

OSO.130.1.2016

Wojewoda Świętokrzyski
Wydział Organizacji i Kadr
Pani Edyta Suchoń
Dyrektor Wydziału

W odpowiedzi na pismo znak OK.V.431.1.2015 z dnia 12.17.2015 w sprawie wystąpienia pokontrolnego z kontroli przeprowadzonej w dniach 2 – 6 listopada 2015 roku, dotyczącej działania systemów teleinformatycznych, używanych do realizacji zadań publicznych zgodnie z rozporządzeniem Rady ministrów z dnia 12 kwietnia 2012 r. informuję, iż przedstawione oceny i uwagi zostały przyjęte do wiadomości i stosowania w praktyce, mianowicie:

Ad. 1), Ad. 2) Odnośnie dokonywania bieżących przeglądów i aktualizacji przepisów wewnętrznych regulujących zasady Systemu Zarządzania Bezpieczeństwem Informacji oraz corocznego szacowania i analiz ryzyka systemów teleinformatycznych, został powołany zespół ds. Zarządzania Bezpieczeństwem Informacji, realizujący powyższe kwestie. Zarządzenie Wójta Gminy w załączniku.

Ad. 3) W wyniku przeprowadzonej procedury wynikającej z Prawa Zamówień Publicznych, aktualnie dokonywana jest analiza umowy z zewnętrzną firmą Centrum Bezpieczeństwa Informatycznego, która przedstawiła najkorzystniejszą ofertę dotyczącą przeprowadzenia audytu bezpieczeństwa informatycznego w urzędzie. Audyt zostanie przeprowadzony po podpisaniu umowy, tj. w pierwszym półroczu bieżącego roku.

Ad. 4) Zespół powołany zarządzeniem Wójta Gminy (o którym mowa w pkt. 1 i 2 niniejszego pisma) został zobowiązany do bieżącej aktualizacji dokumentacji związanej z przetwarzaniem informacji a także opracowywanie i wdrażanie wewnętrznych przepisów w praktyce, w przypadkach zmian ustawowych lub potrzeb własnych.

Ad. 5) Zalecenia w tym zakresie zostały już zrealizowane. Wdrożono i dostosowano do obecnych przepisów serwer pracujący pod kontrolą systemu Debian który przechowuje dzienniki systemowe przez okres 2 lat a kopie tych dzienników są składowane na zewnętrznych nośnikach i przechowywane w szafie pancernej.

Ponadto informuję, że z treścią wystąpienia pokontrolnego zostali zapoznani pracownicy Urzędu stosownie do zakresu swoich obowiązków, pod kontem realizacji uwag i zaleceń w nim zawartych.

UPP - Urzędowe Poświadczenie Przedłożenia

Identyfikator Poświadczenia: ePUAP-UPP6410415

Adresat dokumentu, którego dotyczy poświadczenie

Nazwa adresata dokumentu: ŚWIĘTOKRZYSKI URZĄD WOJEWÓDZKI W KIELCACH

Identyfikator adresata: SUWKielce

Rodzaj identyfikatora adresata: ePUAP-ID

Nadawca dokumentu, którego dotyczy poświadczenie

Nazwa nadawcy: GMINA MIEDZIANA GÓRA

Identyfikator nadawcy: g06gk04iln

Rodzaj identyfikatora nadawcy: ePUAP-ID

Dane poświadczenia

Data doręczenia: 2016-01-14T08:30:02.288

Data wytworzenia poświadczenia: 2016-01-14T08:30:02.288

Identyfikator dokumentu, którego dotyczy poświadczenie: DOK7792526

Dane uzupełniające (opcjonalne)

Rodzaj informacji uzupełniającej: Źródło

Wartość informacji uzupełniającej: Poświadczenie wystawione przez platformę ePUAP

Rodzaj informacji uzupełniającej: Identyfikator ePUAP dokumentu

Wartość informacji uzupełniającej: 7792526

Rodzaj informacji uzupełniającej: Informacja

Wartość informacji uzupełniającej: Zgodnie z art 39¹ par. 1 k.p.a. pisma powiązane z przedłożonym dokumentem będą przesyłane za pomocą środków komunikacji elektronicznej.

