**Załącznik nr 1 do Umowy nr …… z dnia ……………**

**Opis przedmiotu zamówienia**

1. **Przedmiot zamówienia:**

**Wykonanie Audytu opracowanych i wdrożonych Polityk Bezpieczeństwa Informacji (PBI)
w Starostwie Powiatowym i pozostałych 17 jednostkach organizacyjnych w ramach realizowanego projektu pn. „Cyberbezpieczny Powiat Głogowski”**, w zakresie:

1. Przeprowadzenia audytu zerowego zgodnie z KRI/KSC.

2. Przeprowadzenia audytu końcowego zgodnego z KRI/KSC - jeżeli zostaną wydane zalecenia poaudytowe.

3. Udzielenia wsparcia poaudytowego.

4. Uzupełnienie załącznika nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” pn. „Ankieta dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego”.

1. **Wykaz jednostek objętych przedmiotem zamówienia:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa jednostki objętej przedmiotem zamówienia** | **Orientacyjna liczba użytkowników****(mogą wystąpić nieznaczne równice w dniu realizacji usługi)** |
|  | Starostwie Powiatowym w Głogowie  | 83 |
|  | I Liceum Ogólnokształcącym im. Bolesława Krzywoustego w Głogowe | 54 |
|  | II Liceum Ogólnokształcącym im. Mikołaja Kopernika w Głogowie | 36 |
|  | Zespole Szkół Technicznych i Ogólnokształcących w Głogowie | 53 |
|  | Zespole Szkół Ekonomicznych im. Jana Pawła II w Głogowie | 72 |
|  | Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie | 43 |
|  | Zespole Szkół Przyrodniczych i Branżowych w Głogowie | 44 |
|  | Zespole Szkół Politechnicznych w Głogowie | 53 |
|  | Zespole Szkół im. Jana Wyżykowskiego w Głogowie  | 62 |
|  | Zespole Placówek Szkolno – Wychowawczych w Głogowie  | 109 |
|  | Powiatowym Centrum Poradnictwa Psychologiczno – Pedagogicznego i Doskonalenia Nauczycieli w Głogowie | 17 |
|  | Głogowskim Centrum Kształcenia Zawodowego w Głogowie | 35 |
|  | Powiatowym Centrum Pomocy Rodzinie w Głogowie | 17 |
|  | Domu Pomocy Społecznej „Magnolia” w Głogowie | 30 |
|  | Powiatowym Środowiskowym Domu Samopomocy w Głogowie  | 13 |
|  | Powiatowym Centrum Administracyjnym w Głogowie | 32 |
|  | Powiatowym Urzędzie Pracy w Głogowie | 51 |
|  | Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej w Głogowie  | 16 |

1. **Szczegółowy zakres przedmiotu zamówienia:**

AD 1. **Przeprowadzenie audytu zerowego zgodnego z KRI/KSC obejmuje:**

* 1. Analizę wstępną stanu bezpieczeństwa informacji w jednostkach wyszczególnionych
	**w pkt. II** **Wykaz jednostek objętych przedmiotem zamówienia** w zakresie objętym Audytem.
	2. Zebranie wstępnych odpowiedzi i dowodów audytowych.
	3. Zdefiniowanie rekomendowanych działań korygujących w zakresie objętym

Audytem.

* 1. Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie

Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) w szczególności:

*A) Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)*

* + - * wyznaczenie osoby do kontaktu – KSC
			* przekazanie danych osoby wyznaczonej – KSC
			* zapewnienie zarządzania incydentem – KSC/KRI
			* zgłaszanie incydentu – KSC
			* zapewnienie obsługi incydentu – KSC
			* zapewnienie dostępu do wiedzy – KSC
			* opracowanie, ustanowienie i wdrożenie SZBI – KRI
			* monitorowanie i przegląd SZBI – KRI
			* doskonalenie SZBI – KRI
			* aktualizowanie regulacji wewnętrznych – KRI
			* inwentaryzacja sprzętu i oprogramowania – KRI
			* przeprowadzanie okresowych analiz ryzyka – KRI
			* postępowanie z ryzykiem – KRI
			* zarządzanie uprawnieniami – KRI
			* szkolenia i uświadamianie – KRI
			* monitorowanie dostępu do informacji – KRI
			* monitorowanie nieautoryzowanych zmian – KRI
			* zabezpieczenie nieautoryzowanego dostępu – KRI
			* ustanowienie zasad bezpiecznej pracy mobilnej – KRI
			* zabezpieczenie informacji przed nieuprawnionym ujawnieniem – KRI
			* zabezpieczenie informacji przed nieuprawnioną modyfikacją – KRI
			* zabezpieczenie informacji przed nieuprawnionym usunięciem lub

