WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

Olsztyn, 3 listopada 2023 r

Wydział Finansów i Kontroli
FK-IV.431.12.2023

Szanowny Pan
Marek Dominiak
Burmistrz Bisztynka
ul. Kościuszki 2
11-230 Bisztynek

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Miejskim w Bisztynku[1], ul. Kościuszki 2, 11-230 Bisztynek, NIP jednostki: 7431976353, REGON jednostki: 510743597.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Marek Dominiak** - Burmistrz wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21.11.2018 r.

- W dniu rozpoczęcia czynności kontrolnych oraz w okresie objętym kontrolą, odpowiedzialnym za realizację zadania objętego kontrolą był Pan [redacted]

- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania była Pani [redacted]

[akta kontroli poz. 21]

Kontrolę przeprowadzili pracownicy Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie:
Radosław Gazda – inspektor wojewódzki; przewodniczący zespołu kontrolnego, legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.716.2023 z 29 sierpnia 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.
Michał Wasilewski – inspektor wojewódzki; członek zespołu kontrolnego, legitymacja służbowa nr 23/2020, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu

[1] Zwanym dalej: Urzędem

Warmińsko-Mazurski Urząd Wojewódzki w Olsztynie
Al. Marsz. J. Piłsudskiego 7/9
10-575 Olsztyn
tel. 89 523 24 44, 89 523 23 33, fax 89 527 74 47
www.olsztyn.uw.gov.pl
info@uw.olsztyn.pl
Skrzynka ESP na ePUAP /WMURZADWOJ/SkrytkaESP

Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.715.2023 z 29 sierpnia 2023 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 8-9]

Kontrolę przeprowadzono w dniach 8-29 września 2023 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 5/2023.

[akta kontroli poz. 22-23]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 23 stycznia br. - rozpoczęto czynności kontrolne w Urzędzie oraz dokonano oględzin serwerowni na miejscu w jednostce. Pozostałe dni (24 stycznia - 10 lutego br.) kontrola była prowadzona zdalnie, bez osobistej obecności kontrolerów Urzędzie, z wykorzystaniem narzędzi informatycznych do zgromadzenia materiału dowodowego, w celu ustalenia stanu faktycznego, a następnie dokonania oceny działalności jednostki kontrolowanej, a także sformułowanie ewentualnych zaleceń pokontrolnych. W dniu rozpoczęcia czynności kontrolnych okazano legitymacje oraz upoważnienia do kontroli, poinformowano o zasadach kontroli w trybie hybrydowym, wymaganych dokumentach do kontroli oraz formach i terminie ich przekazywania.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2023 r., poz. 57). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2022 r.

[akta kontroli poz. 1, 15]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tj. Dz. U. z 2023 r., poz. 190), w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. z 2023 r., poz. 57)[2], rozdziału III i IV 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. z 2017 r. poz. 2247 ze zm.)[3], jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli poz. 1, 15]

Burmistrz Bisztynka upoważnił Inspektora ds. informatyki do udzielania informacji w okresie trwania czynności kontrolnych.

[akta kontroli poz. 24]

[2] Zwanej dalej: ustawą
[3] Zwanego dalej: rozporządzeniem KRI

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**
Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez Urząd przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań zleconych z zakresu administracji rządowej wykorzystywane są 3 niżej wymienione systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:

[redacted]

[akta kontroli poz. 11-12, 16]

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

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że 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 KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

a) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;
b) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Urząd posiada aktywną Elektroniczną Skrzynkę Podawczą **/00529278/SkrytkaESP**, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.
W kontroli ustalono, że Urząd dysponuje Elektroniczną Skrzynką Podawczą (ESP), która działa zgodnie z określonymi prawnie wymogami, jednakże na stronie internetowej BIP Urzędu nie opublikowano informacji o uruchomieniu ESP oraz o metodach dostarczania i wymaganiach dla dokumentów elektronicznych, wynikających z § 3 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. *w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych* (t.j. Dz.U. z 2018 poz.180). Brak spełnienia powyższych wymogów stanowi uchybienie skutkujące niedoinformowaniem petentów o uruchomieniu ESP oraz o metodach dostarczania i wymaganiach dla dokumentów elektronicznych. Przyczyna uchybienia jest niestosowanie obowiązujących przepisów w przedmiotowym zakresie. Osobą odpowiedzialną jest pracownik nadzorujący działanie ESP Urzędu.

