Załącznik nr 1 do zapytania ofertowego

znak BUA.271.65.2025 z dnia 17 listopada 2025 r.

**Opis Przedmiotu Zamówienia**

**(OPZ)**

dla postępowania pn.

**Przeprowadzenie szkoleń, aktualizacji SZBI oraz audytu w ramach realizacji projektu Cyberbezpieczny Samorząd**

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego (EFRR) oraz Budżetu Państwa w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Konkurs grantowy pn. „Cyberbezpieczny Samorząd” nr FERC.02.02-CS.01-001/23

Spis treści

[1. Szkolenie dla pracowników UG i GOPS z zakresu Cyberbezpieczeństwa 3](#_Toc212637062)

[2. Szkolenie dla Kadry Zarządczej, Inspektora IODO oraz Informatyka UG i GOPS z zakresu Cyberbezpieczeństwa. 6](#_Toc212637063)

[3. Przegląd i aktualizacja SZBI dla UG 9](#_Toc212637064)

[4. Przegląd i aktualizacja SZBI dla GOPS 12](#_Toc212637065)

[5. Audyt KRI dla UG i GOPS 15](#_Toc212637066)

# Szkolenie dla pracowników UG i GOPS z zakresu cyberbezpieczeństwa

| **Parametr** | **Charakterystyka (wymagania minimalne) - Szkolenie dla pracowników UG i GOPS** |
| --- | --- |
| **Platforma szkoleniowa** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Wykonawca zapewni dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń internetowych. 2. Symulator musi być  narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie. Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane). W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing’u w  różnych odsłonach, (Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat). 3. Wykonawca zobowiązany jest przekazać zamawiającemu dostęp do platformy na minimum 30 dni od daty szkolenia, wraz z instrukcją obsługi. 4. Wymagania szczegółowe dla platformy symulującej zagrożenia internetowe:    1. Moduł podstron (fałszywych witryn) – moduł ten będzie umożliwiał tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania zainfekowanych załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych.    2. Moduł  czatu – w module tym zaimplementowany zostanie czat z botami, namawiającymi do zakupów różnych produktów powodując wyłudzenie danych osobowych, numerów kart kredytowych itp. Itd. W module tym zostaną zaimplementowane opracowane scenariusze    3. Moduł e-mail – w module tym użytkownik będzie miał do przeglądnięcia kilka wiadomości e-mail przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego” na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład.    4. Moduł edukacyjny – moduł zawierający szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware.       1. Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze. 5. Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail. 6. Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie. 7. Moduł postów społecznościowych, zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste” posty niestanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem. |
| **Zakres szkolenia** | 1. Szkolenie powinno obejmować następujące moduły tematyczne:    1. ***Podstawy prawne i kontekst regulacyjny***       1. Omówieni*e* aktualnych regulacji prawnych dotyczących bezpieczeństwa informacji;       2. *Wskazanie* obowiązków i odpowiedzialności pracowników oraz kadry kierowniczej w kontekście przepisów krajowych i unijnych, w tym m.in. aktów implementujących wymagania NIS 2;       3. Zarządzanie ryzykiem – identyfikacja obszarów ryzyka oraz sposoby jego ograniczania.    2. ***Świadomość zagrożeń i cyberodporność***       1. Charakterystyka współczesnych zagrożeń w cyberprzestrzeni;       2. Omówienie tzw. triady bezpieczeństwa (Poufność – Integralność – Dostępność);       3. Przykłady najczęściej występujących zagrożeń: ataki socjotechniczne, phishing, malware, ransomware, itd.    3. ***Zasady bezpiecznego korzystania z zasobów informacyjnych***       1. Wskazanie aktywów wymagających ochrony (dane, urządzenia, systemy);       2. Rola kontroli dostępu i polityki haseł (zasady tworzenia i przechowywania silnych haseł);       3. Bezpieczeństwo komunikacji: ochrona korespondencji e-mail, komunikatorów, praca zdalna;       4. Zabezpieczenia urządzeń końcowych: szyfrowanie danych, kopie zapasowe, separacja środowisk;       5. Zasady bezpiecznej pracy zdalnej;       6. Wprowadzenie do zagrożeń wynikających z błędów ludzkich – przykłady incydentów z użyciem metod socjotechnicznych.    4. ***Zarządzanie incydentami bezpieczeństwa***       1. Przygotowanie organizacji na wystąpienie incydentu – rola planów i procedur;   Zasady postępowania w przypadku incydentu: wykrycie, reakcja, zgłoszenie, dokumentacja.   1. **Liczba uczestników**: ok. 30 osób. (dwie grupy uczestników po około 15 osób) 2. **Czas trwania szkolenia**: 16 godzin zegarowych (po 8 godzin szkolenia dla jednej grupy). 3. **Forma szkolenia**: stacjonarna (z możliwością zdalnego uczestnictwa w szkoleniu). 4. Zaświadczenia: po zakończeniu szkolenia, każdy uczestnik otrzyma imienne zaświadczenie potwierdzające udział. 5. **Zakres materiałów**: Wykonawca zapewni materiały szkoleniowe (drukowane lub elektroniczne). 6. **Wymagania wobec Wykonawcy**    1. Doświadczenie w przeprowadzeniu co najmniej 2 szkoleń dla jednostek sektora publicznego w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa  w okresie ostatnich 3 lat przed upływem składania ofert;    2. Znajomość obowiązujących regulacji (w szczególności w zakresie ochrony danych osobowych, KRI, KSC, NIS 2);    3. Zespół prowadzący szkolenie powinien posiadać kompetencje z zakresu:       1. *prawa* ochrony danych osobowych,       2. *zarządzania* bezpieczeństwem informacji,       3. *praktycznego* wdrażania systemów zgodnych z ISO/IEC 27001,       4. *reagowania* na incydenty bezpieczeństwa informacji;    4. Możliwość przedstawienia referencji potwierdzających realizację podobnych usług. |

