



Wydział Kontroli
FK-IV.431.2.2024

Szanowna Pani
Beata Mazur
Burmistrz Miasta i Gminy Miłomłyn
ul. Twarda 12
14-140 Miłomłyn

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

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Miasta i Gminy w Miłomłynie¹, ul. Twarda 12, 14-140 Miłomłyn, NIP jednostki: 741101370, REGON jednostki: 000540989.

- W okresie objętym kontrolą oraz w czasie prowadzonych czynności kontrolnych kierownikiem kontrolowanej jednostki był Pan **Stanisław Siwkowski** – Burmistrz, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 21.10.2018 r.
- W okresie objętym kontrolą oraz w dniu rozpoczęcia czynności kontrolnych odpowiedzialnym za realizację zadania objętego kontrolą był ██████████ zatrudniony na podstawie umowy o pracę od dnia 01.12.2006 r.,
- Osobą bezpośrednio nadzorującą pracownika odpowiedzialnego za realizację zadania był ██████████ zatrudniony na podstawie umowy o pracę od dnia 01.12.2008 r.

[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 1/2024, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.155.2024 z 6 marca 2024 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 Zwany dalej: Urzędem

Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.156.2024 z 6 marca 2024 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli poz. 9]

Kontrolę przeprowadzono w dniach 15 marca – 5 kwietnia 2024 r., co zostało odnotowane w książce kontroli Urzędu pod pozycją, Nr 2/2024.

[akta kontroli poz. 22]

Kontrola prowadzona była w trybie hybrydowym, tj. w dniu 15 marca br. – rozpoczęto czynności kontrolne w Urzędzie, dokonano oględzin serwerowni na miejscu w jednostce oraz sporządzono protokół z wykonanych czynności. Pozostałe dni (18 marca – 5 kwietnia 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.

[akta kontroli poz. 19]

~~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 ze zm.). Okres objęty kontrolą: od 1 stycznia do 31 grudnia 2023 r.~~

[akta kontroli poz. 1, 12]

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 ze zm.)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, 12]

² Zwanej dalej: ustawą

³ Zwanego dalej: rozporządzeniem KRI

Burmistrz upoważnił Informatyka (ASI) Urzędu, do udzielania informacji i wyjaśnień w okresie trwania czynności kontrolnych.

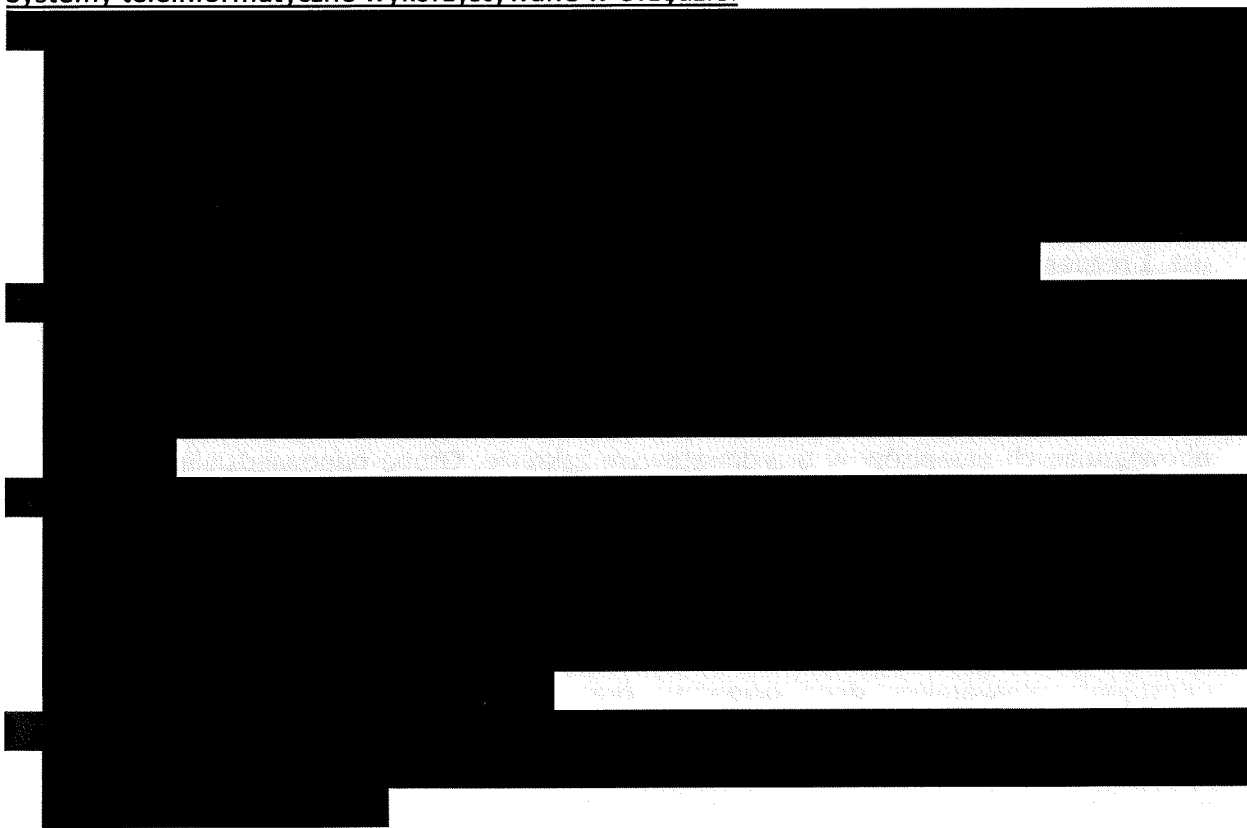
[akta kontroli poz. 17]