Na stronie głównej BIP Urzędu, w zakładce „e-Usługi" zawarto odnośniki do Platformy e-Usług. Platforma e-Usług Publico przeznaczona jest dla mieszkańców, którzy chcą korzystać z usług jednostek samorządu terytorialnego drogą elektroniczną. Aplikacja ta udostępnia obywatelom dane urzędowe oraz umożliwia sprawną komunikację pomiędzy interesantem i pracownikiem urzędu. Platforma e-Usług Publico daje możliwości interakcji interesantowi z wirtualnym biurem obsługi, gdzie uzyska on dostęp do usług realizowanych przez daną jednostkę z opcją umówienia się na spotkanie oraz złożenia dokumentów, zgodnych z dostępnymi i obsługiwanymi formularzami. Dodatkowo platforma jest połączona z systemami dziedzinowymi jednostek samorządowych, dzięki czemu umożliwia realizację płatności w ramach zobowiązań wynikających z podatków i innych opłat w zakresie oferowanych usług, a także dostęp do danych udostępnionych publicznie oraz danych ściśle powiązanych z zalogowanym interesantem. Aby mieszkańcy i interesanci nie przeoczyli aktualności oraz planowanych wydarzeń na terenie gminy, platforma daje możliwość zarządzania i dzielenia się tymi informacjami. Poza wersją internetową platforma e-Usług Publico może być dostępna w formie dedykowanej aplikacji mobilnej.

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, że na stronie BIP w zakładce *Procedury załatwiania spraw*, opublikowany jest przydatny dla petentów wykaz e-usług oraz usług załatwianych w sposób tradycyjny, które realizowane są przez poszczególne departamenty i stanowiska Urzędu.

Ponadto na stronie BIP w powyższej zakładce opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych departamentów i stanowisk w Urzędzie.

Urząd świadczył za pomocą ePUAP usługę „Pismo ogólne do podmiotu publicznego". Usługa przeznaczona jest do tworzenia pism w postaci elektronicznej wnoszonych za pomocą elektronicznej skrzynki podawczej lub doręczanych przez podmioty publiczne za potwierdzeniem doręczenia, w przypadkach gdy łącznie spełnione są następujące warunki:

- organ administracji publicznej nie określił wzoru dokumentu elektronicznego umożliwiającego załatwienie danej sprawy,
- przepisy prawa nie wskazują jednoznacznie, że jedynym skutecznym sposobem przekazania informacji jest jej doręczenie w postaci papierowej.

Jednocześnie należy zaznaczyć, że Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych.

[akta kontroli poz. 25-27]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b 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 kwalifikowanym podpisem elektronicznym.

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że Urząd nie przekazywał do CRWDE wzorów dokumentów. Na stronie BIP w zakładce Procedury załatwiania spraw, opublikowany jest przydatny dla petentów wykaz e-usług oraz usług załatwianych w sposób tradycyjny, które realizowane są przez poszczególne departamenty i stanowiska Urzędu. Ponadto na stronie BIP w powyższej zakładce opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych departamentów i stanowisk w Urzędzie.

[akta kontroli poz. 42]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.3. Model usługowy

– Z § 15 ust. 2 rozporządzenia KRI wynika, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

Strona internetowa Urzędu działa pod adresem https://bisztynek.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.bisztynek.pl/.
Na stronie głównej BIP Urzędu, w zakładce „e-Usługi" zawarto odnośniki do Platformy Publico przeznaczonej dla mieszkańców, którzy chcą korzystać z usług jednostek samorządu terytorialnego drogą elektroniczną. Aplikacja ta udostępnia obywatelom dane urzędowe oraz umożliwia sprawną komunikację pomiędzy interesantem i pracownikiem urzędu.
Ponadto na stronie BIP w zakładce *Procedury załatwiania spraw*, opublikowany jest przydatny dla petentów wykaz e-usług oraz usług załatwianych w sposób tradycyjny, które realizowane są przez poszczególne departamenty i stanowiska Urzędu.
Ponadto na stronie BIP w powyższej zakładce opublikowane są wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych departamentów i stanowisk w Urzędzie.

