1. Audyt systemu bezpieczeństwa informacji.

OPIS PRZEDMIOTU ZAMÓWIENIA

I. ZAKRES PRAC

1. Przeprowadzenie:

a. audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI,

b. analizę efektywności działań w zakresie monitorowania, pomiarów, analizy i oceny SZBI, w tym przegląd wskaźników ryzyka i zgodności.

2. Audyt powinien obejmować:

a. Analiza wstępna i określenie zakresu audytu

· Zdefiniowanie obszarów, lokalizacji oraz jednostek organizacyjnych objętych SZBI.

· Weryfikacja ewidencji obszaru przetwarzania informacji, w tym dokładność danych dotyczących lokalizacji, kondygnacji i adresów.

· Sprawdzenie, czy zakres SZBI jest zgodny z wymaganiami norm ISO/IEC 27001 oraz potrzebami organizacji.

b. Weryfikacja dokumentacji systemowej

· Wprowadzenie do SZBI: Ocena, czy dokumentacja zawiera podstawowe zasady zarządzania bezpieczeństwem informacji i zgodność z cyklem PDCA (Plan-Do-Check-Act).

· Terminy i definicje: Sprawdzenie, czy wszystkie istotne pojęcia są zdefiniowane i zgodne z normami.

· Kontekst organizacji: Analiza czynników wewnętrznych i zewnętrznych oraz ich wpływu na SZBI, w tym analiza ryzyk.

c. Zarządzanie ryzykiem

· Ocena procesu identyfikacji i analizy ryzyk, w tym dokumentacji dotyczącej szacowania ryzyk.

· Analiza działań zaradczych i korygujących dla zidentyfikowanych ryzyk.

d. Zabezpieczenia i deklaracja stosowania

· Weryfikacja, czy deklaracja stosowania zabezpieczeń jest zgodna z Załącznikiem A normy ISO/IEC 27001.

· Ocena skuteczności wdrożonych zabezpieczeń oraz uzasadnienia ewentualnych wyłączeń.

e. Dokumentacja operacyjna

· Polityki i procedury: Sprawdzenie polityk bezpieczeństwa (np. kryptografii, zarządzania dostępem, bezpieczeństwa zasobów ludzkich) i ich zgodności z wymaganiami normatywnymi.

· Ewidencje i rejestry: Ocena kompletności i aktualności ewidencji aktywów, obszarów przetwarzania informacji oraz rejestrów incydentów i zgłoszeń.

· Zarządzanie dostępem: Sprawdzenie procedur przyznawania, zmiany i odbierania dostępu oraz zgodności z dokumentacją.

f. Monitorowanie i doskonalenie SZBI

· Ocena procesów monitorowania, analizy i oceny systemu w odniesieniu do zgodności z wymaganiami i celami bezpieczeństwa.

· Weryfikacja raportów z monitorowania, przeglądów zarządzania i działań korygujących.

· Analiza działań doskonalących, w tym ocena skuteczności realizowanych zmian.

g. Zarządzanie incydentami i ciągłością działania

· Ocena polityki zarządzania incydentami, w tym procedur zgłaszania, oceny i reagowania na incydenty.

· Sprawdzenie planów zarządzania ciągłością działania i odtwarzania po katastrofie, w tym testów i analiz RTO, RPO, MTPD i MBCO.

h. Audyty wewnętrzne

· Weryfikacja programu i planów audytów wewnętrznych, w tym ocena zgodności z wymaganiami ISO/IEC 27001.

· Sprawdzenie raportów z audytów wewnętrznych pod kątem ustaleń, zgodności i zaleceń.

i. Zgodność z przepisami i ochroną danych osobowych

· Ocena dokumentacji dotyczącej przetwarzania danych osobowych, w tym zgodności z RODO.

· Weryfikacja rejestrów czynności przetwarzania danych, ocen skutków dla ochrony danych oraz testów równowagi.

j. Dokumentacja operacyjna

· Analiza polityk i procedur dotyczących korzystania z systemów, urządzeń i sieci.

· Weryfikacja zasad postępowania z nośnikami informacji, tworzenia haseł i korzystania z Internetu oraz poczty elektronicznej.

k. Zarządzanie dostawcami

· Sprawdzenie polityk i procedur związanych z bezpieczeństwem informacji w relacjach z dostawcami.

