



WOJEWODA ŚWIĘTOKRZYSKI

Znak: OK.V.431.1.2018

Kielce, dnia 31-07-2018

Pan

Sebastian Nowackiewicz

Wójt Gminy Sitkówka-Nowiny

WYSTĄPIENIE POKONTROLNE

Kontrolę problemową w Urzędzie Gminy Sitkówka-Nowiny w dniach 12-14 czerwca 2018 roku przeprowadził zespół kontrolerów w składzie:

Marek Rak, Informatyk Wojewódzki – Kierownik Oddziału ds. Informatyki w Wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego - Przewodniczący Zespołu Kontrolnego – na podstawie pisemnego upoważnienia do kontroli numer 346/2018 wydanego z upoważnienia Wojewody przez Dyrektora Wydziału Organizacji i Kadr.

Maciej Terek Główny Specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego - Członek Zespołu Kontrolnego – na podstawie pisemnego upoważnienia do kontroli numer 345/2018 2018 wydanego z upoważnienia Wojewody przez Dyrektora Wydziału Organizacji i Kadr.

Zakres kontroli i okres objęty kontrolą:

Zakres kontroli obejmował działanie systemów teleinformatycznych używanych do realizacji zadań publicznych w okresie od 1.01.2017 r. do 12.06.2018 r. zgodnie z Rozporządzeniem 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 dnia 16 maja 2012 r. poz. 526) wydanym na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64 poz. 565, z późn. zm.). Ocenie podlegały trzy główne obszary tematyczne:

- 1) Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie usług drogą elektroniczną.
- 2) System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
- 3) Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych.

Wykonywanie zadań w kontrolowanym zakresie oceniam pozytywnie z nieprawidłowościami.

USTALENIA KONTROLI	
Akty prawne, na podstawie których dokonano ustaleń w toku kontroli	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych ¹
Obszar kontroli : 1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie usług drogą elektroniczną	
1.1 usługi elektroniczne	
Podstawa prawna	§ 5 ust.2 pkt.1 i pkt.4 rozporządzenia: Interoperacyjność na poziomie organizacyjnym osiągnięta jest przez : • pkt.1 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 • pkt.4 Publikowanie i aktualizowanie w BIP przez przedmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Urząd jedynie na swojej stronie BIP w zakładce „załatwianie spraw” umieścił zakładkę „elektroniczna skrzynka podawcza” a w niej bardzo ogólne informacje (podstawę prawną) wraz z linkiem do serwisu ePUAP http://epuap.gov.pl. Nie umieszczono żadnego opisu procedury realizacji usługi przekazywania, składania dokumentów drogą elektroniczną. Na stronie głównej UG w zakładce kontakty podano adres skrzynki podawczej UG w Sitkowie-Nowiny. Skrzynka systemu epuap obsługiwana jest przez informatyka i przez sekretariat UG. Dowód :akta kontroli plik : Nowiny-BIP-skrytka-1.pdf Strona-UG-skrytka.pdf
Ustalane uchybienia, nieprawidłowości	Kontrolujący nie znaleźli na stronach UG (również BIP) żadnej informacji mówiącej o tym iż można złożyć dokument w postaci elektronicznej poprzez pocztę elektroniczną lub poprzez osobiste przyniesienie dokumentu

¹ Dz. U. z 2016 r., poz. 113, zwane dalej „rozporządzeniem”.