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 4 niżej wymienione systemy teleinformatyczne.

Systemy teleinformatyczne wykorzystywane w Urzędzie:



[akta kontroli poz. 10-11, 13]

- 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 osiągnięta 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 /umigmilomlyn/SkrytkaESP, znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Na stronie BIP Urzędu, zakładka dane teleadresowe → Urząd Miasta i Gminy, podano adres Elektronicznej Skrzynki Podawczej. Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: DOC, RTF, XLS, CSV, TXT, GIF, TIF, BMP, JPG, PDF, ZIP.

Podczas kontroli ustalono, że Urząd dysponuje Elektroniczną Skrzynką Podawczą (ESP), która działa zgodnie z określonymi prawnie wymogami. Na stronie internetowej BIP Urzędu wprowadzono informację o uruchomieniu ESP, jednakże nie opublikowano informacji 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 **uchybiecie** skutkujące niedoinformowaniem petentów 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 Portalu Urzędu (w lewej górnej jego części) istnieje zakładka „*eportal usług mieszkańca*”. 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 eUsług 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.

[akta kontroli poz. 23-25]

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągnięta 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 spraw urzędowych*”, opublikowany jest przydatny dla patentów wykaz usług, które realizowane są przez poszczególne wydziały Urzędu.

Ponadto na stronie BIP w powyższej zakładce opublikowane są karty z opisem danej usługi oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

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

[akta kontroli poz. 26]

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 ujednoczenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednoczenia 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 udostępniana 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.

[akta kontroli poz. 41]

Jednocześnie, na stronie BIP w zakładce „*Procedury spraw urzędowych*”, opublikowany jest przydatny dla patentów wykaz usług, które realizowane są przez poszczególne wydziały Urzędu.

Ponadto na stronie BIP w powyższej zakładce opublikowane są karty z opisem danej usługi oraz wzory wniosków i formularzy niezbędnych do załatwienia wybranych spraw, będących w zakresie działania poszczególnych wydziałów w Urzędzie.

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://www.milomlyn.pl/>, a strona internetowa BIP Urzędu – pod adresem <https://milomlyn.biuletyn.net/>

Na stronie głównej Portalu Urzędu, zawarto bezpośrednie odnośniki (linki) do przydatnych informacji oraz stron przeznaczonych dla mieszkańców Gminy.

Na stronie w zakładce „Procedury spraw urzędowych, opublikowany jest przydatny dla petentów wykaz usług, które realizowane są przez poszczególne wydziały Urzędu.

Ponadto na stronie głównej portalu Urzędu - w zakładce „eportal usług mieszkańca” (zgodnie z opisem w pkt 1.1), działa platforma połączona z systemami dziedzinowymi jednostki, dzięki której możliwa jest realizacja płatności w ramach zobowiązań wynikających z podatków i innych opłat w zakresie oferowanych usług.

[akta kontroli poz. 23-24, 26]

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych realizowanych przez kontrolowane 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. 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, modyfikację, usunięcie lub zniszczenie.