# Szkolenie dla kadry zarządczej, inspektora ODO oraz informatyka UG i GOPS z zakresu Cyberbezpieczeństwa

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne) - Szkolenie dla kadry zarządczej, inspektora ODO oraz informatyka UG i GOPS** |
| **Platforma szkoleniowa** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Wykonawca zapewni dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń internetowych. Symulator musi być  narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie. Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane). W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing’u w  różnych odsłonach, (Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat). Wykonawca zobowiązany jest przekazać zamawiającemu dostęp do platformy na minimum 30 dni od daty szkolenia, wraz z instrukcją obsługi. 2. Wymagania szczegółowe dla platformy symulującej zagrożenia internetowe:    1. Moduł podstron (fałszywych witryn) – moduł ten będzie umożliwiał tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania zainfekowanych załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych.    2. Moduł  czatu – w module tym zaimplementowany zostanie czat z botami, namawiającymi do zakupów różnych produktów powodując wyłudzenie danych osobowych, numerów kart kredytowych itp. Itd. W module tym zostaną zaimplementowane opracowane scenariusze    3. Moduł e-mail – w module tym użytkownik będzie miał do przeglądnięcia kilka wiadomości e-mail przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego” na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład.    4. Moduł edukacyjny – moduł zawierający szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware.       1. Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze.    5. Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail.    6. Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie.    7. Moduł postów społecznościowych, zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste” posty nie stanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem. |
| **Zakres szkolenia** | 1. **Otoczenie prawne i obowiązki kadry kierowniczej**    1. Aktualne wymogi prawne w zakresie bezpieczeństwa informacji (KRI, KSC, RODO po wdrożeniu Dyrektywy NIS 2);    2. Zakres odpowiedzialności kierownictwa w kontekście organizacyjnego nadzoru nad bezpieczeństwem informacji;    3. Kluczowe obowiązki formalne i praktyczne związane z zapewnieniem zgodności organizacji z przepisami;    4. Wprowadzenie do systemowego zarządzania ryzykiem informacyjnym. 2. **Strategiczna świadomość zagrożeń – cyberodporność organizacyjna**    1. Charakterystyka współczesnych zagrożeń dla administracji publicznej;    2. Cyberbezpieczeństwo jako element ładu organizacyjnego i odporności na zakłócenia;    3. Triada bezpieczeństwa (Poufność – Integralność – Dostępność) w zarządzaniu instytucją;    4. Najczęstsze scenariusze zagrożeń oraz ich wpływ na działalność urzędu. 3. **Zasady organizacyjnego bezpieczeństwa**    1. Wskazanie kluczowych zasobów (aktywa, dane, systemy, kadra);    2. Nadzór nad kontrolą dostępu oraz polityką haseł w organizacji;    3. Rola kadry kierowniczej w nadzorze nad bezpieczeństwem komunikacji i pracy zdalnej;    4. Bezpieczeństwo urządzeń końcowych i danych urzędowych;    5. Znaczenie kultury organizacyjnej i świadomości pracowników w budowaniu cyberodporności. 4. **Zarządzanie incydentami i ciągłość działania**    1. Odpowiedzialność zarządcza w planowaniu reakcji na incydenty;    2. Nadzór nad wdrażaniem i stosowaniem procedur reagowania na incydenty;    3. Znaczenie rejestrowania incydentów i ich analiza jako element procesu doskonalenia bezpieczeństwa;    4. Minimalizowanie skutków zdarzeń – podejście zarządcze do ciągłości działania. 5. **Warunki realizacji**    1. **Grupa docelowa**: kadra zarządzająca (około 8 osób).    2. **Czas trwania szkolenia**: 2 godziny zegarowe.    3. **Forma szkolenia**: stacjonarna (z możliwością zdalnego uczestnictwa w szkoleniu).    4. **Potwierdzenie uczestnictwa**: imienne zaświadczenia dla każdego uczestnika.    5. **Materiały szkoleniowe**: zapewnione przez Wykonawcę w formie drukowanej lub elektronicznej. 6. **Wymagania wobec Wykonawcy**    1. Doświadczenie w prowadzeniu szkoleń dla kadry kierowniczej jednostek sektora publicznego;    2. Znajomość praktycznych aspektów realizacji wymogów prawnych w administracji publicznej (w tym RODO, KSC, KRI, NIS 2);    3. Kompetencje zespołu prowadzącego szkolenie w zakresie zarządzania bezpieczeństwem informacji, audytu, analizy ryzyka oraz reagowania na incydenty;    4. Możliwość przedstawienia referencji poświadczających realizację podobnych szkoleń. |

