Załącznik nr 1 do umowy nr ____/__/2026

Zakres audytu zgodności z UoKSC/NIS2:

1. **Audyt organizacyjny**

   - ✓ Regulacje w obszarze zarządzania bezpieczeństwem informacji,
   - ✓ Odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji.

2. **Audyt fizyczny i środowiskowy**

   - ✓ Weryfikacja granic obszaru bezpiecznego,
   - ✓ Weryfikacja zabezpieczeń wejścia/wyjścia,
   - ✓ Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
   - ✓ Weryfikacja bezpieczeństwa okablowania strukturalnego.

3. **Audyt teleinformatyczny**

   - ✓ Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
   - ✓ Przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania ciągłości działania,
   - ✓ Weryfikacja ochrony przed oprogramowaniem szkodliwym,
   - ✓ Weryfikacja procedur zarządzania kopiami zapasowymi,
   - ✓ Weryfikacja procedur związanych z rejestracją błędów,
   - ✓ Weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
   - ✓ Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
   - ✓ Weryfikacja zabezpieczeń nośników wymiennych,
   - ✓ Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania).

4. **Sporządzenie raportów odnośnie:**

   - ✓ spełniania wymagań poszczególnych 3 obszarów

Zakres testów penetracyjnych

Weryfikacja dokumentacji oraz procedur:

- ✓ Zapoznanie się i ocena istniejącej dokumentacji infrastruktury IT w penetrowanej organizacji,
- ✓ Weryfikacja zapisów w umowach usług outsourcingowych.

Skanowanie oraz ataki penetracyjne wewnętrzne:

- ✓ Weryfikacja aktualności oprogramowania, poprawek krytycznych systemów informatycznych oraz aplikacji,
- ✓ Analiza podatności urządzeń w infrastrukturze sieciowej,
- ✓ Sprawdzenie działania systemów ochrony antywirusowej,
- ✓ Szereg ataków na wybrane hosty,
- ✓ Podsłuch aktywny i pasywny sieci komputerowej,
- ✓ Weryfikacja zabezpieczeń baz danych w penetrowanej organizacji,
- ✓ Skanowanie listy otwartych portów na urządzeniach sieciowych,
- ✓ Sprawdzenie poziomu zabezpieczeń przed dostępem dla urządzeń nieautoryzowanych.

Skanowanie oraz ataki penetracyjne zewnętrzne:

- ✓ Testowanie wybranych aplikacji WWW,
- ✓ Zewnętrzne badanie infrastruktury (np. serwera www, serwera aplikacyjnego),
- ✓ Zewnętrzne badanie poziomu bezpieczeństwa sieci (badanie szczelności systemu firewall, sprawdzanie dostępności i typu usług sieciowych),
- ✓ Próby detekcji wykorzystanego oprogramowania,
- ✓ Ukierunkowane ataki na zewnętrzne usługi (detekcja błędów klasy: SQL injection, XSS, Authorization Bypass, DoS, itd.),
- ✓ Badanie obecności i konfiguracji protokołu szyfrującego HTTPS oraz DNS,
- ✓ Analiza poczty elektronicznej (Platforma, zarządzanie kontami, bezpieczeństwo, poufność, ocena ruchu sieciowego – po uprzedniej zgodzie dostawcy zewnętrznego).

Zakres działań socjotechnicznych

- ✓ Badanie uzyskania poufnych informacji od użytkowników – bezpośrednie, mailowe, telefoniczne,
- ✓ Próby umieszczenia szkodliwego oprogramowania na stacjach roboczych,
- ✓ Symulacje uzyskania dostępu do danych poufnych u użytkowników,
- ✓ Weryfikację sposobu przechowywania haseł przez użytkowników, polityki czystego biurka i czystego ekranu,
- ✓ Sprawdzenie ochrony powierzonego sprzętu i dokumentacji,
- ✓ Próby nakłonienia pracowników do wykonania działań potencjalnie niebezpiecznych,
- ✓ Kontrolę skuteczności przyjętych procedur bezpieczeństwa, ich znajomości przez pracowników i stosowania się do nich,
- ✓ Przegląd zabezpieczeń dot. bezpieczeństwa fizycznego.

Zakres audytu ciągłości działania

1. Ocena i weryfikacja polityka ciągłości działania (ocena skuteczności) ISO 22300
2. „Zrozumienia organizacji" – przegląd analiz:
   - ✓ Analizy wpływu na biznes (Business Impact Analysis: BIA)
   - ✓ Analizy Ryzyka (Risk Analysis: RA)
3. Ocena zorganizowania Systemu Zarządzania Ciągłością Działania:
   - ✓ Podziału obowiązków
   - ✓ Zespołu ds. ciągłości działania
   - ✓ Struktury zarządzania kryzysowego
4. Ocena procesu identyfikacji kluczowych i niekluczowych procesów biznesowych
   - ✓ Weryfikacja przyjętych:
   - ✓ RTO (recovery time objective) – czasu w jakim należy przywrócić (wznowić) proces po wystąpieniu awarii
   - ✓ RPO (recovery point objective) – akceptowalny poziom utraty danych wyrażony w czasie
   - ✓ i weryfikacja analiza rozbieżności
5. Przegląd i weryfikacja strategii zachowania ciągłości działania:
   - ✓ Weryfikacja przyjętych scenariuszy
   - ✓ Weryfikacja minimalnych zasobów niezbędnych do realizacji procesów na wcześniej zdefiniowanym poziomie
6. Przegląd i ocena Planu (planów) ciągłości działania, procedur awaryjnych i odtworzeniowych
7. Ocena ciągłości działania w kontekście outsourcowanych procesów
8. Ocena efektywność Systemu Zarządzania Ciągłością Działania
   - ✓ Testy (praktyczne testy w Centrali oraz ośrodku zapasowym)
   - ✓ Aktualizacja planów (Przegląd zarządzania)
   - ✓ Uświadamianie oraz szkolenia
9. Przegląd procesu tworzenia i odzyskiwania kopii zapasowych
10. Ocena wyposażenia serwerowni w lokalizacji podstawowej i zapasowej
11. Działania korygujące oraz podsumowanie
12. Harmonogram działań oraz ocena działań