Zgodnie z wyjaśnieniem uzyskanym z Urzędu w przedmiotowej sprawie, cyt.: 



W okazanej dokumentacji Urzędu, kontrolujący nie stwierdzili dodatkowych opracowanych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby szczegółowe zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną.

Zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, opracowanie procedur umożliwi 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.

W związku z powyższym brak szczegółowych procedur dotyczących wykonywania czynności kancelaryjnych, w których określone byłyby zasady obiegu dokumentów wpływających i wypływających drogą elektroniczną ocenia się jako uchybienie. Stwierdzone uchybienie skutkować może brakiem zabezpieczenia informacji, w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Osobą odpowiedzialną jest Kierownik kontrolowanej jednostki.

Jednocześnie kontrolujący poddają pod rozważenie Kierownictwu kontrolowanej jednostki wprowadzenie na stałe w Urzędzie (wyjście z fazy testów) elektronicznego systemu zarządzania dokumentami, który z pewnością wpłynie na usprawnienie przepływu dokumentów w podmiocie, znacząco usprawni ich archiwizację oraz zapewni łatwy dostęp do dokumentów archiwalnych, co z kolei wpłynie na przyspieszenie załatwianych spraw w tym realizowanych przez podmiot usług oraz pozwoli na minimalizowanie nakładu pracy a także podniesie poziom Bezpieczeństwa Informacji. Celem wdrożenia systemu elektronicznego zarządzania dokumentacją jest wyeliminowanie z obiegu wewnętrznego podmiotu dokumentów papierowych, co spowodowałoby dodatkowo obniżenie kosztów.

[akta kontroli poz. 41]

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

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”, w celu zapewnienia jednolitego i adekwatnego systemu zarządzania bezpieczeństwem danych w Urzędzie, [REDACTED]

[akta kontroli poz. 30-31]

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 zarządzania 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.

[REDAKTION]

Odnosząc się do przekazanych wyjaśnień, należy stwierdzić, że w Urzędzie nie opracowano i nie wdrożono całościowej SZBI, w szczególności nie wdrożono zaktualizowanej polityki bezpieczeństwa informacji - PBI. Opracowana i wdrożona Polityka Ochrony Danych Osobowych, nie obejmowała wszystkich informacji jakie są przetwarzane w Urzędzie, lecz przede wszystkim dane osobowe. 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. Przyczyną nieprawidłowości jest niestosowanie przepisów i wytycznych w tym zakresie. 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.

[REDAKTION]

Odnosząc się do przekazanego wyjaśnienia, należy stwierdzić, że w Urzędzie w 2023 r. nie były prowadzone dodatkowe działania w postaci kontroli oraz sprawdzeń, w zakresie utrzymania oraz zarządzania bezpieczeństwem informacji obejmujące jego monitoring i przegląd, a jedynie doraźne działania w ramach codziennych zadań, z których brak jest dokumentacji potwierdzającej ich przeprowadzenie. Ze względu na brak przedmiotowej dokumentacji, kontrolujący nie mogą zweryfikować ich faktycznego przeprowadzenia (rozliczalność).

Brak okresowych przeglądów i monitoringu SZBI w jednostce, należy **ocenić jako uchybienie** skutkujące naruszeniem § 20 ust. 1 rozporządzenia KRI. Osobą odpowiedzialną jest IOD jednostki pełniący funkcję w okresie objętym kontrolą.

Jednocześnie należy wskazać, że 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, że 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. 41]

Burmistrz powołał w jednostce Inspektora Ochrony Danych (IOD) oraz Administratora Systemów Informatycznych (ASI).

[akta kontroli poz. 43-44]

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, rozliczalności lub poufności danych osobowych w Urzędzie w październiku 2022 roku.

Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI analiza ryzyka utraty integralności, dostępności lub poufności informacji powinna być przeprowadzana okresowo. Zdaniem kontrolujących

w uzupełnionej PBI, należy zamieścić zapisy wskazujące (definiujące) „okresowość”, w odniesieniu do przeprowadzania analiza ryzyka. Wskazanie konkretnego okresu (np. co rok) umożliwi kontrolującym weryfikację wywiązania się z ustawowego obowiązku. Jednocześnie należy wskazać, że w przedstawionej kontrolującym analizie ryzyka, błędny jest zapis dotyczący wejścia w życie zapisów dokumentu (10.08.2018), w odniesieniu do daty wdrożenia dokumentu (12.10.2022), świadczący o obowiązywaniu zapisów analizy, przed ich wdrożeniem (wstecznie).