	w postaci elektronicznej na nośniku informatycznym.
1.2 centralne repozytorium wzorów dokumentów elektronicznych	
Podstawa prawna	Art. 19 b ust. 3 ustawy: Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Urząd w badanym okresie nie przekazywał żadnych wzorów dokumentów do centralnego repozytorium wzorów dokumentów elektronicznych. Dowód: akta kontroli plik Załącznik-1 Ankieta, pozycja G12
1.3 Model usługowy	
Podstawa prawna	§ 15 ust. 2 rozporządzenia: Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Urząd nie realizuje i nie zarządza usługami które mają na celu dostarczenie usług na deklarowanym poziomie dostępności. Nie ma opracowanych procedur. Posiadane systemy informatyczne nie wspierają modelu usługowego.
1.4 Współpraca systemów informatycznych z innymi systemami	
Podstawa prawna	§ 5 ust. 3 pkt 3 rozporządzenia: Interoperacyjność na poziomie semantycznym osiągnięta jest przez, m.in. stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań. § 16 ust. 1 rozporządzenia: 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zakres i sposób współpracy systemów informatycznych wewnątrz Urzędu oraz ich współpracy z systemami zewnętrznymi (m.in. innych jednostek administracji publicznej) zbadano na próbie wybranych systemów : • Bestia program do zarządzania budżetami jednostek samorządu terytorialnego • Mikropesel – ewidencja ludności Bestia, program współpracuje z systemem TREZOR (system obsługi budżetu państwa). W programie Bestia generowane są paczki ze sprawozdaniami, program posiada również funkcje które pozwalają na śledzenie wysłanych paczek ze sprawozdaniami patrz funkcja sprawdź status. Mikropesel, program do zarządzania bazą mieszkańców gminy, może pobrać dane z systemu Źródło poprzez moduł SUBSKRYPCJA, w tym przypadku pobieranie tzw. Subskrypcji następuje automatycznie po wybraniu opcji subskrypcja. Wyżej wymienione systemy funkcjonujące w urzędzie gminy są wyposażone w składniki sprzętowe i programowe umożliwiające wymianę danych pomiędzy systemami teleinformatycznymi za pomocą protokołów komunikacyjnych.
1.5 Obieg dokumentów w urzędzie	
Podstawa prawna	§ 20 ust. 2 pkt 9 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególność 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W urzędzie gminy nie wdrożono elektronicznego systemu obiegu dokumentacji, obowiązuje papierowy system wykonywania czynności kancelaryjnych, jako podstawowy sposób załatwiania i rozstrzygania spraw.
1.6 Formaty danych udostępniane przez systemy informatyczne	
Podstawa prawna	§ 17 ust. 1 rozporządzenia: Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków,

	odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą. § 18 ust. 1 rozporządzenia: Systemy teleinformatyczne podmiotów realizujących zadania publiczne, udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia. § 18 ust. 2 rozporządzenia: Jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	System Bestia (zarządzanie budżetem jednostki samorządu terytorialnego) wymiana danych pomiędzy innymi systemami odbywa poprzez generowane pliki w formacie XML. System Mikropesel (zarządzanie bazą mieszkańców gminy) urządzenie gminy nie posiadał dokumentacji, na podstawie której można określić w jakim formacie system Mikropesel pobiera informacje z systemu Źródło za pomocą modułu subskrypcja.
Ocena obszaru kontroli	Pozytywna z nieprawidłowościami
Obszar kontroli : 2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych	
2.1 Dokumenty z zakresu bezpieczeństwa informacji. Zaangażowanie kierownictwa podmiotu	
Podstawa prawna	§ 20 ust. 1 rozporządzenia: Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. § 20 ust. 2 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji. § 20 ust. 2 pkt 1 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie

	aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Zarządzenie Nr WG.173.2015 Wójta Gminy Sitkówka-Nowiny z dnia 30 grudnia 2015 roku dotyczy jedynie części procedur wynikających z ustawy o ochronie danych osobowych i aktów wykonawczych pominięto zupełnie regulacje wynikające z Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności. Brak dokumentacji w tym zakresie wykazał przeprowadzony w roku 2016 audyt w zakresie bezpieczeństwa informacji Dowód :akta kontroli plik : Zarządzenie-WG-173-2015.pdf
Ustalone uchybienia, nieprawidłowości	W UG nie opracowano, a tym samym nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji. Ograniczono się jedynie do opracowania Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznych służącym do przetwarzania danych osobowych tylko w zakresie danych osobowych. Ostatnia aktualizacja regulacji wewnętrznych została wykonana na koniec roku 2015. Przez ostatnie dwa lata czyli 2016-2017 do dnia kontroli nie dokonano przeglądu dokumentacji w celu aktualizacji. Zgodnie z Zarządzeniem nr WG.173.2015 Wójta Gminy Sitkówka-Nowiny z dnia 30 grudnia 2015 roku w sprawie ochrony danych osobowych w Urzędzie Gminy Sitkówka-Nowiny w załączniku numer 1 „Polityka Bezpieczeństwa u Urzędzie Gminy Sitkówka-Nowiny” część II, § 8, punkt a) i b) napisano iż ASI raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego polegający na ustaleniu poprawności działania. W urzędzie gminy nie ma żadnej dokumentacji świadczącej o wykonywaniu przeglądów systemów informatycznych przez ASI. Nie zastosowano się również do rekomendacji po audytowych z roku 2016.
2.2 Analiza zagrożeń związanych z przetwarzaniem informacji	
Podstawa prawna	§ 20 ust. 2 pkt 3 rozporządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Brak przeprowadzonej analizy ryzyka w UG roku 2017 do dnia kontroli. Przeprowadzony audyt w roku 2016 wskazuje na brak przeprowadzenia analizy ryzyka również w roku 2016. Reasumując od co najmniej trzech lat w UG nie przeprowadzono analizy ryzyka utraty integralności, dostępności lub poufności informacji. (brak identyfikacji aktywów, zagrożeń, zabezpieczeń, podatności, następstw). Dowód: akta kontroli plik 2018-06-12-13-56-31-01-2016-audyt, strona 7
Ustalane uchybienia, nieprawidłowości	Do dnia zakończenia czynności kontrolnych nie przedstawiono dokumentów potwierdzających wykonywanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co stanowi naruszenie § 20 ust. 2 pkt 3 rozporządzenia.
2.3 Inwentaryzacja sprzętu i oprogramowania informatycznego	
Podstawa prawna	§ 20 ust. 2 pkt 2 Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Nie ma prowadzonego inwentarza sprzętu i oprogramowania informatycznego. W roku 2016 był prowadzony inwentarz sprzętu i oprogramowania informatycznego za pomocą specjalistycznego oprogramowania komputerowego, co potwierdza również przeprowadzony w roku 2016 audyt bezpieczeństwa informacji. W 2017 roku z niewyjaśnionych powodów zaniechano prowadzenie inwentarza sprzętu i oprogramowania informatycznego.
Ustalane uchybienia, nieprawidłowości	UG w Sitkówce –Nowiny nie prowadzi ani nie utrzymuje aktualnego inwentarza sprzętu komputerowego i oprogramowania.
2.4 Zarządzanie uprawnieniami do pracy w systemach informatycznych	
Podstawa prawna	§ 20 ust. 2 pkt 4: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. § 20 ust. 2 pkt 5 Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez

	m.in. zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Ustalono iż pracownicy posiadają stosowne uprawnienia w systemach informatycznych, adekwatne do realizowanych zadań określonych w zakresach obowiązków. Brak jest natomiast zdefiniowanych procedur związanych z nadawaniem uprawnień w systemach informatycznych, otwieraniem i zamykaniem kont. Zgodnie z Zarządzeniem nr WG.173.2015 Wójta Gminy Sitkówka-Nowiny z dnia 30 grudnia 2015 roku w sprawie ochrony danych osobowych w Urzędzie Gminy Sitkówka-Nowiny w załączniku numer 1 „Polityka Bezpieczeństwa u Urzędzie Gminy Sitkówka-Nowiny” część II, § 1, punkt a) i b), napisano iż użytkownik po uzyskaniu upoważnienia oraz podpisaniu oświadczenia składa ustnie wnioski do ASI o nadanie identyfikatora i hasła do systemu informatycznego. Zapis o złożeniu ustnego wniosku powoduje to że cała procedura zakładania konta w systemie informatycznych nie posiada atrybutu rozliczalności zgodnie z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności. Dowód :akta kontroli plik : Zarządzenie-WG-173-2015.pdf, załącznik nr2
Ustalane uchybienia, nieprawidłowości	Brak opracowanych procedur zakładania i likwidacji kont w systemach informatycznych co powoduje iż te czynności nie posiadają atrybutu rozliczalności.
2.5 Szkolenia pracowników zaangażowanych w proces przetwarzania informacji	
Podstawa prawna	§ 20 ust. 2 pkt 6 Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	UG nie okazał żadnej dokumentacji świadczącej o przeprowadzonych szkoleniach pracowników w roku 2017, natomiast w roku 2018 zostało przeprowadzonych szereg szkoleń związanych „Reformą ochrony danych osobowych przygotowanie do RODO”, oraz szkolenie

	w zakresie ochrony danych osobowych.
Ustalono uchybienia, nieprawidłowości	Nie przeprowadzono w roku 2017 szkoleń pracowników z zagadnień: • Zagrożeń bezpieczeństwa informacji • Skutków naruszenia zasad bezpieczeństwa informacji w tym odpowiedzialności prawnej • Stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko ludzkich błędów.
2.6 Praca na odległość i mobilne przetwarzanie danych	
Podstawa prawna	§ 20 ust. 2 pkt 8: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych z dnia 30 grudnia 2015, nie opracowano procedur tzw. pracy na odległość czy mobilnego przetwarzania danych. W UG Sitkówka-Nowiny nie wykorzystuje się mobilnego przetwarzania danych ani pracy na odległość. Dowód :akta kontroli plik : Zarządzenie-WG-173-2015.pdf, załącznik nr2
2.7 serwis sprzętu komputerowego i oprogramowania	
Podstawa prawna	§ 20 ust. 2 pkt 10: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Badaniem w zakresie zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji objęto umowę na licencję i serwis systemu Mikropesel z roku 2018 (Nr 173/COI/L/2018/SMP) z Centralnym Ośrodkiem Informatyki z siedzibą w Warszawie. W paragrafie 4 niniejszej umowy zostały zawarte zapisy gwarantujące przestrzeganie wymogów wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, o powierzeniu przetwarzania danych osobowych, o przetwarzaniu danych osobowych na urządzeniach i oprogramowaniu zapewniającym wysoki poziom bezpieczeństwa Dowód :akta kontroli plik : 2018-06-12-14-04-43-01-2018-umowa-Mikropesel

2.8 Procedury zgłaszania incydentów naruszenia BI	
Podstawa prawna	§ 20 ust. 2 pkt 13: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określonym i z góry ustalony sposób, umożliwiając szybkie podjęcie działań korygujących.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych z dnia 30 grudnia 2015 r. w paragrafie 14 opisano bardzo ogólnie procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego. Procedura ta nie posiada atrybutów rozliczalności, w urzędzie gminy brak jakiegokolwiek dokumentacji w tym zakresie. Nie został opracowany rejestr incydentów oraz nie ma procedury zgłaszania incydentów. Zwracał na ten fakt uwagę również przeprowadzony audyt bezpieczeństwa informacji w roku 2016 Dowód: akta kontroli plik : Zarządzenie-WG-173-2015.pdf, załącznik nr2
Ustalane uchybienia, nieprawidłowości	Brak opracowanej procedury zgłaszania incydentów, brak szkolenia pracowników urzędzie gminy w tym zakresie. Brak prowadzonego rejestru incydentów.
2.9 Audyt wewnętrzny z zakresu bezpieczeństwa informacji	
Podstawa prawna	§ 20 ust. 2 pkt 14: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez m.in. zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Audyt bezpieczeństwa informacji został przeprowadzony przez firmę zewnętrzną w roku 2016. W urzędzie gminy znajduje się dokumentacja po audytowa zawierająca zalecenia, rekomendacje. Niestety nie uwzględniono zaleceń i rekomendacji po audytowych z roku 2016, również nie przeprowadzono audytu w roku 2017.
Ustalane uchybienia, nieprawidłowości	Brak przeprowadzonego audytu bezpieczeństwa informacji w roku 2017, nie wykonanie zaleceń, rekomendacji po audytowych z roku 2016
2.10 Kopie zapasowe	
Podstawa prawna	§ 20 ust. 2 pkt 12 lit. b: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. minimalizowanie ryzyka utraty informacji w wyniku awarii.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych z dnia 30 grudnia 2015

