dobre praktyki   Omówienie najważniejszych wniosków z pokazów.  Przegląd dobrych praktyk:   1. zasada ograniczonego zaufania, 2. weryfikacja źródła informacji, 3. bezpieczne korzystanie z e-maila i internetu, 4. aktualizacje oprogramowania i systemów, 5. odpowiedzialność użytkownika za dane. | |
| **Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, SZBI** | | |
| **Wymagania ogólne** | Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), z elementami normy ISO/IEC 27001, aby spełnić zgodność dyrektywy NIS2 oraz obowiązującymi przepisami prawa. | |
| **Zakres i Etapy Wdrożenia SZBI** | 1. Audyt Wstępny:   Wykonawca przeprowadzi audyt wstępny, którego celem będzie ocena aktualnego stanu systemu bezpieczeństwa informacji w Urzędzie Gminy Zator.   1. Ocena zgodności z wymaganiami § 20 ust. 2 rozporządzenia KRI oraz normą ISO/IEC 27001, aby sprawdzić aktualny stan bezpieczeństwa informacji w Urzędzie Gminy Zator. 2. Analiza zabezpieczeń: Przeprowadzenie szczegółowej analizy zabezpieczeń systemów IT, identyfikacja luk w zabezpieczeniach oraz przedstawienie rekomendacji działań naprawczych dla Urzędu Gminy Zator. 3. Sporządzenie raportu z audytu wstępnego: Raport powinien zawierać szczegółowe wyniki analizy stanu systemu bezpieczeństwa informacji, z uwzględnieniem rekomendacji działań naprawczych i doskonalących. 4. Konsultacje: Wykonawca zorganizuje spotkania z zespołem odpowiedzialnym za wdrożenie SZBI w Urzędzie Gminy Zator celem omówienia wyników audytu wstępnego oraz przedstawienia zaleceń i planu działań naprawczych. 5. Podpisanie raportu przez audytorów: Raporty z audytu wstępnego muszą być podpisane przez audytorów, którzy przeprowadzili ocenę. 6. Opracowanie Polityk i Procedur SZBI:   Wykonawca opracuje i wdroży niezbędne polityki oraz procedury SZBI zgodne z wymaganiami normy ISO/IEC 27001 oraz przepisami krajowymi.   1. Polityka bezpieczeństwa informacji: Opracowanie polityki bezpieczeństwa informacji, która będzie zgodna z normą ISO/IEC 27001 oraz wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa. 2. Cele i zakres SZBI: Zdefiniowanie celów i zakresu SZBI na podstawie analizy kontekstu organizacji, uwzględniając specyficzne zagrożenia i ryzyka, które mogą wystąpić w Urzędzie Gminy Zator. 3. Procedury zarządzania incydentami: Opracowanie procedur reagowania na incydenty związane z bezpieczeństwem informacji, w tym zasady postępowania w przypadku naruszenia ochrony danych. 4. System zarządzania dostępami: Opracowanie systemu zarządzania dostępem, kontrola uprawnień użytkowników oraz wdrożenie ścisłych procedur kontrolujących dostęp do systemów IT i danych w Urzędzie Gminy Zator. 5. Plan ciągłości działania (BCP) oraz plan reagowania na incydenty: Opracowanie dokumentów określających procedury zapewnienia ciągłości działania w przypadku awarii, jak i reagowania na incydenty związane z cyberbezpieczeństwem. 6. Ocena zgodności wdrożonych procedur: Analiza i ocena zgodności opracowanych polityk i procedur z normą ISO/IEC 27001 oraz przepisami prawa krajowego, ze szczególnym uwzględnieniem ustawy o krajowym systemie cyberbezpieczeństwa oraz regulacji NIS2. 