Załącznik nr 4

WYMOGI DLA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA PODMIOTU WAŻNEGO BĘDĄCEGO PODMIOTEM PUBLICZNYM

I. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej:

1) inwentaryzację produktów ICT, usług ICT i procesów ICT służących do przetwarzania informacji;
2) 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;
3) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, w zakresie:
   a) ochrony fizycznej miejsc, w których jest przetwarzana informacja, w przypadku przetwarzania danych w urządzeniach znajdujących się pod kontrolą podmiotu,
   b) ochrony wykorzystującej oprogramowanie zabezpieczające lub sprzętowe zabezpieczenia, w które są wyposażone urządzenia przetwarzające informacje, albo
   c) udokumentowania mechanizmów zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami w przypadku korzystania z usług dostawcy chmury obliczeniowej lub dostawcy usługi centrum przetwarzania danych;
4) 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;
5) stosowanie zasad przyznania minimalnych uprawnień niezbędnych dla realizacji zadań;
6) bezzwłoczne 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;

7) modyfikację zakresu przyznanych uprawnień, jeżeli jest to zasadne z uwagi na zmianę charakteru wykonywanych zadań i zakresu dostępu do informacji;
8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) 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;
10) wykonywanie zapasowych kopii danych odseparowanych logicznie i fizycznie od danych przetwarzanych w systemach informacyjnych dla realizacji zadania publicznego;
11) testowanie pod kątem kompletności i możliwości odtworzenia danych zawartych w zapasowych kopiach;
12) przygotowanie i testowanie procedury w przypadku wystąpienia awarii lub incydentu;
13) stosowanie oprogramowania antywirusowego;
14) stosowanie zasad cyberhigieny przez pracowników korzystających z systemów informacyjnych, w tym kierownika podmiotu;
15) monitorowanie częstotliwości wydawania kolejnych wersji produktów ICT, źródeł dystrybucji produktów ICT oraz cyklu życia produktów ICT w celu zapewnienia bezpieczeństwa systemu informacyjnego;
16) 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;
17) stosowanie środków minimalizujących wystąpienie incydentów przez szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak:
    a) rodzaje cyberzagrożeń,
    b) podstawowe zasady cyberhigieny,
    c) reagowania na wystąpienie incydentu,
    d) świadomość skutków naruszenia zasad bezpieczeństwa informacji;

18) określenie procedur i zasad działania podmiotu na wypadek wystąpienia cyberzagrożenia lub w przypadku wystąpienia incydentu.

II. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym może dodatkowo obejmować:

1) stosowanie środków zapewniających bezpieczeństwo informacji, w tym produktów ICT, usług ICT lub procesów ICT minimalizujących ryzyko błędów ludzkich;
2) stosowanie dedykowanych usług poczty elektronicznej dla podmiotu na podstawie umowy lub w ramach wspólnego wykonywania obowiązków z zakresu cyberbezpieczeństwa przy pomocy jednostki wyznaczonej, o której mowa w art. 16e ust. 1;
3) zapewnienie wysokiej dostępności systemów informacyjnych:
   a) w zakresie określenia czasu dostępu do systemów informacyjnych,
   b) przez zapewnianie zdolności działania systemu informacyjnego i jego dostępności niezależnie od wystąpienia awarii lub incydentu;
4) określanie i kontrolowanie zasad korzystania przez podmiotu publicznego będącego podmiotem ważnym z:
   a) ogólnodostępnych usług dostawców chmury obliczeniowej,
   b) usług ogólnodostępnych dużych generatywnych modeli sztucznej inteligencji;
5) monitorowanie dostępu do informacji oraz stanu działania systemów informacyjnych za pomocą dedykowanego oprogramowania wykorzystywanego przez pracowników albo korzystanie w tym zakresie z usług dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa;
6) testowanie poziomów bezpieczeństwa systemów informacyjnych oraz zasad cyberhigieny przez pracowników;
7) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa systemów informacyjnych;
8) zapewnienie aktualności wykorzystywanych produktów ICT oraz usług ICT;
9) stosowanie dodatkowych środków technicznych i organizacyjnych, jeżeli jest to konieczne dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych.

III. Podmiot ważny będący podmiotem publicznym dokonuje przeglądu systemu zarządzania bezpieczeństwem informacji:

1) co najmniej raz w roku albo
2) bezzwłocznie w przypadku wydania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji, w zakresie, w jakim dotyczy ona systemów informacyjnych, produktów ICT lub usług ICT podmiotu, albo
3) bezzwłocznie w przypadku wystąpienia okoliczności, które mogą wpłynąć na ryzyko wystąpienia incydentu poważnego i wymagających ponownego zrealizowania działań opisanych w przyjętym systemie zarządzania bezpieczeństwie informacji lub zmian w samym systemie.

IV. Podmiot ważny będący podmiotem publicznym dokumentuje realizację działań wskazanych do realizacji w systemie zarządzania cyberbezpieczeństwa.