# Przegląd i aktualizacja SZBI dla UG

1. **Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001:2022 z 25 października 2022 roku.**
2. ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie „Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych” w §20 „System zarządzania bezpieczeństwem informacji” (SZBI) zobowiązuje instytucje publiczne do opracowania strategii działania SZBI rozumianej jako zespół dobrych praktyk, mających na celu dbałość o bezpieczeństwo informacji w Gminie. Podejście bazuje na szacowaniu ryzyka i poziomach akceptacji ryzyka dla organizacji zaprojektowanych, tak aby skutecznie postępować i zarządzać ryzykiem. Na SZBI składają się: polityka, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. Wymagane jest zapewnienie poufności, integralności i dostępności informacji. Wymagania minimalne dla dokumentacji SZBI:
   1. Procedury operacyjne
      1. Procedura identyfikacji zagrożeń i oceny ryzyka
      2. Procedura zarządzania ryzykiem
      3. Procedura nadzorowania systemu informacji
      4. Procedura zarządzania dostępem
      5. Procedura zarządzania incydentami bezpieczeństwa informacji
      6. Procedura monitorowania i audytu
      7. Procedura zarządzania zmianami
      8. Procedura zarządzania dostawcami
      9. Procedura zarządzania ciągłością działania
      10. Procedura zarządzania szkoleniami i świadomością
   2. Instrukcje operacyjne
      1. Instrukcja tworzenia haseł
      2. Instrukcja obsługi systemów bezpieczeństwa
      3. Instrukcja obsługi narzędzi monitorujących
      4. Instrukcja obsługi procedury audytu
      5. Instrukcja obsługi systemu raportowania incydentów
      6. Instrukcja obsługi narzędzi zarządzania ryzykiem
      7. Instrukcja obsługi systemu zarządzania dokumentacją
   3. Instrukcje techniczne
      1. Instrukcja konfiguracji oprogramowania antywirusowego
      2. Instrukcja konfiguracji zapór sieciowych
      3. Instrukcja konfiguracji systemów monitorowania
      4. Instrukcja konfiguracji narzędzi szyfrowania danych
      5. Instrukcja konfiguracji systemów uwierzytelniania
   4. Plany i strategie
      1. Plan zarządzania incydentami
      2. Plan ciągłości działania
      3. Strategia zapewnienia bezpieczeństwa fizycznego
      4. Strategia monitorowania i audytu
      5. Strategia zarządzania zmianami
      6. Strategia zarządzania dostawcami
      7. Strategia zarządzania ryzykiem
      8. Strategia zarządzania dostępem
      9. Strategia zarządzania szkoleniami i świadomością
   5. Rejestr dokumentów i rejestr zabezpieczeń
   6. Raporty i dokumentacja audytowa
   7. Procesy certyfikacji i dokumentacja związana z audytem certyfikującym
   8. Schemat organizacyjny i uprawnienia w zakresie zarządzania SZBI
