Znak:Fn.1431. 7 .2019

Łagów, dnia 26-07- 2019r.

Odpowiadając na Pani wniosek (email) z dnia 15 lipca 2019 roku o udostępnienie informacji publicznej informuję, że :
W odpowiedzi na maila odpowiadamy i przesyłamy:

1. Plan audytu na 2018 r. i 2019 r.
2. Program zadania
3. Sprawozdanie z zadania audytowego
4. W 2019 roku zadania są w trakcie realizacji

BURMISTRZ
Paweł Marwicki

Jednocześnie informuję, iż jeśli zamierza Pani wykorzystać uzyskaną informację w celu jej ponownego wykorzystania w rozumieniu art.2 ust.2 ustawy z dnia 25 lutego 2016r. o ponownym wykorzystaniu informacji sektora publicznego /tekst jednolity Dz. U. z 2018r. poz. 1243/ to jest „ art.2.2. Przez ponowne wykorzystywanie należy rozumieć wykorzystywanie przez osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej, zwane dalej "użytkownikami", informacji sektora publicznego, w celach komercyjnych lub niekomercyjnych innych niż pierwotny publiczny cel, dla którego informacja została wytworzona" - należy zwrócić się do Organu udostępniającego informację, celem ustalenia warunków jej ponownego wykorzystania.

Jawność danych dotycząca imienia i nazwiska, adresu e-mail i nr tel. została wyłączona na podstawie art. 1 i 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych /Dz. U. z 2016 r. poz. 922 z późniejszymi zmianami/. Wyłączenia jawności dokonał Paweł Marwicki – Burmistrz Miasta i Gminy Łagów.

Urząd Miasta i Gminy
26-025 Łagów, ul. Rynek 62
tel. 41 343 70 54, fax 41 343 70 5
woj. świętokrzyskie

(Pieczęć jednostki)

PLAN AUDYTU WEWNĘTRZNEGO NA 2018 ROK

I. Wstęp

1) Informacje o sposobie prowadzenia audytu wewnętrznego.

Audyt wewnętrzny prowadzony przez audytora usługodawcę niezatrudnionego w jednostce (art. 275 pkt 2 ustawy o finansach publicznych z dnia 27 sierpnia 2009 r. / Dz. U. z 2016 r., poz. 1870/).

2) Plan audytu został opracowany uwzględniając:

- cele i zadania Urzędu Miasta i Gminy w Łagowie;
- priorytety Burmistrza Miasta i Gminy w Łagowie;
- przepisy 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)
- analizę zasobów osobowych komórki audytu wewnętrznego.

Przygotowując Plan audytu wewnętrznego dla Urzędu Miasta i Gminy w Łagowie na 2018 r. odstąpiono od przeprowadzenia analizy ryzyka, gdyż planowane zadania wynikają z priorytetów Burmistrza oraz ww. 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.

Poniższa mapa przedstawia działania jakie będą podejmowane przez audytora usługodawcę w poszczególnych obszarach działalności jednostki i jednostkach organizacyjnych Urzędu Miasta.

Lp.	Nazwa obszaru działalności jednostki/ nazwę jednostki organizacyjnej	Rodzaj działań planowanych do podjęcia
1.	Środowisko Informatyczne	Zadanie zapewniające
2.	Gospodarka finansowa	Czynności doradcze
3.	Zarządzanie jednostką	Czynności doradcze

II. Planowane działania:

1) *Zadania zapewniające*

L.p.	Wstępnie proponowany zakres zadania	Nazwa obszaru działalności jednostki	Ryzyka, które wpłynęły na ocenę ryzyka w danym obszarze, z przypisaniem do kategorii	Powiązanie zadania zapewniającego z celami/zadaniami jednostki	Dodatkowe informacje
1.	Audyt bezpieczeństwa teleinformatycznego 2018 r.	Środowisko Informatyczne	Nie dotyczy	Zarządzanie i administrowanie systemami i sieciami informatycznymi oraz bazami danych.	Zadanie realizowane co roku.
2.	Priorytety Burmistrza Miasta i Gminy w Łagowie audyt zlecony.	Zarządzanie jednostką	Nie dotyczy	UG oraz jednostki organizacyjne wg. potrzeb bieżących.	