7. Opracowanie dokumentacji systemowej: Wykonawca opracuje pełną dokumentację systemu zarządzania bezpieczeństwem informacji, instrukcje operacyjne oraz polityki wewnętrzne dotyczące cyberbezpieczeństwa. 8. Audyt Końcowy:   Po wdrożeniu SZBI, wykonawca przeprowadzi audyt końcowy, który oceni zgodność systemu z normą ISO/IEC 27001 oraz wymaganiami przepisów prawa.   1. Ocena zgodności z wymaganiami § 20 ust. 2 rozporządzenia KRI oraz normą ISO/IEC 27001 po zakończeniu wdrożenia SZBI. 2. Analiza zabezpieczeń: Wykonawca przeprowadzi szczegółową analizę zabezpieczeń po wdrożeniu SZBI, identyfikując luki oraz przedstawiając rekomendacje działań naprawczych. 3. Sporządzenie raportu z audytu końcowego: Raport z audytu końcowego będzie zawierał wyniki analizy, wskazówki dotyczące dalszego doskonalenia systemu oraz rekomendacje naprawcze. 4. Podpisanie raportu przez audytorów: Raport z audytu końcowego musi być podpisany przez audytorów przeprowadzających ocenę. 5. Dostosowanie dokumentacji do specyfiki jednostki, w ścisłej współpracy z zespołem odpowiedzialnym za wdrożenie SZBI w Urzędzie Gminy Zator. 6. Analiza punktów normy ISO 27001: Wykonawca przeanalizuje szczegółowo każdy punkt normy ISO 27001 w odniesieniu do wyników audytu wstępnego oraz oceni aktualny stan wdrożenia wymagań normy w jednostkach. 7. Dostosowanie procedur do realiów organizacyjnych: Wdrażane procedury muszą być praktyczne, spójne z codziennym funkcjonowaniem organizacji oraz zapewniać zgodność z KRI oraz normą ISO 27001. 8. Opracowanie Dokumentacji:   Wykonawca zobowiązany jest do opracowania pełnej dokumentacji zgodnej z normą ISO/IEC 27001.   1. Dokumenty wymagane przez Zamawiającego: m.in. Księga Systemu Zarządzania Bezpieczeństwem Informacji, Polityka Bezpieczeństwa Informacji, Plan Kontynuacji Działania (BCP), procedury audytu wewnętrznego, zarządzania incydentami, bezpieczeństwa fizycznego, procedura nadzoru nad dokumentami. | |
| **Przeprowadzenie analizy ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach przetwarzania danych** | | |
| **Wymagania ogólne** | Przedmiotem zamówienia jest przeprowadzenie kompleksowej analizy ryzyka w odniesieniu do zasobów (systemów, osób, technologii, lokalizacji, danych) zaangażowanych w procesy przetwarzania danych osobowych oraz innych danych chronionych, realizowanych przez Zamawiającego.  Zamawiający wymaga od Wykonawcy dostarczenia:   1. Kompletnego raportu z analizy ryzyka, 2. Plan postępowania z ryzykiem (akceptacja lub działania korygujące), 3. Dokumentację zgodną z wymaganiami ISO 27001, RODO oraz gotową do przedstawienia organom kontrolnym (UODO, KSC), 4. Wnioski do dalszego wykorzystania przy projektowaniu środków zabezpieczających i doskonaleniu SZBI. | |
| **Cele działania i wymagane efekty** | 1. Identyfikacja i ocena ryzyk dla procesów przetwarzania danych osobowych, 2. Powiązanie ryzyk z zasobami organizacji (aktywami informacyjnymi), 3. Zapewnienie zgodności z wymaganiami RODO (art. 24, 32, 35), ISO/IEC 27001:2022, wytycznymi UODO oraz ustawą o krajowym systemie cyberbezpieczeństwa, 4. Opracowanie planu postępowania z ryzykiem i zaleceń dla właścicieli procesów. | |