   9. Plan komunikacji wewnętrznej w zakresie SZBI
   10. Dokumentacja związana z wdrożeniem systemu zarządzania SZBI
   11. Procesy kontrolne i monitorujące związane z dokumentacją SZBI
   12. Dokumentacja szkoleń pracowników w zakresie SZBI
   13. Ewidencja incydentów bezpieczeństwa informacji
   14. Zasoby związane z audytem wewnętrznym i zewnętrznym
   15. Procedury dokumentacji zmian w systemie zarządzania SZBI
   16. Mapy procesów w zakresie zarządzania bezpieczeństwem informacji
   17. Procedury oceny zgodności z wymaganiami normy ISO 27001
   18. Dokumentacja dotycząca ewaluacji efektywności systemu zarządzania SZBI
   19. Dokumentacja dotycząca audytu wewnętrznego
   20. Raporty dotyczące wyników audytów i przeglądów SZBI
   21. Dokumentacja dotycząca działań korygujących i zapobiegawczych
   22. Procedury dokumentacji usuwania danych i aktywów
   23. Instrukcje dotyczące kierowania wypadkami i awariami
   24. Procedury dokumentacji zarządzania systemami monitoringu i wykrywania zagrożeń
   25. Procedury dokumentacji zarządzania zasobami ludzkimi w kontekście bezpieczeństwa informacji
   26. Dokumentacja dotycząca zarządzania incydentami związanymi z ochroną danych osobowych (RODO/GDPR)
   27. Instrukcje dotyczące dokumentacji zarządzania systemami kontroli dostępu fizycznego
   28. Procedury dokumentacji zarządzania uprawnieniami i kontrolą dostępu do systemów informatycznych
   29. Dokumentacja dotycząca planowania i wdrażania systemów monitorowania i reagowania na incydenty cybernetyczne
   30. Instrukcje dotyczące dokumentacji zarządzania zgodnością z wymaganiami regulacji branżowych i prawnych
   31. Procedury dokumentacji zarządzania zewnętrznymi dostawcami usług IT i infrastruktury
   32. Dokumentacja dotycząca zarządzania ryzykiem dla projektów IT i procesów biznesowych
   33. Instrukcje dotyczące dokumentacji przeglądów i ocen skuteczności systemu zarządzania bezpieczeństwem informacji
   34. Procedury dokumentacji zarządzania konfiguracją systemów informatycznych i aplikacji
   35. Dokumentacja dotycząca zarządzania reputacją i wizerunkiem firmy w kontekście bezpieczeństwa informacji
   36. Instrukcje dotyczące dokumentacji zarządzania monitorowaniem i analizą zagrożeń informacyjnych
   37. Procedury dokumentacji zarządzania testami penetracyjnymi i oceną podatności systemów informatycznych.
   38. Aktualizację dokumentacji przeprowadzi audytor wiodący legitymujący się ważnymi certyfikatami:
       1. System Zarządzania Ciągłością Działania wg normy PN-EN ISO 22301
       2. System Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001
   39. Wykonawca przedstawi ważne certyfikaty audytora na żądanie Zamawiającego.