Rodzaj informacji uzupełniającej: Pouczenie

Wartość informacji uzupełniającej: Zgodnie z art 39¹ par. 1d k.p.a. istnieje możliwość rezygnacji z doręczania pism za pomocą środków komunikacji elektronicznej.

Dane dotyczące podpisu

Poświadczenie zostało podpisane - aby je zweryfikować należy użyć oprogramowania do weryfikacji podpisu

Lista podpisanych elementów (referencji):

referencja ID-9fc54231-ba90-11e5-94e1-001a645ae9b2 :

referencja ID-9fc56940-ba90-11e5-94e1-001a645ae9b2 : Pismo%20og

%C3%B3lne%20do%20podmiotu%20publicznego%20-%20Pismo%20og

%C3%B3lne%20do%20podmiotu%20publicznego.xml

referencja ID-9fce9103-ba90-11e5-94e1-001a645ae9b2 : #ID-9fce9101-ba90-11e5-94e1-001a645ae9b2

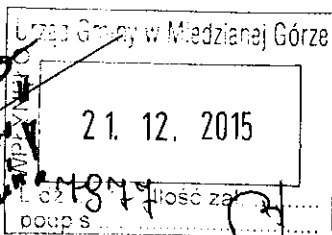
Świętokrzyski Urząd Wojewódzki

Kielce, 2015-12-17

25-516 Kielce

Aleja IX Wieków Kielc 3 / _

OK.V.431.1.2015



19.01.16

INFORMACJA

WYSTĄPIENIE POKONTROLNE

W załączeniu przesyłam wystąpienie pokontrolne z kontroli przeprowadzonej w dniach od 2 do 6 listopada 2015 roku.

Załączniki:

1. Wystąpienie pokontrolne Miedziana Góra.(1163046_932180).pdf
2. Wystąpienie pokontrolne Miedziana Góra.(1163046_932180).pdf.xades

Dokument został podpisany, aby go zweryfikować należy użyć
oprogramowania do weryfikacji podpisu

Data złożenia podpisu: 2015-12-17T12:33:43.969Z

Podpis elektroniczny



WOJEWODA ŚWIĘTOKRZYSKI

Kielce, dnia 17-12-2015

Znak: OK.V.431.1.2015

**Pan
Zdzisław Wrzałka
Wójt Gminy
Miedziana Góra**

WYSTĄPIENIE POKONTROLNE

Zakres kontroli:

Przedmiotem kontroli jest działanie systemów teleinformatycznych używanych do realizacji zadań publicznych 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.).

**Okres objęty
kontrolą:**

Od 01.01.2014 r. do dnia kontroli.

Zespół kontrolerów:

- Marek Rak, Informatyk Wojewódzki – Kierownik Oddziału ds. Informatyki w Wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego - Przewodniczący Zespołu Kontrolnego – upoważnienie do kontroli nr 933/2015 z dnia 30 października 2015r.
- Maciej Terek Główny Specjalista Oddziału ds. Informatyki w Wydziale Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego - Członek Zespołu Kontrolnego – upoważnienie do kontroli nr 934/2015 z dnia 30 października 2015r.
- Monika Wic, Zastępca Dyrektora Wydziału Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego - Członek Zespołu Kontrolnego – upoważnienie do kontroli nr 932/205 z dnia 30 października 2015r.

**Termin
przeprowadzenia
kontroli:**

Od 2 do 6 listopada 2015 r.