[akta kontroli poz. 25-27]

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez systemy teleinformatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej ze względu na fakt, że jednostka nie świadczyła usług elektronicznych na zewnątrz za pomocą tych systemów. Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

– § 5 ust. 3 pkt 3 rozporządzenia KRI interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;
– § 16 ust. 1 rozporządzenia KRI systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w 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.

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje, np. o obywatelu/podmiocie, takie jak PESEL, REGON, NIP, dane adresowe itp. Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: [redacted]

[akta kontroli poz. 42]

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że 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.

[redacted]

Opracowanie procedur dotyczących wykonywania czynności kancelaryjnych, w których określone są zasady obiegu dokumentów wpływających drogą elektroniczną oraz zakres stosowania elektronicznego obiegu dokumentów, zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Opracowanie zasad postępowania z dokumentacją elektroniczną (wnioski elektroniczne, e-maile) oraz wymagań organizacyjno-technicznych dotyczących zarządzania tą dokumentacją pozwala właściwie dbać o jej bezpieczeństwo.

[akta kontroli poz. 27]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI 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/IEC 10646 wraz ze zmianami lub normę ją zastępującą;
- § 18 ust. 1 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;
- § 18 ust. 2 rozporządzenia KRI 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.

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: [redacted]

[akta kontroli poz. 42]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI 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;
- § 20 ust. 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków

umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;
- § 20 ust. 2 pkt 1 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", celem określenia reguł j zasad obowiązujących przy przetwarzaniu danych osobowych, [redacted]

[akta kontroli poz. 29, 43]

Realizacja zadań w zakresie ochrony danych wymaga od podmiotu publicznego opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie.
Podstawowym elementem SZBI jest **Polityka Bezpieczeństwa Informacji**. Zgodnie z definicją zawartą w rozporządzeniu KRI §2 pkt 15 *polityka bezpieczeństwa informacji jest to zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania.*
Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji. PBI może określać aktywa oraz ich właścicieli, oraz sposób szacowania ryzyka i postępowania z ryzykiem.
Zazwyczaj w ramach SZBI funkcjonują inne polityki, regulaminy i procedury np.:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.
- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;

- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.

Dokumentację SZBI stanowią także:

- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka BI;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszenia BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

W Urzędzie nie opracowano i nie wdrożono całościowej SZBI, w szczególności nie wdrożono zaktualizowanej polityki bezpieczeństwa informacji - PBI.

[redacted]

[akta kontroli poz. 42]

[redacted] Mając na względzie przepisy § 20 ust. 3 rozporządzenia KRI należy uznać, że przyjęta w Urzędzie polityka stanowi tylko jedną ze składowych dokumentacji ustanawiającej SZBI w jednostce i nie dopełnia w całości obowiązku wynikającego z cytowanych powyżej przepisów. Z § 20 ust. 3 rozporządzenia KRI wynika ponadto, że wymagania określone w ust. 1 tego paragrafu uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (*Polska Norma PN-EN ISO/IEC 27001:2017 Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą (*PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.*).
Jednocześnie w pkt 5.1 Polskiej Normy PN-EN ISO/IEC 27002, wskazano wymóg opracowania i stosowania polityki bezpieczeństwa informacji - PBI.
Powyższe stanowi nieprawidłowość, skutkującą naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD pełniący funkcję w tym okresie.