# Przegląd i aktualizacja SZBI dla GOPS

1. **Aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001:2022 z 25 października 2022 roku.**
2. ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie „Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych” w §20 „System zarządzania bezpieczeństwem informacji” (SZBI) zobowiązuje instytucje publiczne do opracowania strategii działania SZBI rozumianej jako zespół dobrych praktyk, mających na celu dbałość o bezpieczeństwo informacji w Gminie. Podejście bazuje na szacowaniu ryzyka  i poziomach akceptacji ryzyka dla organizacji zaprojektowanych, tak aby skutecznie postępować i zarządzać ryzykiem. Na SZBI składają się: polityka, procedury, wytyczne, związane zasoby i działania, wspólnie zarządzane przez organizację dążącą do ochrony jej aktywów informacyjnych. Wymagane jest zapewnienie poufności, integralności i dostępności informacji. Wymagania minimalne dla dokumentacji SZBI:
   1. Procedury operacyjne
      1. Procedura identyfikacji zagrożeń i oceny ryzyka
      2. Procedura zarządzania ryzykiem
      3. Procedura nadzorowania systemu informacji
      4. Procedura zarządzania dostępem
      5. Procedura zarządzania incydentami bezpieczeństwa informacji
      6. Procedura monitorowania i audytu
      7. Procedura zarządzania zmianami
      8. Procedura zarządzania dostawcami
      9. Procedura zarządzania ciągłością działania
      10. Procedura zarządzania szkoleniami i świadomością
   2. Instrukcje operacyjne
      1. Instrukcja tworzenia haseł
      2. Instrukcja obsługi systemów bezpieczeństwa
      3. Instrukcja obsługi narzędzi monitorujących
      4. Instrukcja obsługi procedury audytu
      5. Instrukcja obsługi systemu raportowania incydentów
      6. Instrukcja obsługi narzędzi zarządzania ryzykiem
      7. Instrukcja obsługi systemu zarządzania dokumentacją
   3. Instrukcje techniczne
      1. Instrukcja konfiguracji oprogramowania antywirusowego
      2. Instrukcja konfiguracji zapór sieciowych
      3. Instrukcja konfiguracji systemów monitorowania
      4. Instrukcja konfiguracji narzędzi szyfrowania danych
      5. Instrukcja konfiguracji systemów uwierzytelniania
   4. Plany i strategie
      1. Plan zarządzania incydentami
      2. Plan ciągłości działania
      3. Strategia zapewnienia bezpieczeństwa fizycznego
      4. Strategia monitorowania i audytu
      5. Strategia zarządzania zmianami
      6. Strategia zarządzania dostawcami
      7. Strategia zarządzania ryzykiem
      8. Strategia zarządzania dostępem
      9. Strategia zarządzania szkoleniami i świadomością
   5. Rejestr dokumentów i rejestr zabezpieczeń
   6. Raporty i dokumentacja audytowa
   7. Procesy certyfikacji i dokumentacja związana z audytem certyfikującym
