OCENA ZGODNOŚCI Z KRI*/ UoKSC**

Zasady oceny

Każdemu z zagadnień (opisywanych wymagań), w polu oznaczonym na żółto, należy przypisać ocenę wg poniższej skali:

0	Brak informacji o spełnieniu wymagania.
1	Zbieżność oświadczeń osób audytowanych.
2	Informacja udokumentowana.

Lp.	Opis wymagania	Podstawa	Audytowany	Dowody	Ustalenia	Ocena
1	Wyznaczenie osoby do kontaktu	Art. 21 UoKSC				0
2	Przekazanie danych osoby wyznaczonej	Art. 22 ust. 1 pkt 5 UoKSC				0
3	Zapewnienie zarządzania incydentem	Art. 22 ust. 1 pkt 1 UoKSC				0
4	Zgłaszanie incydentu	Art. 22 ust. 1 pkt 2 UoKSC Art. 23 UoKSC				0
5	Zapewnienie obsługi incydentu	Art. 22 ust. 1 pkt 3 UoKSC				0
6	Zapewnienie dostępu do wiedzy	Art. 22 ust. 1 pkt 4 UoKSC				0
7	Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI				0
8	Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI				0
9	Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	Par. 20 ust. 1 KRI				0
10	Aktualizowanie regulacji wewnętrznych	Par. 20 ust. 2 pkt 1 KRI				0
11	Inwentaryzacja sprzętu i oprogramowania	Par. 20 ust. 2 pkt 2 KRI				0
12	Przeprowadzanie okresowych analiz ryzyka	Par. 20 ust. 2 pkt 3 KRI				0
13	Postępowanie z ryzykiem	Par. 20 ust. 2 pkt 3 KRI				0

14	Zarządzanie uprawnieniami	Par. 20 ust. 2 pkt 4, 5 KRI				0
15	Szkolenia i uświadamianie	Par. 20 ust. 2 pkt 6 KRI				0
16	Monitorowanie dostępu do informacji	Par. 20 ust. 2 pkt 7 lit. a KRI				0
17	Monitorowanie nieautoryzowanych zmian	Par. 20 ust. 2 pkt 7 lit. b KRI				0
18	Zabezpieczenie nieautoryzowanego dostępu	Par. 20 ust. 2 pkt 7 lit. c KRI				0
19	Ustanowienie zasad bezpiecznej pracy mobilnej	Par. 20 ust. 2 pkt 8 KRI				0
20	Zabezpieczenie informacji przed nieuprawnionym ujawnieniem	Par. 20 ust. 2 pkt 9 KRI				0
21	Zabezpieczenie informacji przed nieuprawnioną modyfikacją	Par. 20 ust. 2 pkt 9 KRI				0
22	Zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem	Par. 20 ust. 2 pkt 9 KRI				0
23	Zawieranie w umowach serwisowych zapisów o bezpieczeństwie	Par. 20 ust. 2 pkt 10 KRI				0
24	Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania	Par. 20 ust. 2 pkt 11 KRI				0
25	Aktualizowanie oprogramowania	Par. 20 ust. 2 pkt 12 lit. a KRI				0
26	Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu	Par. 20 ust. 2 pkt 12 lit. b KRI				0
27	Ochrona systemu przed błędami	Par. 20 ust. 2 pkt 12 lit. c KRI				0
28	Stosowanie mechanizmów kryptograficznych w systemach	Par. 20 ust. 2 pkt 12 lit. d KRI				0
29	Zapewnienie bezpieczeństwa plików systemowych	Par. 20 ust. 2 pkt 12 lit. e KRI				0
30	Zarządzanie podatnościami systemów	Par. 20 ust. 2 pkt 12 lit. f, g KRI				0
31	Kontrola zgodności systemów z regulacjami	Par. 20 ust. 2 pkt 12 lit. h KRI				0

32	Zapewnienie audytu bezpieczeństwa informacji, nie rzadziej niż raz na rok	Par. 20 ust. 2 pkt 14 KRI				0

*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 (Dz.U. z 2017 r. poz. 2247, t.j.)

**Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.).