W myśl § 20 ust. 1 rozporządzenia KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.
Zgodnie z powyższym rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest

także monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Oznacza to, iż realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi. [redacted]

[redacted]

W przekazanej dokumentacji, w ramach prowadzonych czynności kontrolnych nie stwierdzono dowodów świadczących o podejmowaniu dodatkowych działań w zakresie prowadzenia monitoringu i przeglądów przyjętego systemu zarządzania bezpieczeństwem informacji (np. wycinkowe sprawdzenia SZBI, przeglądy Polityki w celu określenia jej właściwości i adekwatności). **Powyższe stanowi uchybienie.**

[redacted]

Rola podmiotu nie kończy się tylko i wyłącznie na opracowaniu i wdrożeniu do eksploatacji systemu zarządzania bezpieczeństwem informacji. Obowiązkiem podmiotu jest także monitorować, przeglądać i utrzymywać jak również doskonalić ten system tak, aby zapewniać poufność, dostępność i integralność informacji. Powyższe oznacza, iż realizacja obowiązku wynikającego z § 20 ust. 1 KRI nie kończy się z momentem wdrożenia do stosowania SZBI, lecz wymaga ona nieustannej uwagi.

[akta kontroli poz. 42]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z nieprawidłowościami.**

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu. Analiza ryzyka jest ważnym wymaganiem nałożonym na administratorów i podmioty przetwarzające. Proces szacowania ryzyka powinien być przeprowadzony i udokumentowany w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki obrony. Szacowanie ryzyka pozwala na aktywne zarządzanie bezpieczeństwem informacji, w tym na przeciwdziałanie zagrożeniom oraz ograniczanie skutków zmaterializowanych ryzyk, a także wpływa na racjonalne zarządzanie środkami finansowymi

poprzez stosowanie zabezpieczeń adekwatnych do oszacowanego poziomu ryzyka. Jednocześnie należy zaznaczyć, że prawidłowo przebiegająca analiza ryzyka nie jest jednorazowym działaniem, lecz regularnie i ciągle monitorowanym procesem.
Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo, a w przypadku stwierdzenia podwyższonego ryzyka w przedmiotowym zakresie, powinny zostać wprowadzone działania minimalizujące to ryzyko.

Kontrolującym przedstawiono dokumentację (stanowiącą akta kontroli) świadczącą o przeprowadzeniu okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji w Urzędzie w 2022 roku.

[akta kontroli poz. 30-31]

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO oraz rozdziałem 1.6 przyjętej PODO, prowadzony jest rejestr czynności przetwarzania. W jednostce powołano również Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.

[akta kontroli poz. 32-34]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Kontrolującym nie przedstawiono dokumentacji w zakresie spełnienia obowiązku wynikającego z § 20 ust. 2 pkt 2 rozporządzenia KRI, tj. prowadzenia inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

[redacted]

Zgodnie z przyjętym Programem kontroli nie sporządzanie bieżącej i aktualnej informacji nt. sprzętu i oprogramowania wykorzystywanego do przetwarzania informacji **stanowi uchybienie**, skutkujące naruszeniem z § 20 ust. 2 pkt 2 rozporządzenia KRI. Powyższe skutkuje również brakiem możliwości sprawnego odtworzenia infrastruktury informatycznej, w przypadku wystąpienia katastrofy lub innego zdarzenia losowego. Osobą odpowiedzialną za powstanie uchybienia jest ASI (Informatyk).

[akta kontroli poz. 42, 44-45]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami.**

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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;
- § 20 ust. 2 pkt 5 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Istotnym elementem polityki BI (bezpieczeństwa informacji) jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

[redacted]

[redacted]

Kontrolujący stwierdzili, że osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania. Jednocześnie należy nadmienić, że we wzorze upoważnienia do przetwarzania danych osobowych przekazanym kontrolującym wraz z dokumentacją do kontroli, zawarto możliwość wskazania zbiorów (systemu teleinformatycznego) do pracy w którym dany pracownik jest upoważniony. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych i pracy w określonym systemie teleinformatycznym.

[akta kontroli poz. 42-43, 46-47]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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.