	w paragrafie 4 określono parametry tworzenia kopii bezpieczeństwa, kopia przyrostowa raz na miesiąc, kopia pełna raz na rok. Kopie przechowywane są na pamięci przenośnej w szafie zamykanej na klucz w pomieszczeniu informatyka.
Ustalone uchybienia, nieprawidłowości	Procedury które zostały opracowane nie posiadają atrybutów rozliczalności, niezawodności. Nie została opracowana dokumentacja dotycząca jakie zbiory podlegają procesowi sporządzania kopii zapasowych, w jakich terminach, nie ma informacji o sprawdzaniach kopii zapasowych pod względem integralności danych. Dowód :akta kontroli plik : Zarządzenie-WG-173-2015.pdf, załącznik nr2
2.11 Projektowanie, wdrażanie i eksploataowanie systemów teleinformatycznych	
Podstawa prawna	§ 15 ust. 1 rozporządzenia: Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	System Bestia (zarządzanie budżetem jednostki samorządu terytorialnego) został opracowany, stworzony i wdrożony w jednostkach samorządu terytorialnego na potrzeby Ministerstwa Finansów które jest właścicielem wszystkich praw autorskich i majątkowych do programu. System Mikropesel został opracowany i stworzony przez Centralny Ośrodek Informatyki który jest instytucją utworzoną przez Ministra Spraw Wewnętrznych i Administracji. Urząd gminy nie posiada dokumentacji związanej z projektowaniem, wdrożeniem systemu Mikropesel.
2.12 Bezpieczeństwo techniczno-organizacyjne dostępu do informacji	
Podstawa prawna	§ 20 ust. 2 Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in.: pkt 7: zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

	pkt 9: zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. pkt 11 rozporządzenia: ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych z dnia 30 grudnia 2015 w paragrafach 1-6 określono sposoby i warunki dostępu do danych, określono poziom złożoności i długości i ważności hasła w AD, określono procedury rozpoczęcia i zakończenia pracy w systemach informatycznych. System Bestia i system Mikropesel posiadają wbudowane moduły umożliwiające śledzenie czynności wykonywanych przez użytkowników ze standardowymi uprawnieniami jak również użytkowników z uprawnieniami administratora. Również system informatyczny oparty o Windows Serwer 2008 posiada takie narzędzia. Zakupiono w roku 2018 serwer NAS z przeznaczeniem na kopie bezpieczeństwa. Podczas kontroli serwer ten był w fazie wdrożenia w urzędzie gminy. Dowód :akta kontroli plik : Załącznik-do-protokołu-ogłędzin.doc, strona 2
2.13 Zabezpieczenia techniczno-organizacyjne systemów informatycznych	
Podstawa prawna	§ 20 ust. 2 pkt 12 zarządzenia: Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez, m.in. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, utratą nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po

	dostreżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa. § 20 ust. 4 zarządzenia: 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.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Urząd gminy zabezpieczył stanowiska komputerowe w zasilacze awaryjne (sprawdzone zostało stanowisko systemu Bestia, Mikropesel, CEIDG), zainstalowane oprogramowanie antywirusowe, pokoje wyposażono w szafy zamykane na klucz. Serwerownia zabezpieczona systemem antywłamaniowym, przeciwpożarowy, zamontowane urządzenia klimatyzacji. Urządzenia aktywne zamontowane w szafie dystrybucyjnej podłączone do zasilaczy awaryjnych. Dowód :akta kontroli plik : Załącznik-do-protokołu-ogłędzin.doc, strony 2,4,7,10
Ustalane uchybienia, nieprawidłowości	Nie zminimalizowano ryzyka utraty informacji w wyniku awarii, nie zapewniono bezpieczeństwa plików systemowych, zdefiniowane w Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych z dnia 30 grudnia 2015 parametry wykonywania kopii bezpieczeństwa są nie wystarczające, nie zdefiniowano również zbiorów podlegających archiwizacji. System wykonywania kopii bezpieczeństwa oparty o serwer NAS był w fazie wdrożenia. Nie kontrolowano systemów informatycznych co do ich zgodności z odpowiednimi normami i politykami bezpieczeństwa. Nie przeprowadzono analizy ryzyka
2.14 Rozliczalność działań w systemach teleinformatycznych	
Podstawa prawna	§ 21 ust. 2 rozporządzenia: W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

	§ 21 ust. 3 rozporządzenia: w zakresie wynikającym z analizy ryzyka poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka. § 21 ust. 4 rozporządzenia: informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	W systemach teleinformatycznych Urzędu dostęp do przetwarzanych informacji odbywa się przez uprawnione osoby i procesy w ustalonym zakresie. W dziennikach systemu informatycznego można dokonać weryfikacji kto, kiedy i co wykonywał. W rejestrach programu Bestia i Mikropesel można zidentyfikować wykonywane czynności przez użytkownika.
Ustalone uchybienia, nieprawidłowości	W toku przeprowadzenia czynności kontrolnych stwierdzono brak mechanizmów i przepisów wewnętrznych regulujących przechowywanie zapisów z dzienników systemów teleinformatycznych, brak kopii zapasowych.
Ocena obszaru kontroli	Negatywna
Obszar kontroli : 3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych	
3.1 Czy system teleinformatyczny spełnia wymagania WCAG 2.0 z uwzględnieniem poziomu AA, określonym w załączniku nr 4 do rozporządzenia KRI?	
Podstawa prawna	§ 19 rozporządzenia: W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.
Ustalenie stanu faktycznego, stanowiące podstawę do oceny	Strona https://nowiny.com.pl posiada zdefiniowany link do strony w wersji dla osób niedowidzących. Dostęp do tego linku za pomocą klawiatury problematyczny. Strona dla osób

	niedowidzących posiada opcje wysokiego kontrastu, pomniejszania i powiększania tekstu. Poruszanie się po stronie za pomocą klawiatury jest praktycznie niemożliwe, dostępne są jedynie listy wyboru natomiast dostęp do treści z poszczególnych list jest niemożliwy lub bardzo utrudniony. Pliki graficzne nie posiadają uzupełnionych atrybutów alt np. (takich miejsc jest wiele) <pre> <ul class="slides"> </pre> W tym przypadku również zasłaniają listę wyboru co utrudnia do niej dostęp oraz dostęp do informacji na stronie. Np. informacje dla mieszkańców a dalej informacje o telefonach do wydziałów urzędu gminy, czy dostęp do formularzy, wniosków czy deklaracji. Zastosowane tabele w stronach np. przyroda, przerwa w dostawie prądu nie posiadają opisów nagłówków, brak znaczników <pre> <table> <caption>Tytuł</caption> <tr><th>Nagłówek</th></tr> <tr><td>Treść komórki</td></tr> </table> </pre> Informacje w zakładce np. <i>Zamknięcie ulicy Chorzowskiej</i> informacja jest podana w formie skanu dokumentu co powoduje że jest niezgodna z WCAG 2.0 (1.4.5 AA), nieoczywista obsługa strony za pomocą klawiatury (2.1). Poruszając się klawiaturą po elementach serwisu (nie ma wyróżnienia elementu aktywnego) co powoduje, że nie wiemy na którym elemencie się aktualnie znajdujemy (2.4.7). Skróty zamieszczone na stronie nie posiadają dodatkowego opisu za pomocą znaczników <abbr>, <acronym>
Ustalone uchybienia, nieprawidłowości	Strona internetowa w wersji dla osób niedowidzących posiada wiele błędów które praktycznie uniemożliwiają dostęp do podstawowych informacji. Najważniejsze błędy to rozmieszczenia grafiki, sposób prezentacji informacji. Utrudniony dostęp do wersji strony dla osób niepełnosprawnych za pomocą zdefiniowanego linku na głównej stronie urzędu gminy. Utrudniony dostęp do funkcjonalności serwisu za pomocą klawiatury. Dowód :akta kontroli plik :