[akta kontroli poz. 45]

W toku prowadzonych czynności kontrolnych stwierdzono, że w jednostce zgodnie z art. 30 RODO, prowadzony jest rejestr czynności przetwarzania.

[akta kontroli poz. 46-50]

Mając powyższe na uwadze przedmiotowe częściowe 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.

Z informacji uzyskanych z Urzędu wynika, że, cyt.: „*Nie posiadamy innej ewidencji sprzętu.*”

Zgodnie z przyjętym Programem kontroli nie sporządzanie bieżącej i aktualnej informacji nt. sprzętu i oprogramowania wykorzystywanego do przetwarzania informacji, zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI **stanowi uchybienie**, skutkujące naruszeniem cytowanego przepisu. 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. 41, 51]

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

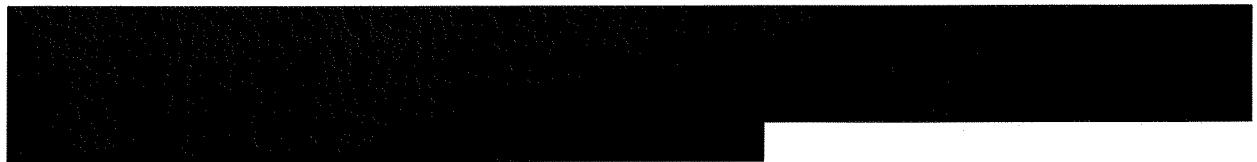
2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

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.



Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienia do ich przetwarzania oraz do przetwarzania danych osobowych w określonym zbiorze danych (systemie), wynikającym z zakresu czynności danego pracownika. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych.

[akta kontroli poz. 32-33]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

W okresie objętym kontrolą w Urzędzie przeprowadzono szkolenie wynikające z § 20 ust. 2 pkt 6 rozporządzenia KRI, w szczególności dla osób zaangażowanych w proces przetwarzania danych. Udział w szkoleniu doskonalącym w zakresie ochrony danych osobowych oraz cyberbezpieczeństwa, potwierdzono listą obecności.

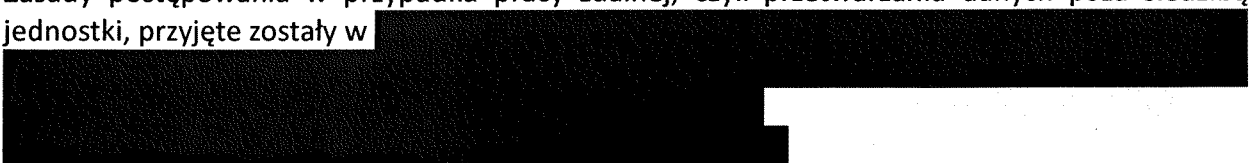
[akta kontroli poz. 34]

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.

Zasady postępowania w przypadku pracy zdalnej, czyli przetwarzania danych poza siedzibą jednostki, przyjęte zostały w



[akta kontroli poz. 31, 41, 52]

Mając powyższe na uwadze przedmiotowe częściowe 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.



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. 54-56]

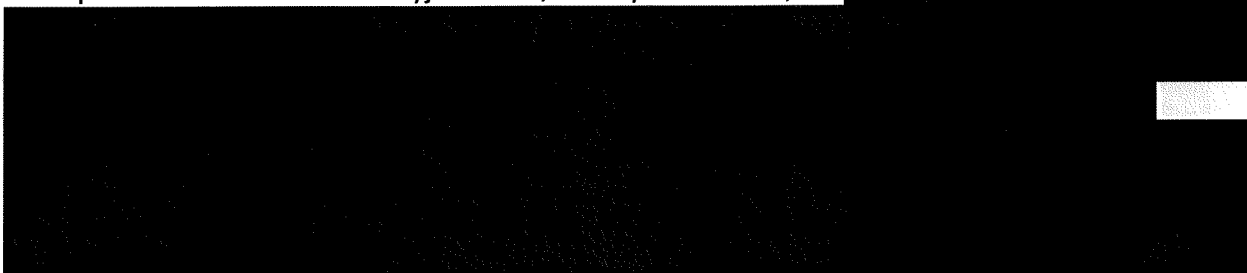
Mając powyższe na uwadze przedmiotowe częściowe zagadnienie ocenia się pozytywnie.