Z informacji uzyskanych z Urzędu wynika, że, pracownicy zaangażowani w proces przetwarzania informacji uczestniczyli w okresie objętym kontrolą w szkoleniu, w zakresie cyberbezpieczeństwa, które swoim programem obejmowało:

- Podstawowe zasady bezpieczeństwa pracy na komputerze.
- OSINT - co to jest biały wywiad, czyli jak i gdzie szukać informacji w sieci.
- Symptomy zainfekowania komputera - przykłady ataków.
- Bezpieczeństwo haseł - budowa, przechowywanie oraz inne bezpieczniejsze metody logowania.
- Podstawowe informacje o atakach na użytkowników - socjotechnika, phishing, spearphishing, malware, pharming, spoofing, spam, spim, scam. Przykłady z życia.
- Podstawy bezpiecznego korzystania ze smartfonu, tabletu.
- Bezpieczne korzystanie z poczty elektronicznej.
- Bezpieczne korzystanie z sieci bezprzewodowych - WI-FI. Rodzaje ataków z wykorzystaniem na sieci bezprzewodowe.
- Do czego cyberprzestępcy mogą wykorzystać nasze dane.
- Prezentacja gadżetów umożliwiających podsłuch, nagrywanie obrazu czy odczyt kart bankomatowych, czyli na co zwrócić uwagę, aby nie zostać nagranym.
- Profil zaufany, a kwalifikowany podpis cyfrowy.
- Cyberhigiena w sieci, czyli zbiór zasad i reguł postpowania dla pracowników zarówno w życiu zawodowym jak i prywatnym.
- Dyskusja nt. cyberhigieny w życiu służbowym i prywatnym.

Potwierdzeniem odbycia szkolenie jest imienna lista uczestników włączona do akt kontroli.

[akta kontroli poz. 35]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.6. Praca na odległość i mobilne przetwarzanie danych

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

[redacted]

[redacted]

Dokumenty te regulują i ustanawiają podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

[akta kontroli poz. 48-49]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

[redacted]

W związku z zakupem ww. systemu podpisane zostały z dystrybutorem stosowne umowy licencyjne, umożliwiające prawidłową eksploatację i rozwój, poprzez możliwość zgłaszania błędów pytań i roszczeń, dotyczących użytkowanego systemu. Zawarte zostały również stosowne umowy powierzenia danych gwarantujące właściwe zabezpieczenie danych w przypadku awarii systemu oraz gwarantujące bezpieczeństwo informacji uzyskanych przez wykonawcę w związku z realizacją umowy.

[akta kontroli poz. 36, 53, 56]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych osobowych, jak również podejmowanych działań korygujących została uregulowana [redacted]

[akta kontroli poz. 29]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

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

Audyt bezpieczeństwa informacji jest procesem przeprowadzanym w celu zidentyfikowania zagrożeń mogących skutkować utratą poufności, integralności lub dostępności informacji. Celem audytu wewnętrznego bezpieczeństwa informacji jest ocena zakresu zgodności Systemu Zarządzania Bezpieczeństwem Informacji jednostki z kryteriami audytu.

[redacted]

Brak przeprowadzenia w okresie objętym kontrolą audytu wewnętrznego w zakresie bezpieczeństwa informacji, skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD kontrolowanej jednostki.

[akta kontroli poz. 42]

Przedmiotowe cząstkowe zagadnienie ocenia się **negatywnie**.

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie kopi zapasowych jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć wykonując regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

[redacted]

[redacted]

Na podstawie udostępnionej dokumentacji oraz wyjaśnień kontrolujący stwierdzili, że w Urzędzie są wykonywane kopie zapasowe z kontrolowanych systemów.
W PBPDO oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe brak jest jakichkolwiek procedur definiujących sposób dokumentowania tych czynności. Zaznaczyć również należy że uściślenia wymaga harmonogram wykonywania kopii zapasowych ujęty w PBPDO oraz Instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe, w stosunku do opisu faktycznie wykonywanych kopii, ujętego w przekazanych wyjaśnieniach.