· Ocena zgodności działań dostawców z wymaganiami organizacji.

l. Zgodność z wymaganiami prawnymi

· Weryfikacja dokumentacji dotyczącej monitorowania i przestrzegania wymagań prawnych, regulacyjnych i umownych.

· Analiza zgodności z politykami zgodności oraz audytami technicznymi.

II. DO ZADAŃ WYKONAWCY BĘDZIE NALEŻEĆ

1. Przeprowadzenie szczegółowej analizy i oceny SZBI, obejmującej:

a. Identyfikację niezgodności i słabości w dokumentacji oraz wdrożeniu systemu.

b. Przeprowadzenie wywiadów z wybranym personelem, w tym Pełnomocnikiem ds. Bezpieczeństwa Informacji.

2. Przekazanie dla Kierownika/Dyrektora Jednostki oraz dla Zamawiającego podpisanego przez audytora raportu z audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI zawierający:

a. Ustalenia audytu: Identyfikacja mocnych stron, niezgodności oraz obszarów wymagających doskonalenia.

b. Rekomendacje: Propozycje działań korygujących i doskonalących.

c. Ocena zgodności z normami i przepisami: Wskazanie poziomu zgodności SZBI z wymaganiami ISO/IEC 27001 i regulacjami prawnymi.

3. Wykonawca udokumentuje wykonanie zadania poprzez okazanie protokołu odbioru.

4. Dokumentowanie realizacji zadania poprzez:

a. Sporządzenie protokołu odbioru audytu.

b. Wskazanie osób odpowiedzialnych za wdrożenie działań pokontrolnych.

III. UPRAWNIENIA

1. Audyt systemu bezpieczeństwa informacji wdrożonego u Grantobiorcy zostanie przeprowadzony na wniosek Grantobiorcy przez audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999):

1. Certified Internal Auditor (CIA);

2. Certified Information System Auditor (CISA);

3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;

4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

5. Certified Information Security Manager (CISM);

6. Certified in Risk and Information Systems Control (CRISC);

7. Certified in the Governance of Enterprise IT (CGEIT);

8. Certified Information Systems Security Professional (CISSP);

9. Systems Security Certified Practitioner (SSCP);

10. Certified Reliability Professional;

11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

2. Zamawiający zastrzega możliwość weryfikacji uprawnień audytorów (ważności uprawnień, akredytacja jednostki wydającej uprawnienia).

2. Audyt zgodności z Standardami Krajowych Ram Interoperacyjności (KRI)

Cele audytu

1. Określenie zakresu zgodności działania procesów, procedur, środków technicznych i organizacyjnych wdrożonych u Zamawiającego z Standardami Krajowych Ram Interoperacyjności.
2. Identyfikacja obszarów doskonalenia przyjętych standardów.

