

WYMAGANIA ZAMAWIAJĄCEGO I ZAKRES AUDYTU

Nazwa obszaru	Opis działań skutkujących podniesieniu poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców
Skuteczność działania infrastruktury	<ul style="list-style-type: none"> -Urządzenia i konfiguracja w zakresie ochrony poczty -Urządzenia i konfiguracja w zakresie ochrony sieci -Urządzenia i konfiguracja w zakresie systemów serwerowych -Urządzenia i konfiguracja w zakresie stacji roboczych -Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa
Procesy zarządzania bezpieczeństwem informacji	<ul style="list-style-type: none"> -Nośniki wymienne - udokumentowany sposób postępowania -Zarządzanie tożsamością / dostęp do systemów w zakresie: <ul style="list-style-type: none"> -- Przydzielanie dostępu -- Odbieranie dostępu -Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa
Monitorowanie i reagowanie na incydenty bezpieczeństwa	<ul style="list-style-type: none"> -Procedury zarządzania incydentami -Raportowanie poziomów pokrycia scenariuszami znanych incydentów -Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa -Monitorowanie i wykrycie incydentów bezpieczeństwa -Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów
Zarządzanie ciągłością działania	<ul style="list-style-type: none"> -Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa -Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa -Procedury wykonywania i przechowywania kopii zapasowych -Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP) -Procedury utrzymaniowe
Utrzymanie systemów informacyjnych	<ul style="list-style-type: none"> -Harmonogramy skanowania podatności -Aktualny status realizacji postępowania z podatnościami -Procedury związane ze z identyfikowaniem (wykryciem) podatności -Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami
Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	<ul style="list-style-type: none"> -Polityka bezpieczeństwa w relacjach z dostawcami -Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa -Dostęp zdalny -Metody uwierzytelnienia

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).
7. Zakresem Audytu objęta będzie cała działalność świadczeniodawcy.

Zamawiający wymaga przeprowadzenia przynajmniej jednej wizyty w miejscu wykonania usługi. Wykonanie pozostałych prac może odbyć się w drodze konsultacji i rozmów za pośrednictwem systemów teleinformatycznych.

Wykonanie prac zostanie potwierdzone podpisaniem protokołu z ich wykonania.

Osobą uprawnioną do podpisania protokołu z Wykonawcą jest Pan Konrad Mołczun.