| **Przygotowanie do analizy** | 1. Przegląd i identyfikacja procesów przetwarzania danych (w oparciu o rejestr czynności przetwarzania, jeżeli jest dostępny), 2. Warsztaty z udziałem właścicieli procesów i przedstawicieli IT (w formie spotkań roboczych), 3. Identyfikacja zasobów i aktywów informacyjnych biorących udział w przetwarzaniu danych (systemy IT, osoby, urządzenia, aplikacje, lokalizacje, media, zbiory danych), 4. Określenie kryteriów oceny wpływu (poufność, integralność, dostępność, rozliczalność). | |
| **Analiza ryzyka** | 1. Identyfikacja zagrożeń i podatności (z uwzględnieniem m.in. typowych incydentów, czynników ludzkich, błędów konfiguracyjnych, awarii sprzętu, wycieków danych, działania osób trzecich, złośliwego oprogramowania), 2. Ocena poziomu ryzyka w odniesieniu do poszczególnych zasobów i procesów, 3. Analiza ryzyka w ujęciu jakościowym (lub mieszanym jakościowo-ilościowym – zależnie od metodyki), 4. Wykorzystanie uznanej metodyki – np. ISO/IEC 27005, NIST RMF, lub metody opracowanej przez UODO (zalecenie dostosowania do kontekstu Zamawiającego), 5. Określenie poziomu akceptowalności ryzyka przez organizację, 6. Określenie ryzyk wysokich wymagających priorytetowego działania. | |
| **Plan postępowania z ryzykiem** | 1. Opracowanie planu działań zmierzających do ograniczenia ryzyka, 2. Rekomendacje środków technicznych i organizacyjnych (w tym kontrole dostępu, monitoring, szyfrowanie, podnoszenie świadomości, zmiana procedur, konfiguracja systemów), 3. Przypisanie właścicieli ryzyka i harmonogramów działań, 4. Powiązanie środków zaradczych z procesami i systemami. | |
| **Raporty i dokumentacja** | Zamawiający wymaga od Wykonawcy dostarczenia:   1. Raportu z analizy ryzyka, zawierającego: 2. Mapę procesów przetwarzania i powiązanych zasobów, 3. Tabelę identyfikacji zagrożeń i podatności, 4. Macierz ryzyka, 5. Opis metodyki i przyjętych założeń, 6. Podsumowanie ryzyk nieakceptowalnych oraz rekomendacje. 7. Planu postępowania z ryzykiem, w podziale na: 8. Ryzyka do zaakceptowania, 9. Ryzyka wymagające ograniczenia lub wyeliminowania, 10. Proponowane działania i środki zaradcze, 11. Wskazanie osób odpowiedzialnych i terminów wdrożenia. 12. Protokół przekazania dokumentacji. | |
| **Wymagania organizacyjne** | 1. Prace analityczne zostaną zrealizowane z uwzględnieniem cyklu spotkań roboczych (online lub stacjonarnych), 2. Wykonawca przeprowadzi minimum jedno spotkanie otwierające i jedno zamykające z Zamawiającym, 3. Dokumentacja zostanie przekazana w formie elektronicznej (edytowalnej i PDF), 4. Wykonawca przekaże pełne majątkowe prawa autorskie do dokumentacji. | |
| **Opracowanie i wdrożenie metodyk i procedur: obsługi incydentów, ciągłości działania kontroli dostępu, bezpieczeństwa pracy zdalnej, używania urządzeń mobilnych** | | |
| **Wymagania ogólne** | Przedmiotem zamówienia jest opracowanie oraz wdrożenie metodyk, zasad i procedur w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa, obejmujących następujące obszary:   1. Obsługa incydentów bezpieczeństwa informacji i cyberbezpieczeństwa, 2. Zapewnienie ciągłości działania oraz zarządzanie kryzysowe, 3. Stosowanie kryptografii i szyfrowania danych, 4. Zarządzanie dostępem i kontrola uprawnień, 5. Bezpieczeństwo pracy zdalnej, 6. Użytkowanie urządzeń mobilnych w środowisku organizacji.   