Zakres (obszar i granice) audytu

1. Analiza zapisów wymagań regulacyjnych wewnętrznych udokumentowanych informacji Systemu Zarządzania Bezpieczeństwem Informacji w kontekście ich zgodności z mającymi zastosowanie wymaganiami prawnymi i regulacyjnymi.
2. Analiza zgodności realizowanych procesów przetwarzania informacji w kontekście ich zgodności z mających zastosowanie wymaganiami prawnymi i regulacyjnymi zewnętrznymi, a w tym co najmniej:
    1. sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych, mające na celu:
        a. zapewnienie obywatelom oraz przedsiębiorcom dostępności usług świadczonych przez podmioty realizujące zadania publiczne w postaci elektronicznej;
        b. zwiększenie efektywności usług świadczonych przez administrację publiczną.
    2. sposoby osiągania interoperacyjności:
        a. ujednolicenie, rozumiane jako stosowanie wspólnych norm, standardów i procedur przez różne instytucje publiczne;
        b. wymienność, definiowana jako zdolność do substytucji produktów, procesów lub usług bez wpływu na ciągłość komunikacji między jednostkami odpowiedzialnymi za realizację zadań publicznych oraz między tymi jednostkami a ich odbiorcami, przy równoczesnym zachowaniu zgodności ze wszystkimi określonymi wymogami funkcjonalnymi i poza funkcjonalnymi;
        c. zgodność produktów, procesów lub usług, uznanych za odpowiednie do zastosowań wspólnych w ramach wyznaczonych warunków, gwarantuje realizację fundamentalnych wymogów przy całkowitym wyeliminowaniu niechcianych konsekwencji.
    3. zastosowanie zasad określonych w ust.1 KRI, podlega uzależnieniu od warunków wynikających z procedury oceny ryzyka oraz z charakterystyk projektowanego systemu teleinformatycznego, jego zakresu działania oraz spektrum dostępnych na rynku rozwiązań w dziedzinie dostaw i usług informatycznych.
    4. metody osiągania interoperacyjności, stosowane przez podmiot wykonujący zadania publiczne, musi respektować zasadę neutralności technologicznej i nie może jej naruszać.
    5. podmioty wykonujące zadania publiczne wdrażają rozwiązania zapewniające interoperacyjność na poziomach organizacyjnym, semantycznym oraz technologicznym.
    6. sposoby osiągania interoperacyjności na poziomie organizacyjnym osiąga się przez:
        a. podmioty realizujące zadania publiczne informują w sposób umożliwiający skuteczne zapoznanie się o metodach dostępu oraz zakresie użytkowym serwisów dla świadczonych przez siebie usług;
        b. wyznaczenie przez ministra odpowiedzialnego za informatyzację miejsca przeznaczonego do publikacji informacji, o których mowa w pkt. 1 KRI;
        c. standaryzację i ujednolicenie procedur przy jednoczesnym uwzględnieniu potrzeby zapewnienia poprawnej współpracy między podmiotami realizującymi zadania publiczne;
        d. publikacja i aktualizacja w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
    7. sposoby osiągania interoperacyjności na poziomie semantycznym osiąga się przez:
        a. stosowanie struktur danych oraz znaczników semantycznych tych danych, zdefiniowanych w treści niniejszego rozporządzenia;

b. zastosowanie struktur danych oraz interpretacja danych zawartych w tych strukturach, publikowanych w repozytorium interoperacyjności zgodnie z regulacjami określonymi w § 8 ust. KRI 3 oraz § 10 ust. KRI 5, 6, 11 i 12;

c. implementacja w rejestrach prowadzonych przez podmioty publiczne odniesień do rejestrów zawierających dane referencyjne, w zakresie niezbędnym do wykonania zadań.

8. sposoby osiągania interoperacyjności na poziomie technologicznym osiąga się przez:
   a. Zastosowanie minimalnych wymogów dla systemów teleinformatycznych, zdefiniowanych w rozdziale IV;
   b. Stosowanie przepisów zawartych w regulacjach odrębnych, a w sytuacji ich braku - uwzględnienie postanowień odpowiednich Polskich Norm, norm międzynarodowych lub standardów uznawanych za dobre praktyki przez organizacje międzynarodowe.
9. w repozytorium interoperacyjności, obok struktur danych określonych w § 8 ust. KRI 3 oraz w § 10 ust. KRI 5, 6, 11 i 12, publikowane są również rekomendacje interoperacyjności, będące dobrymi praktykami ułatwiającymi osiągnięcie interoperacyjności na wszystkich poziomach wymienionych w § 5.
10. informacje publikowane w repozytorium interoperacyjności oznaczone są w szczególności:
    a. nazwą;
    b. opisem;
    c. wersją;
    d. datą i czasem publikacji;
    e. statusem obowiązywania;
    f. identyfikatorem pozwalającym na identyfikację osoby publikującej.
11. opublikowana informacja nie może być modyfikowana lub usunięta z repozytorium.
12. dla systemów teleinformatycznych służących do realizacji zadań publicznych stosuje się rozwiązania oparte na modelu usługowym.
13. do opisu protokołów i struktur wymiany danych usługi sieciowej wykorzystuje się Web Services Description Language (WSDL).
14. organ podmiotu udostępniającego usługę sieciową, w celu zapewnienia poprawnej współpracy systemów teleinformatycznych, przekazuje opis, o którym mowa w ust. 2, do repozytorium interoperacyjności.
15. w przypadkach uzasadnionych specyfiką podmiotu publicznego lub świadczonych przez niego usług dopuszcza się inny model architektury.
16. minister właściwy do spraw informatyzacji zapewnia:
    a. minister właściwy do spraw informatyzacji zapewnia realizację publicznej dyskusji nad rekomendacjami interoperacyjności, przy zachowaniu zasady neutralności technologicznej oraz zgodności z normami zatwierdzonymi przez krajową jednostkę normalizacyjną, bądź normami albo standardami rekomendowanymi lub ustalanymi jako obowiązujące przez organy Unii Europejskiej. Dyskusja ta prowadzona jest w sposób, który zapewnia każdemu interesariuszowi możliwość realnego wpływu na opracowanie rekomendacji;
    b. prowadzenie repozytorium interoperacyjności.
17. w rejestrach publicznych szczególnie wyróżnia się następujące typy obiektów:
    a. osobę fizyczną;
    b. podmiot;
    c. obiekt przestrzenny.
18. dla każdego obiektu wymienionego w ust. 1 KRI, w obrębie danego typu, nadaje się unikatowy identyfikator.
19. strukturę identyfikatorów dla typów obiektów wymienionych w ust. 1 KRI, punkty 1 i 2, a także punkt 3 w zakresie dotyczącym punktu adresowego i działki ewidencyjnej, z uwzględnieniem zastrzeżeń zawartych w ustępach 9 i 10, określa załącznik nr 1 do rozporządzenia.
20. przepis, o którym mowa w ustępie 2 w kontekście ustępu 1 punktu 3, nie wyłącza stosowania przepisów wydanych:
    a. przepis, o którym mowa w ust. 2 w związku z ust. 1 KRI pkt 3, nie wyłącza stosowania przepisów wydanych w wykonaniu dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r., ustanawiającej infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE), opublikowanej w Dzienniku Urzędowym Unii Europejskiej L 108 z 25.04.2007, str. 1, z późniejszymi zmianami, w zakresie interoperacyjności zbiorów i usług danych przestrzennych;