**Kierownik jednostki
kontrolowanej:**

Kierownikiem Jednostki kontrolowanej jest Pan Zdzisław Wrzałka wybrany w wyborach bezpośrednich w dn. 30 listopada 2014r. W okresie od 1.01. 2014. do 30.11.2014. kierownikiem Jednostki kontrolowanej był Pan Maciej Lubecki wybrany w wyborach bezpośrednich w dniu 21 listopada 2010 r.

**Podstawa prawna
do przeprowadzenia
kontroli:**

Kontrolę przeprowadzono na podstawie art. 28 ust. 1 pkt. 2 ustawy *o Wojewodzie i administracji rządowej w województwie*¹ oraz art. 6 ust. 4 pkt. 2 ustawy *o Kontroli w administracji rządowej*².

Projekt wystąpienia pokontrolnego przekazano zgodnie z przepisami art. 38 ustawy *o Kontroli w administracji rządowej*.

**Ocena stanu
faktycznego
wynikająca z ustaleń
kontroli:**

Pozytywnie z nieprawidłowościami ocenia się działanie systemów teleinformatycznych wykorzystywanych w Urzędzie Gminy w Miedzianej Górze do realizacji zadań zleconych z zakresu administracji rządowej w latach 2014-2015.

Ocena ogólna ustalona została w oparciu kryteria zawarte w programie kontroli zatwierdzonym przez Dyrektora Wydziału Organizacji i Kadr Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach.

W toku przeprowadzonej kontroli ustalono, że:

**Projektowanie,
wdrażanie i
eksploatacja systemu
teleinformatycznego:**

Kontrolą objęto dwa systemy informatyczne wykorzystywane do realizacji zadań zleconych z zakresu administracji rządowej, tj. „KORELACJA” i „FORTES”, oraz sposób użytkowania informatycznych systemów centralnych, np. Źródło. Na okoliczność kontroli zostały przedstawione oświadczenia producentów obu systemów o zastosowaniu przy realizacji oprogramowania rozwiązań gwarantujących zapewnienie poufności, integralności i rozliczalności przetwarzania danych których mowa w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 Nr 100, późn. zm. 1024). w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

¹ Ustawa z dnia 23 stycznia 2009 r., o *Wojewodzie i administracji rządowej w województwie* (Dz. U. nr 31, poz. 206 z późn. zm.).

² Ustawa z dnia 15 lipca 2011 r. o *Kontroli w administracji rządowej* (Dz. U. Nr 185, poz. 1092).

³ Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (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.).

Ocena częściowa: Pozytywnie ocenia się działalność Jednostki w zakresie wdrożenia i eksploatacji systemu.

Zarządzanie usługami realizowanymi przez systemy teleinformatyczne

Urząd Gminy w Miedzianej Górze nie zarządza systemami informatycznymi w modelu usługowym, w związku z powyższym obszar ten nie został poddany ocenie kontrolerów.

Ocena częściowa: W związku z brakiem realizacji usługi, nie sformułowano w tym obszarze oceny częściowej

System zarządzania bezpieczeństwem informacji:

W Jednostce wdrożono w 2007 r. System Zarządzania Bezpieczeństwem Informacji, który nie podlegał okresowym przeglądom i do dnia kontroli nie został zaktualizowany. Działanie takie było niezgodne z § 20 pkt.1 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 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.).

W Jednostce nie zatrudniono audytora wewnętrznego, Urząd korzysta z usług audytora zewnętrznego. W okresie objętym kontrolą nie został przeprowadzony audyt wewnętrzny w zakresie bezpieczeństwa informacji co jest niezgodne z § 20 ust.2 pkt. 14 z wyżej wymienionego rozporządzenia³.

Wójt Gminy powołał, a następnie zgłosił do GIODO, Administratora Bezpieczeństwa Informacji w osobie Pana Michała Tokara – informatyka. Kontrolujący stwierdzili, jednak że Administrator Bezpieczeństwa Informacji w Urzędzie Gminy nie złożył oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa Informacji co jest niezgodne z § 20 ust.2 pkt. 4 wspomnianego wyżej rozporządzenia³.

