WOJEWODA LUBUSKI

Władysław Dajczak

Gorzów Wlkp., dnia 18 października 2019 r.

NK-II.431.1.3.2019.MWoł.

Pan
Radosław Sosnowski
Burmistrz Lubniewic

Wystąpienie pokontrolne
z kontroli przeprowadzonej w Urzędzie Miejskim w Lubniewicach

Na podstawie art. 28 ust.1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz.U.2019.1464 tj.), art. 2 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U.2011.185.1092) pracownicy Wydziału Nadzoru i Kontroli oraz Biura Obsługi Urzędu i Rozwoju Systemów Informatycznych Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. w składzie:

- Małgorzata Wołejko – starszy inspektor wojewódzki – przewodnicząca zespołu,
- Michał Piaskowski – kierownik Oddziału Informatyki,
- Izabela Milczarek – informatyk ds. administrowania systemami informatycznymi

na podstawie pisemnych upoważnień do przeprowadzenia kontroli nr: 143/1-3/2019 z dnia 18 czerwca 2019 r., w dniach od 25 czerwca 2019 r. do 31 lipca 2019 r. przeprowadzili kontrolę problemową w trybie zwykłym w Urzędzie Miejskim w Lubniewicach.
Kontrola została odnotowana w książce kontroli pod pozycją nr 4/2019.

Przedmiotem kontroli było działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2019.700 tj.).
Okres objęty kontrolą – stan obecny.

Do projektu wystąpienia pokontrolnego zastrzeżenia nie zostały wniesione. Wobec powyższego stosownie do art. 47 ustawy o kontroli w administracji rządowej przekazuję Panu niniejsze wystąpienie pokontrolne.

W wyniku przeprowadzonej kontroli dokonano następujących ustaleń:

W okresie objętym kontrolą funkcję Burmistrza Lubniewic pełnił Radosław Sosnowski. Jak wynika z Regulaminu Organizacyjnego Urzędu Miejskiego w Lubniewicach wprowadzonego Zarządzeniem Nr 5/W/2019 Burmistrza Lubniewic z dnia 18 marca 2019 r. zadania z zakresu działania systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań zleconych z zakresu administracji rządowej należą do Referatu Organizacyjnego. Osoba odpowiedzialną za wykonywanie ww. zadań jest Pani Małgorzata Kuzajewska-Moskwa – kierownik Referatu Organizacyjnego.

1. **Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.**

1.1.Usługi elektroniczne.

Zgodnie z *art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2019.700 tj.)*: Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.

Zgodnie z *§ 5 ust. 2 pkt 1 i 4 rozporządzenia 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.2017.2247 t.j.).*

Urząd Miejski w Lubniewicach nie publikuje usług elektronicznych, nie ma także opisanych kart usług opisujących sposób załatwienia spraw. Jedyną usługą elektroniczną świadczoną przez urząd jest „Pismo ogólne do Urzędu” na platformie ePUAP.

1.2.Centralne repozytorium wzorów dokumentów elektronicznych.

Zgodnie z *art. 19 b ust. 3 ustawy*: Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich

bezpiecznym podpisem elektronicznym.
W trakcie kontroli ustalono, że urząd w badanym okresie do centralnego repozytorium wzorów dokumentów ePUAP nie przekazywał wzorów dokumentów elektronicznych.

1.3.Model usługowy

Zgodnie z *§ 15 ust. 2 rozporządzenia*: Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
Nieprawidłowość:
- brak formalnych procedur zarządzania usługami.

1.4.Współpraca systemów teleinformatycznych z innymi systemami

Zgodnie z *§ 5 ust. 3 pkt 3 rozporządzenia*: Interoperacyjność na poziomie semantycznym osiągana jest przez m.in. stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.
Według *§ 16 ust. 1 rozporządzenia*: Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.
Urząd Miejski posiada zintegrowany system do zarządzania gminą i na tym poziomie interoperacyjność systemów jest na odpowiednim poziomie.