b. na podstawie art. 19 ust. 1 KRI pkt 6-10 i ust. 1a KRI, art. 24b ust. 4, art. 26 ust. 2 KRI oraz art. 47b ust. 5 KRI ustawy z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne, opublikowanej w Dzienniku Ustaw z 2017 r., poz. 2101.

21. minister właściwy do spraw informatyzacji publikuje w repozytorium interoperacyjności, dostępnym na platformie ePUAP, schemat XML struktury danych cech informacyjnych obiektów, o których mowa w ust. 1 KRI.
22. podmioty realizujące zadania publiczne, korzystające z wymiany informacji za pośrednictwem środków komunikacji elektronicznej lub dokumentów elektronicznych sporządzonych według wzorów elektronicznych, w których wykorzystywane są obiekty, o których mowa w ustępie pierwszym, są zobowiązane stosować strukturę danych cech informacyjnych tych obiektów zgodnie ze strukturą opublikowaną przez ministra właściwego do spraw informatyzacji. Publikacja ta odbywa się w postaci schematów XML w repozytorium interoperacyjności, na podstawie wniosków organu prowadzącego rejestr referencyjny odpowiedni dla danego typu obiektu.
23. w strukturze, o której mowa w ustępie szóstym, należy szczególnie zawrzeć nazwy i zakresy danych cech informacyjnych obiektów,
24. jeśli z przepisów prawa wynika konieczność stosowania podzbioru cech informacyjnych obiektu, o którym mowa w ustępie pierwszym, należy zachować typy i zakresy danych, które zostały określone w schemacie, o którym mowa w ustępie szóstym.
25. jeśli podmiot publiczny prowadzi rejestr publiczny, który obejmuje typ obiektu, jakim są osoby fizyczne nieposiadające numeru PESEL, identyfikacja takiej osoby odbywa się zgodnie z cechą informacyjną właściwą dla danego rejestru.
26. jeśli podmiot publiczny prowadzi rejestr publiczny, który obejmuje typ obiektu, jakim są podmioty nieposiadające nadanego numeru identyfikacyjnego REGON, identyfikacja tego podmiotu odbywa się zgodnie z cechą informacyjną właściwą dla danego rejestru.
27. struktury danych dodatkowych cech informacyjnych, o których mowa w ust. 9 i 10 KRI, podlegają zgłoszeniu do repozytorium interoperacyjności.
28. organ władzy publicznej, który prowadzi rejestr publiczny zawierający obiekty inne niż wymienione w ustępie pierwszym, wnioskuje do ministra właściwego do spraw informatyzacji o opublikowanie w repozytorium interoperacyjności, funkcjonującym w ramach platformy ePUAP, schematu XML dla struktur danych cech informacyjnych tych obiektów.
29. podmiot publiczny, który prowadzi rejestr publiczny i udostępnia informacje z tego rejestru w drodze wymiany, jest zobowiązany zapewnić rozliczalność takiej operacji.
30. podmiot otrzymujący informacje z rejestru publicznego w drodze wymiany jest zobowiązany do ochrony tych informacji na poziomie nie niższym niż poziom ochrony stosowany w danym rejestrze.
31. przy określaniu funkcjonalności rejestrów publicznych oraz systemów teleinformatycznych uwzględnia się potrzebę zapewnienia podmiotom uprawnionym możliwości realizacji zadań wynikających z odrębnych przepisów.
32. wymiana danych pomiędzy rejestrami publicznymi ogranicza się wyłącznie do informacji niezbędnych dla prawidłowego funkcjonowania tych rejestrów.
33. wymiana danych odbywa się poprzez bezpośrednie odwołanie do danych referencyjnych przez rejestr, który inicjuje wymianę.
34. jeżeli wymiana danych w trybie określonym w ustępie drugim jest niemożliwa lub znacznie utrudniona, dopuszcza się przeprowadzenie wymiany danych w inny sposób, w tym przez kopiowanie danych przez rejestr inicjujący wymianę.
35. podczas tworzenia lub modernizacji rejestrów publicznych oraz systemów teleinformatycznych uwzględnia się potrzebę zapewnienia bezpłatnego dostępu oraz publikacji w repozytorium interoperacyjności opisów usług, schematów XML oraz innych wzorów.