2) *Czynności doradcze*

L.p.	Obszar działalności jednostki		
1.	Zarządzanie jednostką	Konsultacje w zakresie kontroli zarządczej	U M i G oraz jednostki organizacyjne wg. potrzeb bieżących.
2.	Zarządzanie jednostką	Priorytety Burmistrza Miasta i Gminy w Łagowie audyt zlecony.	U M i G oraz jednostki organizacyjne wg. potrzeb bieżących.

3) *Monitorowanie realizacji zaleceń oraz przeprowadzanie czynności sprawdzających*

L.p.	Temat zadania zapewniającego	Nazwa obszaru działalności jednostki	Ocena ryzyka	Dodatkowe informacje	Rok zakończenia zadania zapewniającego
Monitorowanie realizacji zaleceń					
1.	Ocena systemu zarządzania bezpieczeństwem informacji na przykładzie wybranych zagadnień realizowanych w Urzędzie Miasta i Gminy w Łagowie	Środowisko Informatyczne	wysokie	-	2018 r.

Czynności sprawdzające					
1.	-	-	-	-	-

4) **Inne zadania realizowane przez audytora usługodawcę:**

- przygotowanie planu audytu na 2018 r. oraz sprawozdawczość roczna za 2018 r.;
- samoocena audytu wewnętrznego za 2018 r.

mgr Grzegorz Palacz

06.03.2019 — Audytor Wewnętrzny

data — *(Podpis i pieczęć audytora usługodawcy)*

BURMISTRZ

Paweł Marwicki

06.03.2019

data — *(Podpis i pieczęć Burmistrza)*

(Pieczęć jednostki)

Urząd Miasta i Gminy
26-025 Łagów, ul. Rynek 62
tel. 41 343 70 54, fax 41 343 70 51
woj. świętokrzyskie

PLAN AUDYTU WEWNĘTRZNEGO NA 2019 ROK

I. Wstęp

1) Informacje o sposobie prowadzenia audytu wewnętrznego.

Audyt wewnętrzny prowadzony przez audytora usługodawcę niezatrudnionego w jednostce (art. 275 pkt 2 ustawy o finansach publicznych z dnia 27 sierpnia 2009 r. / Dz. U. z 2016 r., poz. 1870/).

2) Plan audytu został opracowany uwzględniając:

- cele i zadania Urzędu Miasta i Gminy Łagów;
- priorytety Burmistrza i Gminy Łagów;
- przepisy 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)
- analizę zasobów osobowych komórki audytu wewnętrznego.

Przygotowując Plan audytu wewnętrznego dla Urzędu Miasta i Gminy Łagów na 2019 r. odstąpiono od przeprowadzenia analizy ryzyka, gdyż planowane zadania wynikają z priorytetów Burmistrza Miasta i Gminy oraz ww. 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.

Poniższa mapa przedstawia działania jakie będą podejmowane przez audytora usługodawcę w poszczególnych obszarach działalności jednostki i jednostkach organizacyjnych Gminy.

Lp.	Nazwa obszaru działalności jednostki/ nazwę jednostki organizacyjnej	Rodzaj działań planowanych do podjęcia
1.	Środowisko Informatyczne	Zadanie zapewniające
2.	Gospodarka finansowa	Czynności doradcze
3.	Zarządzanie jednostką	Czynności doradcze

II. Planowane działania:

1) Zadania zapewniające

L.p.	Wstępnie proponowany zakres zadania	Nazwa obszaru działalności jednostki	Ryzyka, które wpłynęły na ocenę ryzyka w danym obszarze, z przypisaniem do kategorii	Powiązanie zadania zapewniającego z celami/zadaniami jednostki	Dodatkow informacj
1.	Audyt bezpieczeństwa teleinformatycznego 201Ȝ r.	Środowisko Informatyczne	Nie dotyczy	Zarządzanie i administrowanie systemami i sieciami informatycznymi oraz bazami danych.	Zadanie realizowar co roku.