Zakres audytu podatności stron WWW

- ✓ Weryfikacja aktualizacji oprogramowania używanego w ramach działania stron www
- ✓ Weryfikacja stosowania i aktualności certyfikatów SSL
- ✓ Weryfikacja błędów konfiguracji aplikacji lub serwerów pod kątem dostępu do danych sesji
- ✓ Weryfikacja dostępu do archiwalnych wersji stron www
- ✓ Weryfikacja udostępniania stron testowych
- ✓ Weryfikacja dostępu do paneli administracyjnych CMS
- ✓ Weryfikacja dostępu do paneli administracyjnych urządzeń sieciowych oraz innych elementów infrastruktury zlokalizowanej na styku z siecią WAN
- ✓ Weryfikacja MFA (weryfikacji wieloetapowej) do paneli administracyjnych
- ✓ Weryfikacja pomocy zdalnej dla klientów

Zakres aktualizacji dokumentacji SZBI zgodnie z wymaganiami NIS 2:

- ✓ organizacja systemu bezpieczeństwa informacji;
- ✓ zarządzanie aktywami;
- ✓ zarządzanie zasobami ludzkimi;
- ✓ organizacja bezpieczeństwa fizycznego i środowiskowego;
- ✓ zarządzanie komunikacją i eksploatacją;
- ✓ rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania;
- ✓ kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
- ✓ akwizycja, rozwój i utrzymanie systemu;
- ✓ zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- ✓ zarządzanie ciągłością działania;
- ✓ zarządzania kopiami zapasowymi;
- ✓ zarządzania monitoringiem;
- ✓ zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
- ✓ używania urządzeń komputerowych;
- ✓ metoda szacowania i postępowania z ryzykiem;

Program szkolenia dla managerów:

- ✓ Wprowadzenie do cyberbezpieczeństwa. Zarządzanie bezpieczeństwem informacji.
- ✓ Znaczenie procedur cyberbezpieczeństwa w instytucji publicznej. Otoczenie prawne cyberbezpieczeństwa jednostek sektora publicznego.
- ✓ Odpowiedzialność za naruszenie procedur cyberbezpieczeństwa.
- ✓ Ochrona komputera. Podstawowe zasady, filary bezpieczeństwa. Antywirus, aktualizacje, zapora sieciowa, kopie zapasowe, szyfrowanie danych.
- ✓ Bezpieczeństwo fizyczne obiektu, urządzeń oraz pracowników. Kontrola dostępu.
- ✓
- ✓ Weryfikacja osób. Zasada czystego biurka.
- ✓ Socjotechnika - manipulacja użytkownikiem. Jakie błędy popełniają pracownicy?
- ✓
- ✓ Omówienie prawdziwych zdarzeń.
- ✓ Zarządzanie dostępem. Bezpieczeństwo haseł. Zasady, analiza, metody tworzenia, menager haseł, dwuskładnikowe uwierzytelnianie.
- ✓ Wycieki danych. Minimalizacja ryzyka. Identyfikacja zagrożeń.
- ✓ Cyberzagrożenia. Świadomość pracowników oraz ich edukacja.
- ✓ Omówienie popularnych ataków cybernetycznych z zakresu mailingu (phishing), SMS-ów (smishing), kontaktów telefonicznych (vishing), komunikatorów internetowych, portali społecznościowych.
- ✓ Okresowe przeglądy/audyty cyberbezpieczeństwa, testy penetracyjne oraz socjotechniczne – zaplanowanie regularności przeglądów.
- ✓ Coroczna analiza incydentów na podstawie okresowych przeglądów jak i wykrytych przez systemy teleinformatyczne

- ✓
- ✓ Coroczna aktualizacja dokumentacji SZBI w oparciu o analizę incydentów
- ✓ Przegląd procedur zgłaszania incydentów – system S46
- ✓ Znajomość zasad ciągłości działania wg normy ISO/IEC-22301 w odniesieniu do możliwości i aktualnych zasobów urzędu
- ✓ Kontrole rejestrów analiz ryzyka dostawców (wymaganie deklaracji stosowania zabezpieczeń, aktualizacja ankiet analiz ryzyka, audyt dostawców kluczowych)
- ✓ Kontrole rejestru przydzielania uprawnień i ich odbierania
- ✓ Procedury zapoznawania pracowników z zasadami bezpieczeństwa danych i egzekwowanie ich przestrzegania.
- ✓ Cyberbezpieczeństwo – cykl zamkniętego koła – stały monitoring, analiza, wnioski, wdrażanie, ewaluacja.
- ✓ Procedury powołania ASI, zgłoszenia do NASK oraz współpracy z sektorowym CSIRT.
- ✓ Korekty systemów SIEM i SOAR oraz EDR/XDR w kontekście zbierania i analizy logów wewnętrznych (licencje opensource, onpremis, SOC)
- ✓ Analiza procedur do procesów sieciowych, jako systemów krytycznych
- ✓ Planowanie wydatków w odniesieniu do art. 21 dyrektywy NIS2 w zakresie rocznych budżetów na podnoszenie cyberbezpieczeństwa.
- ✓ Analiza funkcjonowania procesów i procedur zawartych w dokumentacji SZBI w odniesieniu do stanu faktycznego