1.5.Obieg dokumentów w Urzędzie.

Zgodnie z *§ 20 ust. 2 pkt 9 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu, jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
W Urzędzie Miejskim w Lubniewicach w celu zarządzania obiegiem dokumentów i dokumentacją stosowane są procedury i zasady postępowania z dokumentami wpływającymi do urzędu zawarte w Instrukcji Kancelaryjnej, stanowiącej załącznik do *rozporządzenia*

Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych i rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U.2011.14.67).

W urzędzie obowiązuje tradycyjny („papierowy") system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania spraw.

1.6.Formaty danych udostępniane przez systemy teleinformatyczne.

Zgodnie z *§ 17 ust. 1 rozporządzenia*: Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/1EC 10646 wraz ze zmianami lub normę ją zastępującą.
Zgodnie z *§ 18 ust. 1 rozporządzenia*: Systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia.
Wg *§ 18 ust. 2 rozporządzenia*: Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.
W toku kontroli dokonano weryfikacji kodowania znaków, w odniesieniu do informacji wymienianych przez systemy urzędu z innymi systemami zewnętrznymi, na drodze teletransmisji, która wykazała stosowanie standardu Unicode UTF-8.

W obszarze wymiany informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną działalność urzędu **oceniono pozytywnie z uchybieniami**.

2. System zarządzania bezpieczeństwem informacji w systemach informatycznych.

2.1.Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu.

Zgodnie z *§ 20 ust. 1 rozporządzenia*: Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Zgodnie z *§ 20 ust. 2 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji.

Zgodnie z *§ 20 ust. 2 pkt 1 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie aktualizacji regulacji wewnętrznych w zakresie - dotyczącym zmieniającego się otoczenia.

Burmistrz Lubniewic wydał Zarządzenie Nr 106/36/W/2013 z dnia 02 września 2013 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Lubniewicach.

Nieprawidłowość:

- Polityka jest skoncentrowana wyłącznie na danych osobowych i nie obejmuje swym obszarem ochrony wszystkich danych w urzędzie;
- Polityka zawiera duże rozbieżności w stosunku do rzeczywistości.

2.2.Analiza zagrożeń związanych z przetwarzaniem informacji.

Zgodnie z *§ 20 ust. 2 pkt 3 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Urząd Miejski w Lubniewicach nie przedstawił dokumentów potwierdzających wykonanie analizy ryzyka.

Nieprawidłowość:

- Brak dokumentacji analizy ryzyka.

2.3.Inwentaryzacja sprzętu i oprogramowania informatycznego.

Zgodnie z *§ 20 ust. 2 pkt 2 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. utrzymanie aktualności inwentaryzacji sprzętu

i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Urząd Miejski ma przygotowaną., wydrukowaną dokumentację z opisem każdej stacji, jej konfiguracji i zainstalowanym oprogramowaniem. Badanie kontrolne wykazało zgodność ze stanem rzeczywistym.

2.4.Zarządzanie uprawnieniami.

Zgodnie z *§ 20 ust. 2 pkt 4 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

Zgodnie z *§ 20 ust. 2 pkt 5 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

W trakcie kontroli stwierdzono, że ewidencja uprawnień jest prowadzona na zasadzie wystawiania pracownikom upoważnień do systemów informatycznych przez Inspektora Danych Osobowych na wniosek burmistrza. Brakuje jasnych procedur nadawania i odbierania uprawnień. Brakuje potwierdzeń wniosków i wykonanych prac w formie papierowej lub elektronicznej. Nieformalne procedury opierają się na przekazach ustnych, których nie można potwierdzić.

2.5.Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Zgodnie z *§ 20 ust. 2 pkt 6 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, 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.

Urząd Miejski w Lubniewicach przeprowadził w 2018 roku kompleksowe szkolenia z ochrony danych osobowych. Szkoleniem byli objęci wszyscy pracownicy urzędu. Z uwagi na incydenty stwierdzone podczas kontroli warto rozważyć pogłębienie szkoleń pracowników w tematyce bezpieczeństwa informacji i przeprowadzać je z większą częstotliwością.