2) Czynności doradcze

L.p.	Obszar działalności jednostki		
1.	Zarządzanie jednostką	Konsultacje w zakresie kontroli zarządczej	UMiG oraz jednostki organizacyjne wg. potrzeb bieżących.
2.	Audyt zlecony przez Wójta		

3) *Monitorowanie realizacji zaleceń oraz przeprowadzanie czynności sprawdzających*

L.p.	Temat zadania zapewniającego	Nazwa obszaru działalności jednostki	Ocena ryzyka	Dodatkowe informacje	Rok zakończenia zadania zapewniającego
Monitorowanie realizacji zaleceń					
1.					
2.					
Czynności sprawdzające					
1.	-	-	-	-	-

4) **Inne zadania realizowane przez audytora usługodawcę:**

- przygotowanie planu audytu na 2020 r. oraz sprawozdawczość roczna za 2019 r.;

12.12.2019 ..... Inspektor Grzegorz Palacz Audytor Wewnętrzny

data *(Podpis i pieczęć audytora usługodawcy)*

12.12.2019 r. ..... BURMISTRZ Paweł Marwicki

data *(Podpis i pieczęć Burmistrza)*

Urząd Miasta i Gminy

Ul. Rynek 62

26 – 026 Łagów

PROGRAM ZADANIA AUDYTOWEGO

Temat zadania	Zarządzanie bezpieczeństwem informacji w Urzędzie Miasta i Gminy Łagów.	
Komórka audytowana	Urząd Gminy i Miasta Łagów	
Okres objęty audytem	II półrocze 2018 r.	
Oznaczenie zadania:	Nr: 1/2018 Rodzaj: zadanie planowe – wynikające z Planu audytu wewnętrznego na 2018 r.	
1.	**Typ działalności:**	wspomagająca
	Obszar działania:	1. Środowisko informatyczne. 2. Zarządzanie urzędem
	Obszar ryzyka:	1. Zarządzanie i administrowanie systemami i sieciami informatycznymi oraz bazami danych, 2. Bezpieczeństwo pracowników, informacji i dokumentów.
2.	**Cel zadania**	1. Zebranie informacji na temat zapewnienia opracowania i wprowadzenia w życie procedur bezpieczeństwa informacji w Urzędzie Miasta i Gminy Łagów..

		2. Wykazanie ewentualnego braku uregulowań bezpieczeństwa informacji w opracowanych procedurach.
3.	**Podmiotowy zakres zadania**	**Koordynator Bezpieczeństwa Informacji (ABI ASI).**
4.	**Przedmiotowy zakres zadania**	W ramach audytu zostaną zebrane informacje dotyczące: 1) polityki bezpieczeństwa informacji, **WYŁĄCZENIA Z ZADANIA**: Audytem nie objęto obszaru informacji niejawnych.
5.	**Istotne ryzyka w obszarze ryzyka objętym zadaniem:**	Zidentyfikowane zostały następujące istotne ryzyka (zagrożenia, problemy) w obszarze ryzyka objętym zadaniem audytowym: 1. Brak procedur bezpieczeństwa informacji. 2. Brak procedur ochrony danych osobowych. 3. Opracowane procedury są niezgodne z przepisami prawa. 4. Nie wdrożono w życie opracowanej Polityki Bezpieczeństwa Informacji. 5. Nie przekazano opracowanej dokumentacji bezpieczeństwa informacji do zapoznania się pracownikom i potwierdzenia obowiązku jej przestrzegania. 6. Nie przypisano ról i nie przekazano zakresów odpowiedzialności za bezpieczeństwo informacji. 7. Polityka bezpieczeństwa informacji nie zawiera zasad zarządzania informacją. 8. Nie przeprowadzono szkoleń (zewnętrznych i wewnętrznych) osób zaangażowanych w proces przetwarzania informacji.
6.	**Techniki audytu:**	**Przeprowadzając zadanie audytowe wykorzystane zostaną następujące techniki:** Niniejszy audyt wewnętrzny prowadzony jest w formie zadania zapewniającego. W ramach gromadzenia informacji niezbędnych do wypełnienia ankiety można stosować następujące techniki: 1. Lista sprawdzająca. 2. Rozmowy/wywiady. 3. Analiza dokumentacji.
7.	**Akty prawne i inne dokumenty stanowiące odniesienie w trakcie audytu**	1. ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, 2. rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla systemów teleinformatycznyc .(Dz. U. poz. 526 z dnia 12 kwietnia 2012 r.),