zniszczeniem – KRI

* + - * zawieranie w umowach serwisowych zapisów o bezpieczeństwie – KRI
			* ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – KRI
			* aktualizowanie oprogramowania – KRI
			* minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – KRI
			* ochrona systemu przed błędami – KRI
			* stosowanie mechanizmów kryptograficznych w systemach – KRI
			* zapewnienie bezpieczeństwa plików systemowych – KRI
			* zarządzanie podatnościami systemów – KRI
			* kontrola zgodności systemów z regulacjami – KRI
			* zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – KRI
			* bezpieczeństwo chmury obliczeniowej - KRI
1. Opracowanie raportu z audytu bez wydania zaleceń lub wydanie raportu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących.

AD 2. **Przeprowadzenie audytu końcowego zgodnego z KRI/KSC,** jeżeli zostaną wydane zalecenia poaudytowe dla audytu zerowego (jeżeli audyt zerowy zostanie zakończony bez wydania zaleceń Wykonawca nie realizuje audytu końcowego), **obejmuje:**

1. Analizę końcową stanu bezpieczeństwa informacji w jednostkach wyszczególnionych

w **pkt. II Wykaz jednostek objętych przedmiotem zamówienia** w zakresie objętym Audytem.

1. Zebranie końcowych odpowiedzi i dowodów audytowych.
2. Zdefiniowanie rekomendowanych działań korygujących w zakresie objętym Audytem.
3. Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie

Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) w szczególności:

* 1. *Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)*
		+ wyznaczenie osoby do kontaktu – KSC
		+ przekazanie danych osoby wyznaczonej – KSC
		+ zapewnienie zarządzania incydentem – KSC/KRI
		+ zgłaszanie incydentu – KSC
		+ zapewnienie obsługi incydentu – KSC
		+ zapewnienie dostępu do wiedzy – KSC
		+ opracowanie, ustanowienie i wdrożenie SZBI – KRI
		+ monitorowanie i przegląd SZBI – KRI
		+ doskonalenie SZBI – KRI
		+ aktualizowanie regulacji wewnętrznych – KRI
		+ inwentaryzacja sprzętu i oprogramowania – KRI
		+ przeprowadzanie okresowych analiz ryzyka – KRI
		+ postępowanie z ryzykiem – KRI
		+ zarządzanie uprawnieniami – KRI
		+ szkolenia i uświadamianie – KRI
		+ monitorowanie dostępu do informacji – KRI
		+ monitorowanie nieautoryzowanych zmian – KRI
		+ zabezpieczenie nieautoryzowanego dostępu – KRI
		+ ustanowienie zasad bezpiecznej pracy mobilnej – KRI
		+ zabezpieczenie informacji przed nieuprawnionym ujawnieniem – KRI
		+ zabezpieczenie informacji przed nieuprawnioną modyfikacją – KRI

• zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – KRI

• zawieranie w umowach serwisowych zapisów o bezpieczeństwie – KRI

• ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – KRI

• aktualizowanie oprogramowania – KRI

• minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – KRI

• ochrona systemu przed błędami – KRI

• stosowanie mechanizmów kryptograficznych w systemach – KRI

• zapewnienie bezpieczeństwa plików systemowych – KRI

• zarządzanie podatnościami systemów – KRI

• kontrola zgodności systemów z regulacjami – KRI

• zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – KRI

• bezpieczeństwo chmury obliczeniowej - KRI

* 1. Opracowanie raportu z audytu bez wydania zaleceń lub wydanie raportu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych
	i korygujących.

IV Udzielanie wsparcia poaudytowego, dla jednostki, której PBI podlegało audytowi w ciągu 30 od dnia zakończenia przeprowadzenia audytu zerowego polegającego na udzielaniu informacji na temat audytowanych elementów wynikających z raportu.

1. Uzupełnienie wypełnienie załącznika nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” – ankieta dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Uzupełnienia obejmuje wypełnienie części dokumentu w odniesieniu dla każdej jednostki organizacyjnej objętej przedmiotem umowy w zakresie „stanu zrealizowania” oraz dokonania „opisu zrealizowanego zakresu zmian” określonych dla wymienionych działań.