Czynności kontrolne wykazały także, że Urząd Gminy nie posiada dokumentów świadczących o przeprowadzaniu okresowej samooceny funkcjonowania systemu Zarządzania Bezpieczeństwem Informacji jak i o przeprowadzeniu okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co zalecono w § 20 ust.1 i ust.3 w/w rozporządzenia³.

Także dokumentacja dotycząca osób zaangażowanych w proces przetwarzania informacji w Urzędzie Gminy nie odzwierciedlała

³ Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (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.)

rzeczywistych uprawnień posiadanych przez użytkowników. Przykładowo - Wójt Gminy – Pan Zdzisław Wrzałka posiadał uprawnienia do użytkowania aplikacji Źródło, co nie zostało ujęte w dokumencie – Wykaz osób którym nadano uprawnienia do pracy w systemie, a co jest niezgodne § 20 ust. 2 pkt.4. w/w rozporządzenia³

Kontrolujący ustalili, że Urząd Gminy zapewniał szkolenia zewnętrzne i wewnętrzne dla pracowników zaangażowanych w proces przetwarzania informacji w okresie poddanym kontroli.

Kontrolowana Jednostka prawidłowo zapewnia ochronę przetwarzanych informacji przed ich kradzieżą, awarią nieuprawnionym dostępem stosując następujące zabezpieczenia :

- monitoring wizyjny,
- alarm przeciw włamaniowy, przeciwpożarowy,
- zabezpieczenia wejść wybranych pomieszczeń kratą żelazną,
- stosowanie szaf pancernych do przechowywania dokumentów i nośników danych.
- systemy awaryjnego zasilania (UPS),
- Active Directory do kontroli dostępu do danych
- urządzenia UTM do zabezpieczenia sieci Urzędu Gminy
- regularne sporządzanie kopii zapasowych danych przechowywanych na serwerach.

Kontrolujący stwierdzili natomiast brak klimatyzacji w pomieszczeniu serwerowni, co w może skutkować przegrzaniem urządzeń w okresie letnim.

Niezależnie od powyższego Kontrolujący stwierdzili rozbieżności pomiędzy zapisami Polityki Bezpieczeństwa Informacji dotyczącymi zabezpieczenia systemów teleinformatycznych hasłami, w PBI długość haseł została określona na minimum 8 znaków i zmiana hasła pierwszego dnia roboczego następnego miesiąca, a rzeczywistymi ustawieniami w systemie operacyjnym serwera, bowiem długość haseł została zdefiniowana na 7 znaków i maksymalny okres ważności hasła 42 dni.

W Polityce Bezpieczeństwa Informacji Urzędu Gminy są określone zasady zapewniające minimalizację występowania ryzyka kradzieży.

Urząd Gminy w Miedzianej Górze nie wykorzystuje urządzeń mobilnych do wykonywania obowiązków służbowych poza siedzibą Urzędu. Zasady użytkowania w/w urządzeń zostały jednak uregulowane w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych, stanowiącą załącznik nr 6 do Zarządzenia Nr 28 /2007 w sprawie wprowadzenia w Urzędzie Gminy Miedziana Góra „Instrukcji przetwarzania danych osobowych”.

Kontrolowana jednostka zapewnia aktualizację oprogramowania na bieżąco z wyjątkiem oprogramowania serwerowego Windows 2003. W umowach serwisowych firm współpracujących z Urzędem Gminy

są zapisy zapewniające aktualizację oprogramowania. W Urzędzie Gminy są stosowane mechanizmy kryptograficzne w sposób adekwatny do zagrożeń i wymogów prawa. Bezpieczeństwo plików systemowych zostało również zapewnione zgodnie zapisami Polityki Bezpieczeństwa Informacji.