Kryteria oceny ustaleń stanu faktycznego oraz najważniejsze wymagania odnośnie obiektów audytu

Obiekt audytu	Kryterium	Najważniejsze wymagania	Waga %	spełnia (T)/ spełnia w ograniczonym zakresie (SO)/ nie spełnia (N)
dokumentacja zarządzania bezpieczeństwem informacji	Zgodność z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi oraz adekwatność przyjętych rozwiązań (przyjęte rozwiązania są dostosowane do jednostki)	**Zapewnienie ustanowienia systemu zarządzania bezpieczeństwa informacji**	15	-
		Zapewnienie, że procedury wewnętrzne tworzone są w oparciu o obowiązujące przepisy prawa w zakresie bezpieczeństwa informacji	10	
		Zapewnienie, że opracowana dokumentacja bezpieczeństwa informacji przekazana została do zapoznania się pracownikom	10	-
		Zapewnienie, że osoby zaangażowane w proces przetwarzania informacji objęte zostały szkoleniem.	4	-
		Zapewnienie, że polityka bezpieczeństwa informacji zawiera:	16	
		• *definicję, zakres oraz znaczenie bezpieczeństwa informacji,*	*2*	
		• *zakres i cele polityki bezpieczeństwa informacji,*	*2*	
		• *zasady ochrony informacji,*	*2*	
		• *uregulowania odpowiedzialności pracowników Urzędu za bezpieczeństwo Informacji,*	*2*	
		• *określenie klasyfikacji informacji i sposób ich ochrony,*	*2*	
		• *określenie organizacji bezpieczeństwa informacji w zakresie współpracy z podmiotami zewnętrznymi,*	*2*	

		• *deklarację stosowania zabezpieczeń,*	2	
		• *zasady zarządzania ryzykiem,*	2	
		Zapewnienie, że dokumentacja zarządzania systemem informatycznym reguluje zasady przetwarzania danych osobowych w zakresie:	16	
		• *nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,*	2	
		• *stosowania metod i środków uwierzytelnienia,*	2	
		• *rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu,*	2	
		• *tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,*	2	
		• *sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do przetwarzania danych osobowych,*	2	
		• *sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,*	2	
		• *wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych,*	2	
		• *odebrania uprawnień do przetwarzania danych osobowych,*	2	
		Zapewnienie, że instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji zawiera:	9	
		• *zasady reagowanie na incydent,*	3	
		• *zasady raportowania z incydentu i ewidencjonowanie incydentów,*	3	

		• *zasady analizy incydentu.*	*3*	
		Zapewnienie, że kierownictwo wspiera działania w zakresie bezpieczeństwa informacji w całej organizacji	**10**	
		Zapewnienie, że przypisano role i zakresy odpowiedzialności za bezpieczeństwo informacji	**10**	-
Razem			**100%**	-

Pozytywna ocena nt. zgodności oraz adekwatności opracowanych procedur systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy Łagów może zostać sformułowana w przypadku, gdy poziom spełniania najważniejszych wymagań **jest na poziomie 80%.**

Pozytywna ocena z zastrzeżeniami nt. zgodności oraz adekwatności opracowanych procedur systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy Łagów może zostać sformułowana w przypadku, gdy poziom spełniania najważniejszych wymagań **jest na poziomie 70%.**

Negatywna ocena nt. zgodności oraz adekwatności opracowanych procedur systemu zarządzania bezpieczeństwem informacji w Urzędzie Miasta i Gminy Łagów może zostać sformułowana w przypadku, gdy poziom spełniania najważniejszych wymagań **jest niższy niż 60%.**

Sposób klasyfikowania wyników dla poszczególnych kryteriów.

