

## Spis treści

<b>1. Jak korzystać z załącznika</b>	5
1.1. Co zawiera?	5
1.2. Czego nie zawiera?	5
<b>2. Rekomendacje i dobre praktyki ochrony IK</b>	6
2.1. Działania edukacyjne	7
2.2. Struktura organizacyjna	9
2.3. Strategia wdrożenia	13
2.4. Weryfikacja przyjętych rozwiązań i ich aktualizacja	16
2.4.1. Ćwiczenia	16
2.4.2. Procesy audytowe	17
2.5. Ochrona fizyczna	18
2.5.1. Przykłady fizycznych ataków i incydentów z udziałem infrastruktury krytycznej	18
2.5.2. Działania organizacyjne i zapobiegawcze	19
2.5.3. Modele ochrony fizycznej	21
2.5.4. Techniczne środki ochrony fizycznej	25
2.6. Ochrona techniczna	30
2.6.1. Ogólne wymagania dotyczące obiektów budowlanych	30
2.6.2. Ochrona przeciwpożarowa	33
2.6.3. Działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług	35
2.6.4. Działania techniczne mające na celu zapewnienie ciągłości funkcjonowania IK	36

2.7. Ochrona osobowa	37
2.7.1. Postępowanie w trakcie zatrudniania	37
2.7.2. Postępowanie w stosunku do zatrudnionych	39
2.7.3. Ochrona kluczowego personelu	41
2.7.4. Usługodawcy/podwykonawcy	41
2.7.5. Postępowanie z odchodzącymi z pracy	41
2.8. Ochrona teleinformatyczna	43
2.8.1. Przykłady cyberataków na infrastrukturę krytyczną	43
2.8.2. Zasady ochrony teleinformatycznej IK	45
2.9. Ochrona prawna	65
2.10. Plan odbudowy	66