2.6.Praca na odległość i mobilne przetwarzanie danych.

Zgodnie z *§ 20 ust. 2 pkt 8 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Urządzenia mobilne w Urzędzie Miejskim w Lubniewicach są wynoszone poza siedzibę urzędu. Poza pocztą elektroniczną nie ma zdalnego dostępu do zasobów urzędu. Jedynie firma zewnętrzna posiada bezpieczne, szyfrowane kanały komunikacji do zdalnej pomocy.

Nieprawidłowość:

- Urządzenia mobilne nie są szyfrowane.

2.7.Serwis sprzętu informatycznego i oprogramowania.

Wg § 20 ust. 2 pkt 10 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Urząd Miejski w Lubniewicach posiada umowę w zakresie obsługi informatycznej z firmą zewnętrzną. Wszystkie umowy posiadają zapisy o powierzeniu przetwarzania danych osobowych.

2.8.Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Zgodnie z *§ 20 ust. 2 pkt 13 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Incydenty bezpieczeństwa informacji nie są monitorowane i rejestrowane. Rejestr incydentów nie zawiera zapisów.

Nieprawidłowość:

- W wyniku działań kontrolnych ujawniono co najmniej kilka incydentów. Zarządzanie incydentami jest bardzo ważnym aspektem systemu zarządzania bezpieczeństwem informacji. Jest to podstawowe narzędzie przy badaniu podatności systemów informatycznych. Brak zarejestrowanych incydentów świadczy o braku monitorowania systemów w kontekście występowania incydentów, a także o niewystarczającej wiedzy pracowników na temat definicji i sposobu zgłaszania incydentu.

2.9.Audyt wewnętrzny w zakresie bezpieczeństwa informacji.

Zgodnie z *§ 20 ust. 2 pkt 14 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Nieprawidłowość:

W ostatnich latach nie wykonywano audytów bezpieczeństwa informacji.

2.10. Kopie zapasowe.

Zgodnie z *§ 20 ust. 2 pkt 12 lit. B rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii.

Kopie bezpieczeństwa są wykonywane na osobnym urządzeniu (NAS). Użytkownicy mają dostęp do zasobów sieciowych, ale nie składują tam swoich danych, pozostawiając je na stanowiskach w sposób niezabezpieczony. Może to wynikać z braku szkoleń i formalnych procedur.

Nieprawidłowość:

- Kopie bezpieczeństwa są przechowywane w tym samym pomieszczeniu co dane produkcyjne;
- Brak potwierdzenia okresowego testowania odtwarzania kopii zapasowych.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.

Zgodnie z *§ 15 ust. 1 rozporządzenia*: Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Nieprawidłowość:

- Urząd Miejski w Lubniewicach nie posiada żadnych formalnych regulacji wewnętrznych dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych.

2.12. Zabezpieczenia techniczno-organizacyjne informacji.

Zgodnie z *§ 20 ust. 2 rozporządzenia*: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in.:

pkt 7: zapewnienie ochrony przetwarzania 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) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,

pkt 9: zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,

pkt 11: ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji środków przetwarzania informacji, w tym urządzeń mobilnych.

W Urzędzie Miejskim w Lubniewicach istnieją zabezpieczenia fizyczne minimalizujące wystąpienie ryzyka kradzieży informacji i środków przetwarzania informacji.

Nieprawidłowości:

- Istnieje możliwość dostępu do pomieszczeń przez osoby nieuprawnione, z uwagi na brak zarządzania kluczami.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Wg *§ 20 ust. 2 pkt 12 rozporządzenia***:** Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania;

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii;

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją;

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa;

e) zapewnieniu bezpieczeństwa plików systemowych;

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Wg § 20 ust. 4 rozporządzenia: Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.
Na wszystkich komputerach w Urzędzie Miasta jest zainstalowane oprogramowanie antywirusowe. W wyniku działań kontrolnych nie stwierdzono problemów z aktualizacjami oprogramowania lub definicjami wirusów.
Poświadczenia administracyjne do serwerów i systemów, znane są firmie zewnętrznej i przechowywane w sejfie.