Sposób klasyfikowania wyników dla obu przyjętych kryteriów	**Istotne**	**Średnie**	**Mało istotne**
Obiekt/przykłady ustaleń dla danego poziomu wyników	Ustalenia, które w istotny sposób wpływają na prawidłową organizację systemu zarządzania bezpieczeństwem informacji w jednostce oraz prawidłowe funkcjonowanie wybranych narzędzi systemu zarządzania bezpieczeństwem informacji **powodując**, że nie są one realnymi narzędziami zarządzania. Powinny zostać niezwłocznie usunięte.	Ustalenia, które wpływają na prawidłową organizację systemu zarządzania bezpieczeństwem informacji oraz prawidłowe funkcjonowanie w jednostce wybranych narzędzi systemu zarządzania bezpieczeństwem informacji ale **nie powodując,** że nie są one realnymi narzędziami zarządzania w jednostce.	Ustalenia, które nie wpływają na organizację systemu zarządzania bezpieczeństwem informacji oraz prawidłowe funkcjonowanie wybranych narzędzi systemu zarządzania bezpieczeństwem informacji a dotyczą spełnienia wybranych wymogów formalnych.

dokumentacja systemu zarządzania bezpieczeństwem informacji **w jednostce**	• brak określenia formalnych zasad organizacji i funkcjonowania systemu zarządzania bezpieczeństwem informacji j w jednostce • niejednoznacznie określone zasady systemu zarządzania bezpieczeństwem informacji • brak spójności dokumentacji systemu zarządzania bezpieczeństwem informacji w jednostce	• brak dostępności dokumentacji dla wszystkich osób, dla których jest niezbędna • brak wsparcia przez kierownictwo działań w zakresie bezpieczeństwa informacji w Urzędzie, • nie przeprowadzenie (brak) szkolenia dla osób zaangażowanych w proces przetwarzania informacji	Ustalenia, które nie wpływają na poprawność opracowanej dokumentacji lub wpływają w niewielkim stopniu.

10.	**Założenia organizacyjne**		1. Zadanie audytowe zostanie przeprowadzone zgodnie z metodologią określoną w rozporządzeniu Ministra Finansów dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego (D.U. Nr 21 poz. 108) oraz z procedurami audytu wewnętrznego obowiązującymi w Urzędzie Miasta i Gminy Łagów. 2. Zadanie zostanie przeprowadzone przez audytora Urzędu Gminy Sobków w Kielcach Pobrana dokumentacja zostanie odpowiednio zabezpieczona. 3. Audyt prowadzony będzie w sposób nie zakłócający pracy audytowanych. 4. Audyt rozpoczęty zostanie w styczniu 2018 r. 5. Przewidywane zakończenie audytu IV kwartał 2018 r.	
11.	**Sporządził:**	*Grzegorz Palacz audytor wewnętrzny*	**Data sporządzenia:**	03.09.2018 r.

mgr Grzegorz Palacz
Audytor Wewnętrzny
[redacted]
(podpis audytora wewnętrznego)

Łagów 10 września 2018 roku.

