**Or.SO.2713.7.2022 Załącznik nr 4**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przeprowadzenie diagnozy cyberbezpieczeństwa zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego „Cyfrowa Gmina”.
	1. Spełnienia wymagań KRI:
		* Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
		* Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
		* Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
		* Aktualizowanie regulacji wewnętrznych,
		* Inwentaryzacja sprzętu i oprogramowania,
		* Przeprowadzanie okresowych analiz ryzyka,
		* Postępowanie z ryzykiem,
		* Zarządzanie uprawnieniami,
		* Szkolenia i uświadamianie,
		* Monitorowanie dostępu do informacji,
		* Monitorowanie nieautoryzowanych zmian,
		* Zabezpieczenie nieautoryzowanego dostępu,
		* Ustanowienie zasad bezpiecznej pracy mobilnej,
		* Zabezpieczenie informacji przed nieuprawnionym ujawnieniem,
		* Zabezpieczenie informacji przed nieuprawnioną modyfikacją,
		* Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem,
		* Zawieranie w umowach serwisowych zapisów o bezpieczeństwie,
		* Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania,
		* Aktualizowanie oprogramowania,
		* Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu,
		* Ochrona systemu przed błędami,
		* Stosowanie mechanizmów kryptograficznych w systemach,
		* Zapewnienie bezpieczeństwa plików systemowych,
		* Zarządzanie podatnościami systemów,
		* Kontrola zgodności systemów z regulacjami,
		* Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok.
2. Ocena wybranych aspektów bezpieczeństwa systemów informatycznych, o których mówi Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz. 1560):
	1. Dokumentacji potwierdzającej wykonanie działań wskazanych w ustawie, jak:
		* Identyfikacja usług publicznych, których świadczenie zależy od bezpieczeństwa systemów informatycznych
		* Wskazanie podmiotów odpowiedzialnych za zarządzanie incydentami
		* Publikowanie informacji na temat zagrożeń cyberbezpieczeństwa
		* Zgłoszenie osoby kontaktowej do CSIRT
	2. Opisu identyfikacji systemów informacyjnych wspierających zadania publiczne:
		* Inwentaryzacji składowych systemu
		* Aktualności listy osób odpowiedzialnych za eksploatację systemu
	3. Dokumentacji Systemu Informacyjnego wspierającego zadania publiczne:
		* Raportów z audytów systemów informacyjnych
		* Działań w kierunku szacowania ryzyka
		* Dokumentacji architektury zastosowanych zabezpieczeń
		* Dokumentacji architektury sieci
		* Dokumentacji zmian w systemach informacyjnych
		* Istnienia bazy danych konfiguracji urządzeń aktywnych
		* Dokumentacji monitorowania w trybie ciągłym
		* Dostępności umów z dostawcami (wsparcia technicznego, audytów teleinformatycznych) oraz wyników z audytów
		* Dostępności aktualnej dokumentacji zabezpieczeń fizycznych i środowiskowych
		* Prowadzenia rejestru dostępu do dokumentacji
	4. Dokumentacji procesu zarządzania incydentami:
		* Wdrożenia monitorowania i wykrywania incydentów
		* Istnienia procedury informowania o wykrytych incydentach
		* Istnienia procedury reagowania na incydenty
	5. Weryfikacji aspektów technicznych:
		* Wyników audytu serwisów WWW z uwzględnieniem: wersji serwera http, wersji systemu CMS, bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.), dostępność kompetentnego personelu do utrzymania serwisów.
		* Wyników audytu serwisów pocztowych z uwzględnieniem: poprawności wdrożenia mechanizmów SPF, DKIM i DMARC, poprawności i bezpieczeństwa wdrożenia mechanizmów TLS, dostępności kompetentnego personelu do utrzymania serwisów
		* Wyników audytu lokalnych sieci teleinformatycznych z uwzględnieniem: stosowania mechanizmów segmentacji sieci, izolacji urządzeń końcowych użytkowników, procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji, monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa, dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.
		* Wyników audytu połączenia z siecią Internet z uwzględnieniem: monitorowania ruchu wchodzącego i wychodzącego, stosowanych zabezpieczeń przed atakami DDoS, stosowanych zabezpieczeń przed wyciekiem informacji (DLP), stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.), dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.
	6. Weryfikacji aspektów organizacyjnych:
		* Wyników audytu organizacji zarządzania bezpieczeństwem teleinformatycznym
		z uwzględnieniem: regularnego identyfikowania znanych podatności
		w eksploatowanych systemach IT, terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników, prowadzenia okresowego przeglądu uprawnień użytkowników, prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.
		* Wyników audytu procesów planowania z uwzględnieniem: posiadania planów przywracania usług IT na wypadek awarii, prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT, cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.
3. Wykonanie i przekazanie Raportu z Diagnozy w postaci wypełnienia Arkusza do oceny JST (załącznika nr 8 Konkursu), w tym:
	1. Opisu zakresu przeprowadzonych prac audytowych,
	2. Analizy informacji zebranych podczas audytów,
	3. Wniosków i zaleceń związanych z rozwiązaniem występujących problemów.
4. Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej
	1. Testy styku sieci lokalnej z Internetem przeprowadzane ze stacji roboczej podłączonej do sieci Internet
		* Analiza topologii brzegu sieci,
		* Weryfikacja mechanizmów ochronnych,
		* Próba wykrycia usług sieciowych udostępnianych do Internetu,
		* Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet,
		* Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet,
		* Przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią Internet.
	2. Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji
		* Analiza topologii sieci LAN,
		* Weryfikacja mechanizmów ochronnych w sieci,
		* Analiza komunikacji sieciowej,
		* Skanowanie portów TCP/UDP próba wykrycia usług sieciowych,
		* Skanowanie hostów aktywnych w sieci,
		* Exploitacja dostępnych urządzeń oraz usług w sieci LAN,
		* Przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN.
5. Wykonanie i przekazanie raportu z testów
	1. Opis zakresu przeprowadzonych prac audytowych,
	2. Analizę informacji zebranych podczas audytów,
	3. Wnioski i zalecenia związane z rozwiązaniem występujących problemów.
6. Szkolenie pracowników w zakresie cyberbezpieczeństwa:
	1. Wprowadzenie do bezpieczeństwa informacji w oparciu o Normę ISO/IEC 27001:2017
	2. Przepisy regulujące ochronę danych: RODO i Ustawa o ochronie danych osobowych
	3. Ustawa o krajowym systemie cyberbezpieczeństwa i podstawowe definicje
	4. Podział ról i obowiązków wynikających z przepisów prawa
	5. Praktyczne zasady zapewniania bezpieczeństwa informacji
		* 1. Kontrola dostępu fizycznego, zarządzanie kluczami
			2. Zasady bezpiecznej eksploatacji sprzętu i oprogramowania
			3. Zasada czystego biurka i czystego pulpitu
	6. Cyberbezpieczeństwo w praktyce
		* 1. Informacje uwierzytelniające
			2. Korzystanie z Internetu i poczty elektronicznej
			3. Ataki socjotechniczne
	7. Postępowanie z naruszeniami bezpieczeństwa informacji

Skutki naruszeń i konsekwencje prawne