	Nowiny-WCAG-20-1.pdf
Ocena obszaru kontroli	Pozytywna z nieprawidłowościami
ZALECENIA	• Opracować i opublikować na stronie BIP procedury dotyczące składania dokumentów w formie elektronicznej w urzędzie gminy. • Zaktualizować, opracować i wdrożyć System Zarządzania Bezpieczeństwem Informacji uwzględniając wszelkie informacje przetwarzane w urzędzie gminy (nie tylko dane osobowe) tak aby posiadał atrybuty autentyczności, rozliczalności, niezaprzeczalności i niezawodności • Przeprowadzać okresową analizę ryzyka i utraty integralności, dostępności lub poufności informacji. Sprawdzić czy podejmowane działania minimalizują ryzyko • Opracować i utrzymywać dane inwentarzowe sprzętu komputerowego i oprogramowania służącego do przetwarzania informacji , inwentarz ma zawierać informacje o rodzaju sprzętu i jego konfiguracji, licencjach oprogramowania. • Zaplanować i przeprowadzić szkolenia pracowników zaangażowanych w proces przetwarzania informacji w roku 2018. Szkolenia mają obejmować zagadnienia patrz § 20 ust.2 pkt. 6 rozporządzenia KRI. • Opracować i wdrożyć procedury zgłaszania incydentów naruszenia BI, przeszkolić w tym zakresie pracowników zaangażowanych w proces przetwarzania informacji • Zaplanować i przeprowadzić audyt z zakresu bezpieczeństwa informacji w roku 2018 • Opracować i wdrożyć procedury wykonywania kopii bezpieczeństwa, zapewniający odpowiedni poziom bezpieczeństwa. Opracować procedury dotyczące właściwego przechowywania kopii bezpieczeństwa, testowania. • Opracować i wdrożyć procedury zakładania i likwidacji kont w systemach informatycznych. Procedury mają posiadać atrybuty rozliczalności, niezawodności i niezaprzeczalności. • Dokonać aktualizacji strony internetowej

	wersji dla osób słabowidzących, uwzględnić rozwiązania techniczne umożliwiające swobodne poruszanie się po stronie za pomocą klawiatury. Opracować bardziej intuicyjny sposób przejścia ze strony głównej urzędu gminy na stronę w wersji dla osób słabowidzących. Przetestować strony UG pod kątem zgodności HTML i CSS. Usunąć błędy w publikowaniu grafiki na stronie urzędu gminy w wersji dla osób słabowidzących które uniemożliwiają swobodne korzystanie ze strony.
--	---

Jednocześnie proszę poinformować Wojewodę Świętokrzyskiego, w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag oraz zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań. Ponadto informuję, iż zgodnie z art.48 ustawy z dnia 15 lipca 2011 roku o Kontroli w administracji rządowej (Dz.U.2011.185.1092) od niniejszego wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z up. Wojewody Świętokrzyskiego

Podpis
Marcin Bęben
Dyrektor
Wydział Organizacji i Kadr