2.14. Rozliczalność działań w systemach informatycznych.

Zgodnie z *§ 21 ust 2 rozporządzenia*: W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:
1) systemu z uprawnieniami administracyjnymi;
2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
Zgodnie z *§ 21 ust. 3 rozporządzenia*: W zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w *§ 21 ust. 2 rozporządzenia KRI* są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
1) działań użytkowników nieposiadających uprawnień administracyjnych,
2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny - w zakresie wynikającym z analizy ryzyka.
Zgodnie z *§ 21 ust. 4 rozporządzenia*: informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.
Wszystkie systemy informatyczne stosowane w urzędzie posiadają logi systemowe.
<u>Nieprawidłowość:</u>
- brak kopii zapewniających możliwość ich przechowywania przez okres minimum 2 lat.

W obszarze bezpieczeństwa informacji działalność urzędu **oceniono negatywnie.**

3. **Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.**

Zgodnie z *§ 19 rozporządzenia*: W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu oraz BIP Urzędu ze standardem WCAG 2.0 poprzez wykorzystanie narzędzi dostępnych na stronie internetowej https://validator.w3.org. Strona BIP jest zgodna ze standardem WCAG 2.0, a strona internetowa urzędu zawiera niewielkie nieprawidłowości.

Nieprawidłowość:

- Strona urzędu nie jest dostosowana do dostępu dla osób niepełnosprawnych.

W obszarze dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych działalność urzędu **oceniono pozytywnie z nieprawidłowościami.**

Przedstawiając powyższe ustalenia, zalecam:

1. Dokonać kompleksowego wdrożenia Systemu zarządzania bezpieczeństwem informacji, uwzględniając wszystkie informacje przetwarzane oraz przechowywane w Urzędzie.
2. Przeprowadzać okresową aktualizację dokumentacji SZBI zgodnie z wymogami wskazanymi w § 20 ust. 2 pkt 1 rozporządzenia KRI.
3. Badać podatności systemów informatycznych np. na postawie występujących incydentów i określać zagrożenia. Przeprowadzać okresowe udokumentowane analizy ryzyka i przedstawiać sposób postępowania z ryzykiem.
4. Wykonywać audyty wewnętrzne przynajmniej raz w roku.
5. Wdrożyć procedury zarządzania uprawnieniami.
6. Właściwie zarządzać urządzeniami mobilnymi podczas pracy poza siedzibą urzędu.
7. Prowadzić rejestr incydentów. Opracować procedurę zgłaszania incydentów oraz przeszkolić pracowników w tym zakresie.
8. Stworzyć procedurę wykonywania kopii zapasowych. Testować i dokumentować okresowe odtwarzanie danych. Opracować plany zapewnienia ciągłości działania.
9. Wdrożyć rozwiązania teleinformatyczne zapewniające możliwość przechowywania logów systemowych przez okres minimum 2 lat.

10. Wdrożyć regulacje wewnętrzne dotyczących projektowania, wdrażania, wprowadzania zmian i monitorowania systemów informatycznych.
11. Wdrożyć procedury umożliwiające zarządzanie usługami realizowanymi przez systemy teleinformatyczne, stosować szczegółowe opisy usług na stronach internetowych urzędu.
12. Dostosować strony internetowe do dostępu dla osób niepełnosprawnych.

W terminie 30 dni liczonym od daty otrzymania niniejszego wystąpienia pokontrolnego, proszę o pisemną informację o sposobie wykonania zaleceń i wykorzystaniu wniosków, a także o podjętych działaniach lub przyczynach ich nie podjęcia.

WOJEWODA LUBUSKI

Władysław Dajczak