**Załącznik nr 1 – Szczegółowy opis przedmiotu zamówienia**

**Wykonanie audytu z Krajowych Ram Interoperacyjności rozszerzony do niektórych aspektów z Krajowych Systemów Cyberbezpieczeństwa wraz w przeprowadzeniem diagnozy cyberbezpieczeństwa.**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa elementu | Wymagane minimalne parametry techniczne  |
|  | Wymogi podstawowe | 1. Audyt musi być wykonywany stacjonarnie u Zamawiającego.
2. Audyt ma przeprowadzony przez co najmniej 2 audytorów norm ISO, posiadających certyfikację uzyskaną w jednostce akredytowanej przez PCA),
3. Cały proces audytowy ma zakończyć się przedstawieniem protokołu poaudytowego (w skład którego zawierać się będzie legislacja i dokumenty dodatkowe), zawierającego elementy takie jak:
	1. definicje prawne,
	2. cel audytu,
	3. zasada przeprowadzanego audytu,
	4. kryteria audytu oraz mierniki oceny,
	5. proces przygotowania audytu (wraz z uwzględnieniem współpracy z Zamawiajacym),
	6. wyniki przeprowadzonego audytu przedstawione dwojako:
		* na podstawie wymaganej diagnozy przez Ministerstwo,
		* na podstawie wytycznych Ministerstwa Cyfryzacji dla NIKu w zakresie kontroli systemów teleinformatycznych.
4. W procesie audytowym zostanie wypełniony załącznik nr 8 - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa który jest wymagany obligatoryjnie w Regulaminie Konkursu Grantowego Cyfrowy Powiat.
 |
|  | Minimalny zakres audytu KRI | § 15 ust. 1 KRI Audyt 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.§ 20 ust. 1 KRI Audyt Systemu Zarządzania Bezpieczeństwem Informacji pod kątem poufności, dostępności i integralności.§ 20 ust. 2 pkt 1 KRI Audyt regulacji wewnętrznych w zakresie zmieniającego się otoczenia pod kątem aktualizacji.§ 20 ust. 2 pkt 2 KRI Audyt utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.§ 20 ust. 2 pkt 3 KRI Audyt okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.§ 20 ust. 2 pkt 4 KRI Audyt 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.§ 20 ust. 2 pkt 6 KRI Audyt 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.

§ 20 ust. 2 pkt 7 KRI Audyt 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.

§ 20 ust. 2 pkt 8 KRI Audyt ustanowionych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.§ 20 ust. 2 pkt 9 KRI Audyt zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.§ 20 ust. 2 pkt 10 KRI Audyt umów serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji.§ 20 ust. 2 pkt 11 KRI Audyt zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.§ 20 ust. 2 pkt 12 KRI Audyt 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.

§ 20 ust. 2 pkt 12 lit. b KRI Audyt poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.§ 20 ust. 2 pkt 13 KRI Audyt komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.§ 20 ust. 2 pkt 14 KRI Audyt ciągłości wykonywania audytu wewnętrznego.§ 20 ust. 4 KRI Audyt występowania dodatkowych zabezpieczeń, niezależnych od zakresu, o którym mowa w § 20 ust. 2 pkt 1:14, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne.§ 21 ust. 2 KRI Audyt 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.

§ 21 ust. 3 KRI Audyt występowania procedur spoza zakresu § 20 ust. 2 pkt 1:14, 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.

§ 21 ust. 4 KRI Audyt procedur związanych z dziennikami systemowymi. |
|  | Minimalny zakres audytu Cyberbezpieczeństwa | Weryfikacja aspektów ujętych w przepisach ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa w formie audytu |
|  | Wymogi jakie mają spełniać obie osoby wykonujące audyt | Posiadać uprawnienia:Audytora wiodącego Systemów Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001:2017 (certyfikacja uzyskana w jednostce akredytowanej przez Polskie Centrum Akredytacji),Audytora wiodącego Systemów Zarządzania Ciągłością Działania wg normy PN-EN ISO 22301:2020 (certyfikacja uzyskana w jednostce akredytowanej przez CQI & IRCA),Wymagana jest również znajomość norm ISO z serii 223xx, 24xxx, 27xxx, 29xxx, 31xxx, |