Ryzyko wynikające z wykorzystania opublikowanych podatności technicznych systemów jest minimalizowane z wyjątkiem oprogramowania serwerowego Windows 2003, które nie jest już wspierane przez producenta i nie ukazują się żadne aktualizacje systemu.

W Polityce Bezpieczeństwa Informacji Urzędu Gminy są opisane procedury postępowania na wypadek zaistnienia incydentu, brakuje natomiast dokumentu określającego listę osób upoważnionych przez ABI które mają prawo do podejmowania odpowiednich kroków w razie wystąpienia incydentu. Ze względu na brak zarejestrowanych incydentów kontrolerzy nie są w stanie ocenić funkcjonowania związanych z tym procedur.

Ocena częściowa:

Pozytywnie z nieprawidłowościami ocenia się działalność jednostki w zakresie systemu zarządzania bezpieczeństwem informacji.

Rozliczalność:

W kontrolowanej jednostce rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów za wyjątkiem systemu firmy Fortes, gdzie dostęp do logów systemowych był niemożliwy z uwagi na fakt iż informatyk zatrudniony w Urzędzie Gminy nie posiada uprawnień administratora do systemu. Powyższe uprawnienia posiada jedynie Przedsiębiorstwo Informatyczne Fortes, z którym kontrolowany podpisał umowę na działanie systemu.

W Urzędzie Gminy zatrudniony informatyk nie posiadał wiedzy na temat czasu przechowywania logów systemowych. Z obserwacji kontrolujących wynikało że czasookres przechowywania logów systemowych nie przekraczał kilku miesięcy. Powyższe naruszało § 21 ust. 4 rozporządzenia³.

W jednostce kontrolowanej kopie dzienników są systematycznie składowane na taśmach magnetycznych i przechowywane w oddzielnym pomieszczeniu w zabezpieczonej szafie pancerniej. Nie stwierdzono prowadzenia dzienników systemowych na nośniku papierowym.

Ocena częściowa:

Pozytywnie z nieprawidłowościami ocenia się działalność Jednostki w zakresie rozliczalności systemów teleinformatycznych.

Zalecenia:

W związku z powyższym uprzejmie proszę Pana Wójta o rozważenie możliwości podjęcia następujących działań w celu

niedopuszczenia do powstania podobnych nieprawidłowości w przyszłej działalności podległej Panu jednostki. W szczególności należy zadbać o:

- ✓ 1. Dokonywanie bieżących przeglądów i aktualizacji przepisów wewnętrznych regulujących zasady Systemu Zarządzania Bezpieczeństwem Informacji.
- ✓ 2. Coroczne szacowanie i analizę ryzyka posiadanych systemów teleinformatycznych zgodnie z przyjętą w jednostce metodą.
- ✓ 3. Zapewnienie raz do roku audytu w zakresie bezpieczeństwa informacji.
- ✓ 4. Bieżące aktualizowanie dokumentów i wykazów dotyczących przetwarzania informacji i posiadanych uprawnień, a także znajomości wewnętrznych przepisów dotyczących bezpieczeństwa informacji.
- ✓ 5. Zabezpieczenie przechowywania zapisów z dzienników systemowych tzw. logów z serwera pracującego pod kontrolą systemu Debian przez okres dwóch lat od dnia ich zapisu.
- ✓ 6. Składowanie ww. dzienników systemowych na zewnętrznych nośnikach informatycznych w warunkach zapewniających bezpieczeństwo informacji.

Jednocześnie proszę poinformować Wojewodę Świętokrzyskiego, w terminie 30 dni od daty otrzymania niniejszego wystąpienia pokontrolnego o sposobie wykorzystania wyżej wymienionych uwag i wniosków oraz o wykonaniu 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* od niniejszego wystąpienia pokontrolnego nie przysługują środki odwoławcze.

Z upoważnienia
Wojewody Świętokrzyskiego

Edyta Suchoń
Dyrektor Wydziału
Wydział Organizacji i Kadr