Urząd Miasta i Gminy Łagów
ul. Rynek 62
Łagów 26-025
Audytor wewnętrzny

SPRAWOZDANIE Z PRZEPROWADZENIA AUDYTU WEWNĘTRZNEGO – ZADANIA ZAPEWNIAJĄCEGO

1.	**Oznaczenie audytu:**	Numer: **AW 1/.2018** Rodzaj: ZADANIE ZAPEWNIAJACE WYNIKAJĄCE Z PLANU AUDYTU NA 2018 r.
2.	**Temat audytu:**	Zarządzanie bezpieczeństwem informacji w Urzędzie Miasta i Gminy Łagów.
3.	**Otrzymują:**	1 Burmistrz Miasta i Gminy Łagów Kierownik Urzędu (do wiadomości); 2. Administrator Systemu Informatycznego; 3. Administrator Bezpieczeństwa Informacji; 2. a/a.
4.	**Upoważnienie do przeprowadzenia audytu wewnętrznego**	Nr 1/2018 z dnia 10 września 2018 r.
5.	**Cel audytu:**	1. Zebranie informacji w zakresie bezpieczeństwa informacji. 2.Weryfikacja wymagań w zakresie zarządzania bezpieczeństwem informacji wynikających z § 20 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 (dalej: rozporządzenie / Dz. U. z 2012 r. poz. 526).
6.	**Obszar audytu:**	1.Środowisko informatyczne: Zarządzanie i administrowanie systemami i sieciami informatycznymi oraz bazami danych; 2. Zarządzanie Urzędem: Bezpieczeństwo pracowników, informacji i dokumentów.

7.	**Zakres przedmiotowy:**	W ramach audytu zostaną zebrane informacje dotyczące: 1) polityki bezpieczeństwa informacji, 2) zarządzania odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.
8.	**Zakres podmiotowy:**	**Administrator Bezpieczeństwa Informacji (ABI).** **Administrator Systemów Informatycznych (ASI).**
9.	**Imię i nazwisko audytora wewnętrznego/usługodawcy:**	Grzegorz Palacz
10.	**Termin przeprowadzenia zadania zapewniającego:**	III – IV kwartał 2018 r.

1. Założenia audytu

Określenia istotnych ryzyk dokonano uwzględniając wymogi stawiane przez przepisy prawa oraz zadania realizowane przez audytora wewnętrznego .

W badanych obszarach istnieje prawdopodobieństwo wystąpienia następujących istotnych ryzyk:

1) Niewłaściwe uregulowania lub brak uregulowań w badanym procesie.
2) Działania niezgodne z wymogami prawa oraz regulacjami wewnętrznymi.
3) Brak zapewnienia środków ochrony fizycznej dla zabezpieczenia informacji prawnie chronionej.
4} Niewłaściwy obieg i przechowywanie dokumentów stanowiących informację prawnie chronioną.
5) Ujawnienie danych osobowych przez pracownika.
6) Przetwarzanie danych osobowych przez pracowników bez stosownych upoważnień i uprawnień dostępu.
7) Naruszenie zasad ochrony fizycznej danych osobowych.
8) Utrata danych lub ich poprawności.
9) Niewykrycie wszystkich przypadków niewykonywania kopii bezpieczeństwa.
10) Używanie nielegalnego oprogramowania.
11) Niska jakość przeprowadzanych szkoleń informatycznych.
12) Awarie sprzętu.

Na ryzyka występujące w badanym obszarze, mogą wpływać następujące czynniki:

1) przepływ informacji oraz współpraca wewnątrz komórki audytowanej,
2) sprawowanie nadzoru w zakresie badanej działalności,
3) zła organizacja pracy.

Narzędzia i techniki przeprowadzania zadania:

1) analiza dokumentacji źródłowej oraz regulacji wewnętrznych w zakresie badanej działalności
2) uzyskiwanie wyjaśnień i informacji od pracowników w zakresie objętym zadaniem,
3) porównanie danych i sprawdzenie rzetelności informacji,
4) badanie istniejących mechanizmów kontrolnych,
5) testy/listy kontrolne.

Dowody wykorzystane do dokonania ustaleń:

1) uregulowania zewnętrzne oraz wewnętrzne dotyczące badanej działalności,

2) dokumentacja źródłowa,
3) wyjaśnienia uzyskane od audytowanych.

2. Najważniejsze ustalenia audytu

W Urzędzie obowiązują sformalizowane zasady bezpieczeństwa informacji. Informatyk Urzędu zgodnie z obszarem działania określonym w zakresach czynności odpowiadają za ochronę systemów i sieci informatycznych.

Audytem nie objęto obszaru informacji niejawnych.
Realizując cel audytu dokonano przeglądu regulacji wewnętrznych obowiązujących w Urzędzie w badanym obszarze pod kątem ich aktualności, kompletności, spełnienia podstawowych wymogów określonych w§ 20 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 (dalej: Rozporządzenie / Dz. U. z 2012 r. poz. 526).