[akta kontroli poz. 29, 42, 50-52]

W przypadku prowadzenia testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz przydatności utworzonych kopii podczas próby symulowanego przywrócenia

i uruchomienia oprogramowania, [redacted]

[redacted]

[akta kontroli poz. 29, 42, 43, 55]

[redacted]

W świetle powyższego, brak udokumentowania działań na miejscu w jednostce (protokół potwierdzający) w zakresie wykonywania testów w celu sprawdzenia poprawności wytworzonych kopii zapasowych, należy uznać za **uchybienie** skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Przyczyną powstania uchybienia jest niestosowanie przepisów prawa w tym zakresie oraz przyjętych norm. Osobą odpowiedzialną jest informatyk urzędu.

Regularne testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Prawidłowo zdefiniowana polityka kopii bezpieczeństwa oraz gruntownie przetestowane procesy odtwarzania systemów teleinformatycznych są istotnymi aspektami w każdej jednostce, której procesy opierają się na działaniu systemów informatycznych. Prawidłowo zdefiniowana i wykonana procedura pozwala mieć pewność, że w razie awarii systemu, wytworzone backupy spełnią swoje zadanie i nie odbije się to negatywnie na ciągłości działania jednostki.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami.**

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI 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.

[redacted] Na obsługę zainstalowanego w okresie objętym kontrolą oprogramowania (system informatyczny) zawarte zostały stosowne umowy licencyjne (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. Zakupiony system teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

[redacted]

[akta kontroli poz. 36, 43, 53, 56]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:

- 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 zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;

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

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego bieżącego dostępu uprawnionym użytkownikom, stosowany jest szereg zabezpieczeń technicznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

[akta kontroli poz. 42]

Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: 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, 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;
- § 20 ust. 4 rozporządzenia KRI 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.

W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, poprzez:

[redacted]

[redacted]

Stwierdzone uchybienie, skutkować może utratą przetwarzanych informacji w wyniku awarii sprzętu. [redacted]. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

[akta kontroli poz. 19-20]

Przedmiotowe cząstkowe zagadnienie ocenia się **pozytywnie z uchybieniami**.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

- § 21 ust. 2 rozporządzenia KRI 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;
- § 21 ust. 3 rozporządzenia KRI 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;
- § 21 ust. 4 rozporządzenia KRI 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.

Zgodnie z § 21 ust. 1 KRI, rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach). Z informacji uzyskanych w trakcie kontroli wynika, [redacted]

[akta kontroli poz. 42, 54]

Mając na uwadze powyższe, przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

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

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19 rozporządzenia

KRI, 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 KRI.

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.

Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego planu od tła. Niski poziom kontrastu utrudnia korzystanie z witryny przede wszystkim użytkownikom o mniejszej ostrości wzroku, a także osobom niedowidzącym. Celem ułatwienia postrzegania tekstu użytkownikom niedowidzącym można również umożliwić zmianę wielkości tekstu bez utraty jego czytelności lub funkcjonalności serwisu internetowego. Zarówno strona internetowa BIP Urzędu, jak i portal www. Urzędu, zawierała elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niedowidzące. Zastosowane ułatwienia to:

- możliwość doboru odpowiedniego kontrastu (ciemny-jasny),
- możliwość powiększenia wielkości liter na stronie,
- moduł wyszukiwania.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla portalu internetowego Urzędu, nie wykazała jakichkolwiek błędów. W przypadku strony BIP walidacja wykazała 1 błąd. Analiza ujawnionego błędu wskazuje na brak tekstu alternatywnego w przypadku powiązanego ze stroną obrazu (zdjęcia). Wskazane przez walidator zdjęcie, jest tzw. obrazem „powitalnym" nie przekazującym w swej treści ważnych dla korzystającego ze strony informacji.
WAVE-WCAG jest narzędziem do automatycznego testowania dostępności serwisów internetowych. Pomaga administratorom tworzyć bardziej dostępne strony internetowe. W wyniku automatycznej analizy wskazuje ewentualne miejsca, które mogą powodować problemy z dostępnością.

[akta kontroli poz. 39-41]

Mając na uwadze powyższe, przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

[redacted]

[redacted]

Proszę Pana Burmistrza o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

II WICEWOJEWODA
WARMIŃSKO-MAZURSKI
Piotr Opaczewski
/podpisano podpisem elektronicznym/