Załącznik nr 3

|  |  |
| --- | --- |
| **Nazwa obszaru** | **Opis działań skutkujących podniesieniu poziomem bezpieczeństwa teleinformatycznego u świadczeniodawców** |
| Skuteczność działania infrastruktury | - 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 | - Nośniki wymienne - udokumentowany sposób postępowania -Zarządzanie tożsamością / dostęp do systemów w zakresie:  -- 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 | - 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 | - 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 | - 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 | - Polityka bezpieczeństwa w relacjach z dostawcami  - Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa  - Dostęp zdalny  - Metody uwierzytelnienia |