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.



W odpowiedzi na udzielone wyjaśnienie, należy stwierdzić, że



[REDAKTION]

W wyniku przeprowadzonej kontroli stwierdzono, że Urząd nie posiadał szczegółowych formalnych zasad zarządzania incydentami – co kwalifikuje się jako uchybienie, a wprowadzone ogólne regulacje nie stanowiły kompletnego systemu, ponieważ nie obejmowały takich zagadnień Jak np.:

- identyfikacja (w tym definicja incydentu), analiza, nadawanie priorytetów, wyszukiwanie powiązań, podejmowanie działań naprawczych, zasady gromadzenia materiału dowodowego dla użytkowników, informacje o ewentualnym postępowaniu dyscyplinarnym dla pracowników, czy też usuwanie przyczyn incydentów;
- precyzyjne określenie w regulacjach zadań i odpowiedzialności dla istotnych ról wskazanych w procesie zarządzania incydentami.

Przyczyna stwierdzonego uchybienia jest opracowanie niepełnych procedur w zakresie § 20 ust. 2 pkt 13 rozporządzenia KRI, co skutkować może niewłaściwym postępowaniem pracowników w przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji. Osoba odpowiedzialna za powstanie uchybienia jest IOD jednostki. Należy jednocześnie podkreślić, że ustanowienie i wdrożenie prawidłowej procedury zarządzania incydentami, uwzględniającej podział zadań i odpowiedzialności, przejrzyste zasady postępowania w sytuacjach wystąpienia zagrożeń, pozwalające na szybkie podjęcie działań korygujących, jest istotnym narzędziem wspierającym proces doskonalenia SZBI.

[akta kontroli poz. 41]

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

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.

[REDAKTION]

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. 41, 53]

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 kopii 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 text block]

[Redacted text block]

Mając na względzie wyjaśnienia uzyskane z Urzędu, w przedmiotowej sprawie należy podnieść fakt, że zarówno w przypadku tworzenia kopii zapasowych, jak i wykonywania testów odtworzeniowych przydatności kopii zapasowych, kontrolujący oparli się tylko i wyłącznie na wyjaśnieniach jednostki, gdyż w przekazanej dokumentacji nie odnaleziono dowodów świadczących o ich wykonywaniu.

[Redacted text block]

Mając powyższe na uwadze należy stwierdzić, że w okresie objętym kontrolą nie wytworzono dokumentacji (rozliczalność) potwierdzającej wykonywanie kopii zapasowych oraz prowadzenie testów odtworzeniowych (np. notatki, wpisy w dzienniku systemowym). Brak dokumentacji świadczącej o wykonaniu kopii zapasowych oraz testów odtworzeniowych, **należy uznać za**

uchybiecie, skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Przyczyną powstania uchybienia jest niestosowanie przepisów prawa w tym zakresie. Osobą odpowiedzialną za uchybienie jest Informatyk jednostki oraz osoba dokonująca przeglądów PODO.

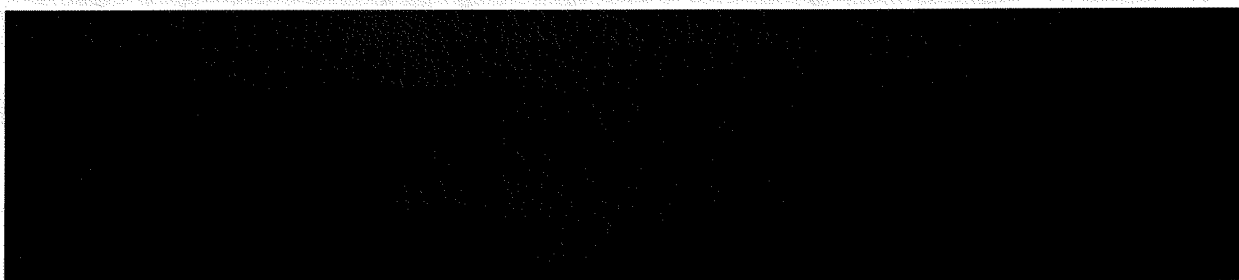
[akta kontroli poz. 35, 41]

Regularne tworzenie i 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 częściowe 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.



[akta kontroli poz. 13, 54-56]

Mając powyższe na uwadze przedmiotowe częściowe zagadnienie ocenia się **pozytywnie**.