36. systemy teleinformatyczne, używane przez podmioty realizujące zadania publiczne, są projektowane, wdrażane oraz eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, użyteczności, wydajności, przenośności i możliwości pielęgnacji. Proces ten odbywa się przy zastosowaniu obowiązujących norm oraz standardów i metodyk uznanych w obrocie profesjonalnym.
37. zarządzania usługami świadczonymi przez systemy teleinformatyczne ma na celu ich dostarczanie na zadeklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
38. wymagania określone w ust. 1 i 2 KRI uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu

realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

39. systemy teleinformatyczne, używane przez podmioty realizujące zadania publiczne, są wyposażane w składniki sprzętowe lub oprogramowanie, które umożliwiają wymianę danych z innymi systemami teleinformatycznymi. Dzieje się to za pomocą protokołów komunikacyjnych i szyfrujących, określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach, ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.
40. w sytuacji, gdy w danej sprawie nie istnieją przepisy, normy lub standardy, o których mowa w ustępie pierwszym, należy stosować standardy uznane na poziomie międzynarodowym, szczególnie te, które zostały opracowane adekwatnie do potrzeb wynikających z realizowanych zadań oraz bieżącego stanu technologii informatycznych:
    a. internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC);
    b. world Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC).
41. informację o dostępności opisów standardów, o których mowa w ust. 2 KRI, minister właściwy do spraw informatyzacji publikuje w Biuletynie Informacji Publicznej.
42. kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych przez podmioty realizujące zadania publiczne lub odbieranych przez te systemy, a także w odniesieniu do informacji wymienianej pomiędzy tymi systemami a innymi systemami drogą teletransmisji – o ile wymiana ta dotyczy wymiany znaków – odbywa się zgodnie ze standardem Unicode UTF-8, który jest określony przez normę ISO/IEC 10646 wraz ze zmianami lub normę, która ją zastąpi.
43. w uzasadnionych przypadkach dopuszcza się kodowanie znaków według standardu Unicode UTF-16, określonego przez normę wspomnianą w ust. 1 KRI.
44. systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych, które zostały określone w załączniku nr 2 do rozporządzenia.
45. jeśli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych, które służą do załatwienia spraw należących do zakresu ich działania, w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.
46. w systemie teleinformatycznym podmiotu realizującego zadania publiczne, służącym do prezentacji zasobów informacyjnych, należy zapewnić, by ten system spełniał wymagania Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, które zostały określone w załączniku nr 4 do rozporządzenia.
47. podmiot realizujący zadania publiczne jest zobowiązany do opracowania i ustanowienia, wdrażania i eksploatacji, monitorowania i przeglądu, a także utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji. Celem tego systemu jest zapewnienie poufności, dostępności i integralności informacji, przy uwzględnieniu takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
48. zarządzanie bezpieczeństwem informacji, realizowane przez kierownictwo podmiotu publicznego, obejmuje w szczególności zapewnienie warunków umożliwiających realizację i egzekwowanie następujących działań:
    a. zapewnienie aktualizacji regulacji wewnętrznych, tak aby odpowiadały one zmieniającemu się otoczeniu;
    b. utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację;
    c. przeprowadzanie okresowych analiz ryzyka związanego z utratą integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
    d. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają odpowiednie uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji;
    e. bezzwłoczna zmiana uprawnień w przypadku zmiany zadań osób, o których mowa w pkt 4;

f. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem zagadnień takich jak:
   a. zagrożenia bezpieczeństwa informacji;
   b. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;
   c. stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

g. zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a. monitorowanie dostępu do informacji;
   b. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji;
   c. Wprowadzenie oraz utrzymanie środków zapobiegawczych mających na celu prewencję przed nieupoważnionym dostępem w zakresie systemów operacyjnych, usług sieciowych oraz aplikacji.

h. ustanowienie fundamentalnych zasad zapewniających bezpieczne warunki pracy podczas przetwarzania danych w trybie mobilnym i pracy zdalnej.

i. implementacja środków ochrony informacji w sposób wykluczający możliwość jej nieautoryzowanego ujawnienia, modyfikacji, usunięcia lub zniszczenia.

j. włączenie do umów serwisowych, zawieranych ze stronami trzecimi, postanowień gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji.

k. ustalenie zasad postępowania z informacjami, mających na celu minimalizację ryzyka kradzieży informacji oraz środków do ich przetwarzania, w tym urządzeń mobilnych.

l. zagwarantowanie adekwatnego poziomu zabezpieczenia systemów teleinformatycznych, co w szczególności zakłada:
   a. utrzymanie aktualności oprogramowania;
   b. minimalizowanie ryzyka utraty informacji w przypadku awarii;
   c. zapewnienie ochrony przed błędami, utratą oraz nieuprawnioną modyfikacją;
   d. zastosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa;
   e. zapewnienie bezpieczeństwa plików systemowych;
   f. zmniejszenie ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych w systemach teleinformatycznych;
   g. bezzwłoczne podejmowanie działań po wykryciu nieujawnionych podatności w systemach teleinformatycznych, które mogą zagrażać bezpieczeństwu;
   h. nadzoru nad zgodnością systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

m. natychmiastowe zgłaszanie incydentów naruszenia bezpieczeństwa informacji w sposób uprzednio ustalony, umożliwiający szybką interwencję korygującą.

n. zapewnienie regularnego audytu wewnętrznego dotyczącego bezpieczeństwa informacji, przeprowadzanego co najmniej raz w roku.

49. wymagania określone w ust. 1 i 2 KRI uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany zgodnie z Polską Normą PN-ISO/IEC 27001, a proces ustanawiania zabezpieczeń, zarządzania ryzykiem oraz audytowania przeprowadzany jest zgodnie z Polskimi Normami związanymi z tą normą, w tym:
   a. PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
   b. PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
   c. PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

50. rozliczalność w systemach teleinformatycznych podlega rzetelnemu dokumentowaniu za pomocą elektronicznych rejestracji w dziennikach systemowych (logach).

51. w dziennikach systemowych obligatoryjnie rejestruje się działania użytkowników lub obiektów systemowych dotyczące dostępu do:

a. w dziennikach systemowych rejestruje się działania użytkowników lub obiektów systemowych dotyczące dostępu do systemu z uprawnieniami administracyjnymi;
b. w dziennikach systemowych rejestruje się działania użytkowników lub obiektów systemowych dotyczące dostępu do konfiguracji systemu, włącznie z konfiguracją zabezpieczeń;
c. w dziennikach systemowych rejestruje się działania użytkowników lub obiektów systemowych dotyczące przetwarzania danych objętych ochroną prawną zgodnie z przepisami prawa.