   8. Schemat organizacyjny i uprawnienia w zakresie zarządzania SZBI
   9. Plan komunikacji wewnętrznej w zakresie SZBI
   10. Dokumentacja związana z wdrożeniem systemu zarządzania SZBI
   11. Procesy kontrolne i monitorujące związane z dokumentacją SZBI
   12. Dokumentacja szkoleń pracowników w zakresie SZBI
   13. Ewidencja incydentów bezpieczeństwa informacji
   14. Zasoby związane z audytem wewnętrznym i zewnętrznym
   15. Procedury dokumentacji zmian w systemie zarządzania SZBI
   16. Mapy procesów w zakresie zarządzania bezpieczeństwem informacji
   17. Procedury oceny zgodności z wymaganiami normy ISO 27001
   18. Dokumentacja dotycząca ewaluacji efektywności systemu zarządzania SZBI
   19. Dokumentacja dotycząca audytu wewnętrznego
   20. Raporty dotyczące wyników audytów i przeglądów SZBI
   21. Dokumentacja dotycząca działań korygujących i zapobiegawczych
   22. Procedury dokumentacji usuwania danych i aktywów
   23. Instrukcje dotyczące kierowania wypadkami i awariami
   24. Procedury dokumentacji zarządzania systemami monitoringu i wykrywania zagrożeń
   25. Procedury dokumentacji zarządzania zasobami ludzkimi w kontekście bezpieczeństwa informacji
   26. Dokumentacja dotycząca zarządzania incydentami związanymi z ochroną danych osobowych (RODO/GDPR)
   27. Instrukcje dotyczące dokumentacji zarządzania systemami kontroli dostępu fizycznego
   28. Procedury dokumentacji zarządzania uprawnieniami i kontrolą dostępu do systemów informatycznych
   29. Dokumentacja dotycząca planowania i wdrażania systemów monitorowania i reagowania na incydenty cybernetyczne
   30. Instrukcje dotyczące dokumentacji zarządzania zgodnością z wymaganiami regulacji branżowych i prawnych
   31. Procedury dokumentacji zarządzania zewnętrznymi dostawcami usług IT i infrastruktury
   32. Dokumentacja dotycząca zarządzania ryzykiem dla projektów IT i procesów biznesowych
   33. Instrukcje dotyczące dokumentacji przeglądów i ocen skuteczności systemu zarządzania bezpieczeństwem informacji
   34. Procedury dokumentacji zarządzania konfiguracją systemów informatycznych i aplikacji
   35. Dokumentacja dotycząca zarządzania reputacją i wizerunkiem firmy w kontekście bezpieczeństwa informacji
   36. Instrukcje dotyczące dokumentacji zarządzania monitorowaniem i analizą zagrożeń informacyjnych
   37. Procedury dokumentacji zarządzania testami penetracyjnymi i oceną podatności systemów informatycznych.
   38. Aktualizację dokumentacji przeprowadzi audytor wiodący legitymujący się ważnymi certyfikatami:
       1. System Zarządzania Ciągłością Działania wg normy PN-EN ISO 22301
       2. System Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001
   39. Wykonawca przedstawi ważne certyfikaty audytora na żądanie Zamawiającego.

