Załącznik nr 1

1. Audyt systemu bezpieczeństwa informacji – 3 jednostki.

ZAKRES PRAC

1. Przeprowadzenie:

a. audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI,

b. analizę efektywności działań w zakresie monitorowania, pomiarów, analizy i oceny SZBI, w tym przegląd wskaźników ryzyka i zgodności.

2. Audyt powinien obejmować:

a. Analiza wstępna i określenie zakresu audytu

· Zdefiniowanie obszarów, lokalizacji oraz jednostek organizacyjnych objętych SZBI.

· Weryfikacja ewidencji obszaru przetwarzania informacji, w tym dokładność danych dotyczących lokalizacji, kondygnacji i adresów.

· Sprawdzenie, czy zakres SZBI jest zgodny z wymaganiami norm ISO/IEC 27001 oraz potrzebami organizacji.

b. Weryfikacja dokumentacji systemowej

· Wprowadzenie do SZBI: Ocena, czy dokumentacja zawiera podstawowe zasady zarządzania bezpieczeństwem informacji i zgodność z cyklem PDCA (Plan-Do-Check-Act).

· Terminy i definicje: Sprawdzenie, czy wszystkie istotne pojęcia są zdefiniowane i zgodne z normami.

· Kontekst organizacji: Analiza czynników wewnętrznych i zewnętrznych oraz ich wpływu na SZBI, w tym analiza ryzyk.

c. Zarządzanie ryzykiem

· Ocena procesu identyfikacji i analizy ryzyk, w tym dokumentacji dotyczącej szacowania ryzyk.

· Analiza działań zaradczych i korygujących dla zidentyfikowanych ryzyk.

d. Zabezpieczenia i deklaracja stosowania

· Weryfikacja, czy deklaracja stosowania zabezpieczeń jest zgodna z Załącznikiem A normy ISO/IEC 27001.

· Ocena skuteczności wdrożonych zabezpieczeń oraz uzasadnienia ewentualnych wyłączeń.

e. Dokumentacja operacyjna

· Polityki i procedury: Sprawdzenie polityk bezpieczeństwa (np. kryptografii, zarządzania dostępem, bezpieczeństwa zasobów ludzkich) i ich zgodności z wymaganiami normatywnymi.

· Ewidencje i rejestry: Ocena kompletności i aktualności ewidencji aktywów, obszarów przetwarzania informacji oraz rejestrów incydentów i zgłoszeń.

· Zarządzanie dostępem: Sprawdzenie procedur przyznawania, zmiany i odbierania dostępu oraz zgodności z dokumentacją.

f. Monitorowanie i doskonalenie SZBI

· Ocena procesów monitorowania, analizy i oceny systemu w odniesieniu do zgodności z wymaganiami i celami bezpieczeństwa.

· Weryfikacja raportów z monitorowania, przeglądów zarządzania i działań korygujących.

· Analiza działań doskonalących, w tym ocena skuteczności realizowanych zmian.

g. Zarządzanie incydentami i ciągłością działania

· Ocena polityki zarządzania incydentami, w tym procedur zgłaszania, oceny i reagowania na incydenty.

· Sprawdzenie planów zarządzania ciągłością działania i odtwarzania po katastrofie, w tym testów i analiz RTO, RPO, MTPD i MBCO.

h. Audyty wewnętrzne

· Weryfikacja programu i planów audytów wewnętrznych, w tym ocena zgodności z wymaganiami ISO/IEC 27001.

· Sprawdzenie raportów z audytów wewnętrznych pod kątem ustaleń, zgodności i zaleceń.

i. Zgodność z przepisami i ochroną danych osobowych

· Ocena dokumentacji dotyczącej przetwarzania danych osobowych, w tym zgodności z RODO.

· Weryfikacja rejestrów czynności przetwarzania danych, ocen skutków dla ochrony danych oraz testów równowagi.

j. Dokumentacja operacyjna

· Analiza polityk i procedur dotyczących korzystania z systemów, urządzeń i sieci.

· Weryfikacja zasad postępowania z nośnikami informacji, tworzenia haseł i korzystania z Internetu oraz poczty elektronicznej.

k. Zarządzanie dostawcami

· Sprawdzenie polityk i procedur związanych z bezpieczeństwem informacji w relacjach z dostawcami.

· Ocena zgodności działań dostawców z wymaganiami organizacji.

l. Zgodność z wymaganiami prawnymi

· Weryfikacja dokumentacji dotyczącej monitorowania i przestrzegania wymagań prawnych, regulacyjnych i umownych.

· Analiza zgodności z politykami zgodności oraz audytami technicznymi.

II. DO ZADAŃ WYKONAWCY BĘDZIE NALEŻEĆ

1. Przeprowadzenie szczegółowej analizy i oceny SZBI, obejmującej:

a. Identyfikację niezgodności i słabości w dokumentacji oraz wdrożeniu systemu.

b. Przeprowadzenie wywiadów z wybranym personelem, w tym Pełnomocnikiem ds. Bezpieczeństwa Informacji.

2. Przekazanie dla Kierownika/Dyrektora Jednostki oraz dla Zamawiającego podpisanego przez audytora raportu z audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI zawierający:

a. Ustalenia audytu: Identyfikacja mocnych stron, niezgodności oraz obszarów wymagających doskonalenia.

b. Rekomendacje: Propozycje działań korygujących i doskonalących.

c. Ocena zgodności z normami i przepisami: Wskazanie poziomu zgodności SZBI z wymaganiami ISO/IEC 27001 i regulacjami prawnymi.

3. Wykonawca udokumentuje wykonanie zadania poprzez okazanie protokołu odbioru.

4. Dokumentowanie realizacji zadania poprzez:

a. Sporządzenie protokołu odbioru audytu.

b. Wskazanie osób odpowiedzialnych za wdrożenie działań pokontrolnych.

III. UPRAWNIENIA

1. Audyt systemu bezpieczeństwa informacji wdrożonego u Grantobiorcy zostanie przeprowadzony na wniosek Grantobiorcy przez audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999):

1. Certified Internal Auditor (CIA);

2. Certified Information System Auditor (CISA);

3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/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 (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), 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

2. Zamawiający zastrzega możliwość weryfikacji uprawnień audytorów (ważności uprawnień, akredytacja jednostki wydającej uprawnienia).