

Mnimalny zakres zadań LCC:

Lp.	Wdrożenie jednolitych mechanizmów oraz świadczenie usług opartych na tych mechanizmach w zakresie:	w związku z zapisami wskazanymi w nw. przepisach Załącznika nr 4 do ustawy o krajowym systemie cyberbezpieczeństwa (w odniesieniu do podmiotów ważnych będących podmiotami publicznymi)	w związku z zapisami wskazanymi w nw. przepisach Załącznika nr 4 do ustawy o krajowym systemie cyberbezpieczeństwa (w odniesieniu do podmiotów ważnych będących podmiotami publicznymi)	w związku z zapisami wskazanymi w nw. przepisach ustawy o krajowym systemie cyberbezpieczeństwa (w odniesieniu do podmiotów kluczowych):	w związku z zapisami wskazanymi w nw. przepisach ustawy o krajowym systemie cyberbezpieczeństwa (w odniesieniu do podmiotów kluczowych):
1	obsługi cyberzagrożeń, incydentów	Pkt I. 12 oraz Pkt I. 18.	Pkt I. 12 oraz Pkt I. 18. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej przygotowanie i testowanie procedury w przypadku wystąpienia awarii lub incydentu oraz określenie procedur i zasad działania podmiotu na wypadek wystąpienia cyberzagrożenia lub w przypadku wystąpienia incydentu.	Art. 8 ust. 1 pkt 2 lit. f), pkt 4 oraz pkt 5 lit. d)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 2. lit. f) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków; Art. 8 ust. 1. pkt 4. zarządzanie incydentami; Art. 8 ust. 1. pkt 5. lit. d) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, z uwzględnieniem konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania;
2	zarządzania aktywami poprzez inwentaryzację produktów usług i procesów ICT oraz wsparcia w opracowaniu i wdrażaniu SZBI	Pkt. I. 1.	Pkt. I. 1. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej inwentaryzację produktów ICT, usług ICT i procesów ICT służących do przetwarzania informacji.	Art. 8 ust. 1 pkt 2 lit. m)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 2. lit. m) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności zarządzanie aktywami;
3	zapewnienia utrzymania bezpiecznych wersji oprogramowania i ich aktualizacji, w tym na urządzeniach mobilnych	Pkt I. 2. oraz Pkt I. 15-16.	Pkt I. 2 oraz Pkt I. 15-16. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej kontrolowanie podstawowych wersji używanego produktów ICT lub usług ICT, a jeżeli to możliwe, korzystanie z mechanizmów kontroli instalacji produktów ICT lub usług ICT na urządzeniach, w tym na urządzeniach mobilnych, monitorowanie częstotliwości wydawania kolejnych wersji produktów ICT, źródeł dystrybucji produktów ICT oraz cyklu życia produktów ICT w celu zapewnienia bezpieczeństwa systemu informacyjnego oraz stosowanie stabilnych wersji produktów ICT lub usług ICT, w stosunku do których nie występują informacje o krytycznych podatnościach, a w przypadku ich wystąpienia dopuszczalne jest stosowanie tych wersji produktów ICT lub usług ICT, które nie stwarzają istotnego negatywnego wpływu na poziom bezpieczeństwa systemów informacyjnych.	Art. 8 ust. 1 pkt 3 oraz pkt 5 lit. b)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 3. zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; Art. 8 ust. 1. pkt 5. lit. b) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji;
4	zarządzania uprawnieniami dostępu	Pkt I. 4-7.	Pkt I. 4-7. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej: dopuszczenie do informacji wyłącznie osób posiadających stosowne uprawnienia do systemów informacyjnych (w tym systemów operacyjnych, usług sieciowych i aplikacji) oraz zapewnienie środków uniemożliwiających nieautoryzowany dostęp do tych systemów, stosowanie zasad przyznania minimalnych uprawnień niezbędnych dla realizacji zadań, bezwzględne cofanie przyznanych uprawnień w przypadku stwierdzenia braku podstawy dostępu do informacji na stałe lub zawieszanie uprawnień w przypadku niewykonywania obowiązków co najmniej przez jeden miesiąc oraz modyfikację zakresu przyznanych uprawnień, jeżeli jest to zasadne z uwagi na zmianę charakteru wykonywanych zadań i zakresu dostępu do informacji.	Art. 8 ust. 1 pkt 2 lit. n)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 2. lit. n) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności polityki kontroli dostępu;

5	ochrony danych w systemach informacyjnych, w tym poprzez kopie zapasowe	Pkt I. 3. lit. b.oraz Pkt I. 10-11 oraz Pkt I. 13.	Pkt I. 3. lit. b.oraz Pkt I. 10-11 oraz Pkt I. 13. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, w zakresie ochrony wykorzystującej oprogramowanie zabezpieczające lub sprzętowe zabezpieczenia, w które są wyposażone urządzenia przetwarzające informacje, wykonywanie zapasowych kopii danych odseparowanych logicznie i fizycznie od danych przetwarzanych w systemach informacyjnych dla realizacji zadania publicznego oraz testowanie pod kątem kompletności i możliwości odtworzenia danych zawartych w zapasowych kopiach oraz stosowanie oprogramowania antywirusowego.	Art. 8 ust. 1 pkt 2 lit. f) oraz pkt 5 lit. a) oraz c)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 2. lit. f) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków; Art. 8 ust. 1. pkt 5. lit. a) oraz c) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym oraz ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym;
6	kontroli bezpieczeństwa komunikacji oraz poczty elektronicznej	Pkt I. 9.	Pkt I. 9. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej kontrolę usług poczty elektronicznej wykorzystującej mechanizmy, o których mowa w art. 24 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.	Art. 8 ust. 1 pkt 2 lit. i)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 2. lit. i) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,
7	doskonalenia kompetencji pracowników z zakresu cyberbezpieczeństwa oraz stosowania zasad cyberhigieny	Pkt I. 14. oraz Pkt I. 17. lit. a-d.	Pkt I. 14. oraz Pkt I. 17. lit. a-d. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej stosowanie zasad cyberhigieny przez pracowników korzystających z systemów informacyjnych, w tym kierownika podmiotu, stosowanie środków minimalizujących wystąpienie incydentów przez szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak: rodzaje cyberzagrożeń, podstawowe zasady cyberhigieny, reagowania na wystąpienie incydentu oraz świadomość skutków naruszenia zasad bezpieczeństwa informacji.	Art. 8 ust. 1 pkt 2 lit. d), i) oraz j)	Art. 8. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający: Art. 8 ust. 1. pkt 2. lit. d), i) oraz j) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności: bezpieczeństwo zasobów ludzkich, edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu oraz podstawowe zasady cyberhigieny;