52. poza informacjami wymienionymi w ust. 2 mogą być rejestrowane działania użytkowników lub obiektów systemowych, oraz inne zdarzenia związane z eksploatacją systemu, o ile wynika to z analizy ryzyka:
a. operacje przeprowadzane przez użytkowników pozbawionych uprawnień administracyjnych;
b. zdarzenia systemowe o niewielkim istotnym znaczeniu dla integralności funkcjonowania systemu;
c. zjawisk i uwarunkowań otoczenia, w którym funkcjonuje system teleinformatyczny.
53. informacje zawarte w rejestrach systemowych są retencjonowane od dnia ich rejestracji przez czas określony w stosownych przepisach prawa, zaś w przypadku ich braku, przez okres nieprzekraczający dwóch lat.
54. dokumentacje związane z rejestracją systemową mogą być przechowywane na zewnętrznych nośnikach danych, z zachowaniem odpowiednich standardów bezpieczeństwa informacji. W wyjątkowych sytuacjach prowadzenie rejestrów systemowych na nośniku papierowym może być uzasadnione.
55. systemy teleinformatyczne podmiotów wykonujących funkcje publiczne, istniejące w dniu wejścia w życie niniejszego rozporządzenia, należy dostosować do wymagań określonych w § 19 w terminie nie dłuższym niż trzy lata od daty wejścia w życie niniejszego rozporządzenia.
56. systemy teleinformatyczne podmiotów odpowiedzialnych za realizację zadań publicznych, które funkcjonują w dniu wejścia w życie niniejszego rozporządzenia zgodnie z dotychczasowymi przepisami, należy dostosować do wymagań określonych w rozdziale IV tego rozporządzenia, nie później jednak niż w dniu pierwszej istotnej modernizacji tych systemów, która nastąpi po wejściu w życie rozporządzenia.
57. do dnia wejścia w życie przepisów dotyczących ustanowienia Ewidencji Miejscowości, Ulic i Adresów jako rejestru publicznego używanego przy opracowywaniu struktury danych punktów adresowych, z wyłączeniem informacji dotyczących współrzędnych geograficznych x, y, krajowym rejestrze urzędowym podziału terytorialnego kraju, zgodnie z ustawą z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2016 r. poz. 1068 oraz z 2017 r. poz. 60), pełni rolę krajowego rejestru podziału administracyjnego.
58. zgodnie z postanowieniami, rozporządzenie nabiera mocy prawnej po upływie 14 dni od daty jego ogłoszenia.

Kryteria audytu

1. Wymagania prawne:
   1. ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,
   2. 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,
2. Wymagania regulacyjne zewnętrzne:
   1. PN-EN ISO/IEC 27001:2017 (2013) Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania,

3. Wymagania regulacyjne wewnętrzne:
   1. System Zarządzania Bezpieczeństwem Informacji i inne wdrożone w organizacji wymagania wewnętrzne dotyczące przetwarzania i bezpieczeństwa informacji.
4. Wymagania w zakresie uprawnień Wykonawcy:
   1. Audyt zostanie przeprowadzony przez co najmniej dwóch Audytorów posiadających co najmniej dwa różne certyfikaty określone w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999):
      a. Certified Internal Auditor (CIA);
      b. Certified Information System Auditor (CISA);
      c. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
      d. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
      e. Certified Information Security Manager (CISM);
      f. Certified in Risk and Information Systems Control (CRISC);
      g. Certified in the Governance of Enterprise IT (CGEIT);
      h. Certified Information Systems Security Professional (CISSP);
      i. Systems Security Certified Practitioner (SSCP);
      j. Certified Reliability Professional;
      k. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Zastosowane metody audytu

1. Przegląd i analiza zapisów wymagań prawnych i regulacyjnych oraz wytwarzanej w związku z tymi wymaganiami dokumentacji związanej bezpośrednio z Standardami Krajowych Ram Interoperacyjności.
2. Przeprowadzanie rozmów z audytowanymi.
3. Wypełnianie list kontrolnych i/lub kwestionariuszy niezbędnych do prawidłowej realizacji Audytu.