Szczegółowe minimalne wymagania do opis przedmiotu zamówienia

Lp.	Nazwa elementu	Wymagane minimalne
1.	Wymogi podstawowe.	1) Audyt musi być wykonywany stacjonarnie u Zamawiającego 2) Audyt ma zostać przeprowadzony przez zespół z udziałem co najmniej dwóch audytorów, 3) Cały proces audytowy ma zakończyć się przedstawieniem protokołu (raportu) poaudytowego, zawierającego co najmniej takie elementy jak: a) definicje prawne; b) cel audytu; c) zasada przeprowadzanego audytu; d) kryteria audytu oraz mierniki oceny; e) wyniki przeprowadzonego audytu uwzględniając obszary z pkt 2 wraz z opisem obszarów zgodnych w zakresie wymogów KRI; f) krytycznych niezgodności, szczególnie wpływających na bezpieczeństwo informacji obszarów audytowych wymagających zmiany oraz doskonalenia; g) wdrożenia procesów poaudytowych mających na celu bieżące i przyszłościowe utrzymanie bezpieczeństwa informacji i systemów IT na poziomie gwarantującym zgodność z KRI; h) zalecenia w zakresie potencjalnych niezgodności; i) określenie zakresu i priorytetu działań naprawczych; 4) Wraz z protokołem (raportem) wyniki oraz ocenę audytu przedstawić na spotkaniu kierownictwu Zamawiającego.
2.	Zakres audytu.	Audyt ma obejmować obszar: a) działań projektowych, wdrożeniowych oraz eksploatacyjnych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk; b) Systemu Zarządzania Bezpieczeństwem Informacji pod kątem poufności, dostępności i integralności; c) regulacji wewnętrznych w zakresie zmieniającego się otoczenia pod kątem ich aktualizacji; d) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację; e) okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy; f) działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

Lp.	Nazwa elementu	Wymagane minimalne
		g) procesów zapewniających szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: – zagrożenia bezpieczeństwa informacji, – skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, – stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich. h) ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, pod kątem: – monitorowania dostępu do informacji, – czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, – zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji; i) ustanowionych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość; j) zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie; k) umów serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji; l) zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych; m) odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: – dbałości o aktualizację oprogramowania, – minimalizowaniu ryzyka utraty informacji w wyniku awarii, – ochronie przed błędami, utratą, nieuprawnioną modyfikacją, – stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, – zapewnieniu bezpieczeństwa plików systemowych, – redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, – niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, – kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa; n) poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii;

Lp.	Nazwa elementu	Wymagane minimalne
		o) komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących; p) ciągłości wykonywania audytu wewnętrznego (kontroli wewnętrznej); q) występowania dodatkowych zabezpieczeń, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych; r) prowadzenia/występowania dzienników systemowych odnotowujących działania użytkowników lub obiektów systemowych, polegających na dostępie do: – systemu z uprawnieniami administracyjnymi, – konfiguracji systemu, w tym konfiguracji zabezpieczeń, – przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa; s) występowania procedur mogących stanowić odnotowywanie działań użytkowników lub obiektów systemowych, a także innych zdarzeń związanych z eksploatacją systemu w postaci: – działań użytkowników nieposiadających uprawnień administracyjnych, – zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, – zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny, – w zakresie wynikającym z analizy ryzyka; t) procedur związanych z dziennikami systemowymi.
3.	Minimalny zakres przedmiotowy audytu - systemy teleinformatyczne oraz usługi	Wykaz systemów IT oraz usług podlegających audytowi: a) Serwery z rodziny Windows i Linux. 14 serwerów fizycznych, 40 serwerów wirtualnych ; b) DMZ – ocena segmentacji sieci; c) Sieć LAN z serwerami i usługami sieciowymi – switche; routery/firewale, urządzenia ochrony poczty elektronicznej, kontrolery domeny, serwery pocztowe, serwery bazodanowe, serwery usługowe; d) Zabezpieczenia usług i systemów RCB. - routery/firewale, urządzenia ochrony poczty elektronicznej, systemy antywirusowe, systemy kontroli VPN, analizatory sieci, skanowanie usług, portów, podatności – **z wyłączeniem aktywnego sprawdzania podatności**. (Testy tego typu można przeprowadzić jedynie na kopiach maszyn produkcyjnych); e) Poczta elektroniczna obsługiwana za pomocą programu Microsoft Exchange OnPremise z klientem Office Outlook firmy Microsoft wraz z systemem antywirusowym, antyspamowym; f) Usługa w ePUAP – skrzynka podawcza Elektronicznej Platformy Usług Administracji Publicznej, w tym podpisy elektroniczne; g) System EZD „Edicta" – system do Elektronicznego Zarządzania Dokumentami. Dostarczony i wspierany przez ZETO, w tym podpisy elektroniczne. System pracuje w architekturze klient-serwer;

Lp.	Nazwa elementu	Wymagane minimalne
		h) System teleinformatyczny z programem „Kadry i Płace" (zarządzanie dokumentami powiązanymi z poszczególnymi pracownikami); i) System teleinformatyczny z programem „Płatnik" – (dedykowane oprogramowanie do tworzenie i weryfikacja dokumentów ubezpieczeniowych oraz wymiana informacji z Zakładem Ubezpieczeń Społecznych); j) Stanowisko platformy Usług Elektronicznych (PUE) ZUS – (oprogramowanie do generowania i przesyłania drogą elektroniczną dokumentów zgłoszeniowych i rozliczeniowych oraz różnego typu pism i wniosków); k) Stanowisko systemu „Bankowość Elektroniczna NBP"- (oprogramowanie do wspomaga obsługi rachunków bankowych); l) System teleinformatyczny z programem „Księgowość Budżetowa i Planowanie" – (usprawnia realizację zadań związanych z ewidencją i rozliczeniem budżetu); m) Program „Środki Trwałe" – (składnik majątku firmowego przewidziany do użytkowania powyżej jednego roku);
4.	Minimalne wymogi, audytorów ze składu zespołu audytowego	Audytorzy powinni posiadać uprawnienia oraz: a) audytora wiodącego Systemów Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001:2017 (certyfikacja uzyskana w jednostce akredytowanej przez Polskie Centrum Akredytacji), oraz/lub, b) audytora wiodącego Systemów Zarządzania Ciągłością; Działania wg normy PN-EN ISO 22301:2020 (certyfikacja uzyskana w jednostce akredytowanej przez CQI & IRCA), oraz/lub, c) certyfikat określony w rozporządzeniu Ministra Cyfryzacji z dnia 12.10.2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu; d) powinni wykazać się przeprowadzeniem co najmniej 3 audytów w zakresie KRI.

Uzgodnił:

Jan Teleon

Opracował:

Jan Danowski