# Audyt KRI dla UG i GOPS

Analiza stanu bezpieczeństwa użytkowanych systemów oraz wskazanie koniecznych działań, które zwiększą poziom bezpieczeństwa IT

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Zakres prac** | 1. Przeprowadzenie audytu bezpieczeństwa, którego celem jest ocena aktualnego – przed przystąpieniem do realizacji projektu - poziomu bezpieczeństwa teleinformatycznego. |
| **Cel audytu** | 1. Celem audytu jest przedstawienie szczegółowego obrazu obecnego stanu bezpieczeństwa organizacji, identyfikacja obszarów wymagających usprawnień. |
| **Wymagania dla jednostki przeprowadzającej audyt** | 1. Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w Ustawie z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560). |
| **Raport z  Audytu Bezpieczeństwa** | 1. Raport z audytu bezpieczeństwa zawiera szczegółowe wyniki analizy, identyfikację potencjalnych zagrożeń, rekomendacje dotyczące poprawy bezpieczeństwa, a także plan działania. 2. Raport stanowi Dokumentację Analizy Przedwdrożeniowej (DAP) opracowanej przez wykonawcę zakresu rzeczowego projektu i zatwierdzonej przez Zamawiającego. |

1. **Audyt bezpieczeństwa – końcowy**

Analiza poziomu bezpieczeństwa po zakończeniu projektu. Weryfikacja osiągnięcia założonych celów projektu.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Zakres prac** | 1. Przeprowadzenie audytu bezpieczeństwa, którego celem jest ocena poziomu bezpieczeństwa teleinformatycznego. |
| **Cel audytu** | 1. Celem audytu jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności zgodnie z projektem w obszarach wskazanych w poniższej tabeli w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa w formie ankiety. 2. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z wyników Audytu wstępnego (audyt „zerowy”)  lub jego brak. |
| **Obszary Audytu** | 1. Ocena skuteczności działania infrastruktury w zakresie:    1. urządzenia i konfiguracja w zakresie ochrony poczty,    2. urządzenia i konfiguracja w zakresie ochrony sieci,    3. urządzenia i konfiguracja w zakresie systemów serwerowych,    4. urządzenia i konfiguracja w zakresie stacji roboczych,    5. urządzenia i konfiguracja w zakresie systemów bezpieczeństwa. 2. Procesy zarządzania bezpieczeństwem informacji:    1. nośniki wymienne - udokumentowany sposób postępowania,    2. zarządzanie tożsamością/dostęp do systemów w zakresie: przydzielanie dostępu, odbieranie dostępu,    3. pomieszczenie/pomieszczenia w dyspozycji Zespołu IT 3. Monitorowanie i reagowanie na incydenty bezpieczeństwa:    1. procedury zarządzania incydentami,    2. raportowanie poziomów pokrycia scenariuszami znanych incydentów,    3. dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa,    4. monitorowanie i wykrycie incydentów bezpieczeństwa,    5. Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów. 4. Zarządzanie ciągłością działania:    1. konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa,    2. raport z przeglądów i testów odtwarzania kopii bezpieczeństwa,    3. procedury wykonywania i przechowywania kopii zapasowych,    4. strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP),    5. procedury utrzymaniowe. 5. Utrzymanie systemów informacyjnych:    1. harmonogramy skanowania podatności,    2. aktualny status realizacji postępowania z podatnościami,    3. procedury związane ze z identyfikowaniem (wykryciem) podatności,    4. współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami. 6. Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:    1. polityka bezpieczeństwa w relacjach z dostawcami,    2. standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa,    3. dostęp zdalny,    4. metody uwierzytelnienia. |
| **Wymagania dla jednostki przeprowadzającej audyt** | 1. Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w Ustawie z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560). 2. Audyt bezpieczeństwa może być przeprowadzony przez:    1. jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;    2. co najmniej dwóch audytorów posiadających:       1. certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu;       2. co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych,   lub   * + 1. co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.  1. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:    1. Certified Internal Auditor (CIA);    2. Certified Information System Auditor (CISA);    3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-ENISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;    4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r  o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;    5. Certified Information Security Manager (CISM);    6. Certified in Risk and Information Systems Control (CRISC);    7. Certified in the Governance of Enterprise IT (CGEIT);    8. Certified Information Systems Security Professional (CISSP);    9. Systems Security Certified Practitioner (SSCP);    10. Certified Reliability Professional;    11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert. |
| **Kryteria Audytu Bezpieczeństwa** | 1. Kryteria Audytu Bezpieczeństwa oparte będą o:    1. Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa.    2. Wymagania normatywne PN-EN ISO/IEC 27001:2017-06.    3. Wymagania normatywne PN-EN ISO 22301:2020-04.    4. Wewnętrzną dokumentację Zamawiającego.    5. Przepisy o Krajowym Systemie Cyberbezpieczeństwa.    6. Standardy Krajowych Ram Interoperacyjności (KRI). 2. Audytowi poddany zostanie wpływ przeprowadzonych inwestycji na podniesienie poziomu cyberbezpieczeństwa Zamawiającego. |