Zamówienie obejmuje opracowanie dokumentacji (metodyki, polityki, procedury).  Dla każdego z wymienionych obszarów Wykonawca opracuje:   1. Metodykę postępowania i ramowe zasady działania organizacji, 2. Politykę lub wytyczne (jeśli dotyczy), 3. Procedury operacyjne (SOP) – instrukcje krok po kroku, 4. Załączniki, formularze, wzory rejestrów, szablony raportów itp.   Wszystkie dokumenty muszą być:   1. Spójne ze standardami: ISO/IEC 27001, ISO/IEC 27002, ISO 22301, NIS2, RODO, 2. Przygotowane w języku polskim, w edytowalnym formacie, 3. Gotowe do przyjęcia i podpisania przez kierownictwo bez konieczności ingerencji Zamawiającego.   Zamawiający wymaga od Wykonawcy dostarczenia:   1. Kompletu dokumentów w wersji edytowalnej i PDF, 2. Listy przekazanych materiałów, 3. Rejestr procedur i ich właścicieli, 4. Dokumentację gotową do przyjęcia przez organizację bez konieczności modyfikacji. | |
| **Obsługa incydentów bezpieczeństwa** | 1. Klasyfikacja i priorytetyzacja incydentów, 2. Role i odpowiedzialności zespołów reagowania, 3. Etapy obsługi: wykrycie, rejestracja, eskalacja, analiza, reakcja, przywrócenie, raportowanie, 4. Prowadzenie rejestru incydentów i raportów końcowych, 5. Wymogi raportowania do CSIRT NASK, UODO, właściwego CSIRT sektora. | |
| **Ciągłość działania i zarządzanie kryzysowe** | 1. Opracowanie polityki ciągłości działania i BIA (analiza wpływu), 2. Identyfikacja funkcji krytycznych i zasobów kluczowych, 3. Plan ciągłości działania (BCP) i plan odtwarzania awaryjnego (DRP), 4. Schematy decyzyjne i zarządzanie kryzysem (CRP), 5. Harmonogramy testów i ćwiczeń, 6. Wzory komunikatów kryzysowych. | |
| **Stosowanie kryptografii i szyfrowania** | 1. Dobór metod szyfrowania danych (w spoczynku i w transmisji), 2. Zarządzanie cyklem życia kluczy kryptograficznych, 3. Wymagania techniczne i organizacyjne dot. stosowania TLS, VPN, S/MIME, GPG, 4. Wymogi w zakresie ochrony nośników danych i kopii zapasowych. | |
| **Kontrola dostępu** | 1. Polityka nadawania, zmiany i odbierania uprawnień, 2. Zasada najmniejszych uprawnień (PoLP), 3. Mechanizmy kontroli logowania, haseł, MFA, 4. Rejestr użytkowników i ich dostępów, 5. Przeglądy i recertyfikacja dostępów, 6. Procedury zarządzania kontami uprzywilejowanymi. | |
| **Bezpieczeństwo pracy zdalnej** | 1. Warunki dopuszczalności pracy zdalnej z perspektywy bezpieczeństwa informacji, 2. Wymagania dot. połączeń zdalnych (VPN, VDI), 3. Lista dozwolonych urządzeń, warunki środowiskowe, 4. Zasady bezpieczeństwa fizycznego i technicznego, 5. Zachowanie prywatności i rozdzielenie danych służbowych od prywatnych. | |
| **Użytkowanie urządzeń mobilnych** | 1. Rejestracja i autoryzacja urządzeń mobilnych, 2. Zasady stosowania urządzeń prywatnych (BYOD) lub służbowych, 3. Wymogi techniczne (szyfrowanie, blokady, MDM), 4. Polityka czystego urządzenia (clean mobile device), 5. Procedura w przypadku zgubienia, kradzieży lub incydentu. | |
| **Dokumentacja** | Wykonawca zapewni pełne prawa autorskie majątkowe do opracowanej dokumentacji.  Dokumentacja będzie zgodna z wymaganiami audytowalnymi – gotowa do okazania jednostce certyfikującej (np. ISO 27001) lub organom nadzoru (np. UODO, KPRM). | |