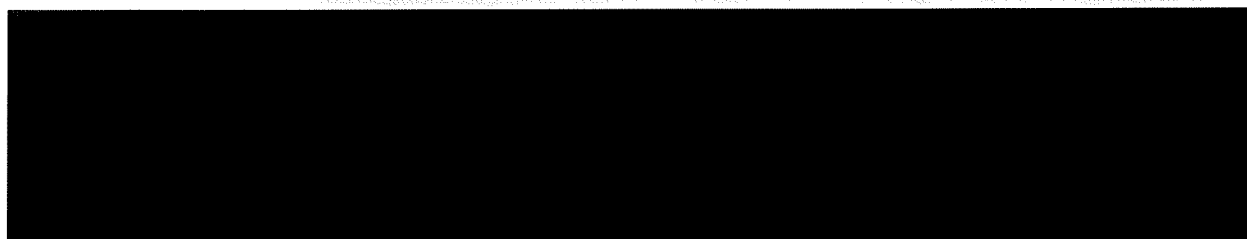
2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

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. 41]

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]

Podczas kontroli dokonano oględzin pomieszczenia serwerowni w Urzędzie, w obecności Pana Wojciecha Ignaczaka Informatyka w Urzędzie Miasta i Gminy Miłomłyn.

W toku oględzin dokonano ustalenia stanu faktycznego i stwierdzono:

[REDACTED]

Ponadto, stwierdzono następujące uchybienie:

[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, że cyt.: 



Rozliczalność jest właściwością systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie, zatem zapewnienie rozliczalności działań polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszystkie działania dostępu do systemu z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i zabezpieczeń, a także działania, gdy przetwarzanie danych podlega prawnej ochronie (np. zgodnie z ustawą o ochronie danych osobowych). Informacje zawarte w dziennikach systemowych powinny być regularnie przeglądane w celu wykrycia działań niepożądanych/nieuprawnionego dostępu oraz powinny być przechowywane w bezpieczny sposób, **co najmniej 2 lata**.



[akta kontroli poz. 41]

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

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 m.in.:

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

Dostępność cyfrowa to cecha rozwiązań cyfrowych (np. stron, aplikacji, systemów), która umożliwia samodzielne korzystanie z nich przez osoby z niepełnosprawnościami. Jednocześnie wiele jej elementów jest uniwersalnych (np. kontrast, napisy), poprawiających użyteczność każdemu, a nie tylko osobom niepełnosprawnym.

Dostępne cyfrowo muszą być między innymi strony internetowe, aplikacje mobilne, systemy teleinformatyczne i wszystkie treści publikowane w Internecie przez podmioty publiczne. To wyzwanie wdrożeniowe, ale także szansa na dotarcie z informacjami i usługami do szerokiej grupy użytkowników, w tym osób z niepełnosprawnościami.

Jednocześnie należy zaznaczyć, że pomimo tego, że dana strona zawiera podstawowe elementy umożliwiające korzystanie z treści na niej zawartych przez osoby niepełnosprawne (np. kontrast, powiększenie czcionki, wyszukiwanie), to strona ta wcale nie musi z automatu spełniać kryteriów dostępności cyfrowej.

Walidacja za pomocą narzędzia <http://wave.webaim.org> tj. walidatora WAVE-WCAG 2.0 dla strony BIP nie wykazała błędów, natomiast walidacja portalu internetowego Urzędu, wykazała 1 błąd dotyczący bardzo niskiego kontrastu pomiędzy kolorami tekstu i tła, w przypadku wskazanego adresu e-mail Urzędu. 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.

Brak pełnej zgodności z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, należy ocenić jako uchybienie. Przyczyną uchybienia jest częściowe niedostosowanie stron internetowych do standardów dostępności, w tym WCAG 2.0.

Skutek uchybienia - brak zapewnienia maksymalnego wsparcia osobom niepełnosprawnym. Odpowiedzialnym za powstanie uchybienia jest osoba nadzorująca portal internetowy kontrolowanej jednostki.

[akta kontroli poz. 27-29]

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

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny, wnoszę o:

[Redacted content]

Proszę Panią Burmistrz o podjęcie działań mających na celu usunięcie stwierdzonych 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.

WOJEWODA
WARMIŃSKO-MAZURSKI
Radosław Król

/podpisano podpisem elektronicznym/