Lista kontrolna

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
1.	Czy zostały opracowane i ustanowione zasady bezpieczeństwa informacji?	X		Polityka bezpieczeństwa przygotowywana, w trakcie wdrażania.
2.	Czy wdrożone zostały do eksploatacji zasady bezpieczeństwa informacji?	X		Zarządzenie Nr 96/18 Burmistrza Miasta i Gminy Łagów z dnia 20 września 2018r. w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta i Gminy Łagów
3.	Czy zapewniony został monitoring i przegląd zasad bezpieczeństwa informacji?	X		Aktualizacja poszczególnych aktów prawa wewnętrznego wynika z zaistniałych potrzeb. Monitoring i przegląd zasad bezpieczeństwa odbywa się na bieżąco obowiązują w Urzędzie mechanizmy kontrolne.
4.	Czy utrzymywany i doskonalony system zarządzania bezpieczeństwem informacji zapewnienia poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność?	X		W urzędzie znajduje się zamykana serwerownia w której zgromadzono serwery na których znajdują się bazy danych, urządzenia odpowiedzialne za wykonywanie i przechowywanie kopii zapasowych oraz monitoring. Dostęp do serwerowni i zgromadzonych tam urządzeń ma wyłącznie osoba odpowiedzialna za obsługę i serwisowanie. Dostęp do urządzeń i zgromadzonych baz możliwy jest wyłącznie po podaniu loginu oraz hasła(osobne loginy i hasła do urządzeń , dodatkowe loginy i hasła do baz danych).

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
§ 20 ust. 2 cyt. rozporządzenia – zarządzanie bezpieczeństwem informacji realizowane w szczególności przez zapewnienie warunków umożliwiających realizację i egzekwowanie następujących działań:				
1.	Czy została zapewniona aktualizacja regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia?	X		Aktualizacja poszczególnych aktów prawa wewnętrznego, o których mowa powyżej wynika z zaistniałych potrzeb i przepisów prawa
2.	Czy zapewnione jest utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację?	X		Aktualizowanie posiadanego sprzętu oraz oprogramowania prowadzone jest na bieżąco, gdy tylko zajdzie potrzeba wymiany sprzętu lub oprogramowania
3.	Czy są przeprowadzane okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowane są działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy?	X		Tak
4.	Czy podejmowane są działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji?	X		Tak
	a) Czy zostały ustanowione zasady kontroli dostępu?	X		Z powyższych uregulowań wewnętrznych wynika, że: 1) w zakresie kont użytkowników Konto jest zakładane na wniosek przełożonego pracownika. W tym celu przełożony zgłasza u Administratora Systemu Informatycznego zapotrzebowanie stworzenia konta i rodzaj dostępu do sieci. ASI nadaje login i zakłada użytkownikowi konto, nadając uprawnienia, przydzielając początkowe hasło z opcją wymuszenia jego zmiany przez użytkownika przy pierwszym logowaniu. Cechy logów użytkownika:

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
				– musi być niepowtarzalny, – jednym loginem może posługiwać się tylko jedna osoba, – login jest natychmiast blokowany po rozwiązaniu z pracownikiem umowy o pracę (wygaśnięciem stosunku pracy), – login pracownika, który rozwiązał umowę o pracę nie może zostać przydzielony innemu pracownikowi. **Zasady korzystania z haseł:** – hasło jest ciągiem co najmniej 8 znaków, musi zawierać zarówno litery małe, duże jak i cytry lub inne znaki. – hasło musi być zmieniane przynajmniej jeden raz w ciągu 30 dni, – hasło jest niejawne – użytkownik nie ma prawa go ujawnić innym użytkownikom, – hasło nie może być powtórzeniem ostatnich 10 haseł, – na użytkowniku jest wymuszana zmiana hasła, – przy wpisywaniu hasła nie jest ono wyświetlane na ekranie, – w przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione. 2) w zakresie przetwarzania danych osobowych: – każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z uregulowaniami zewnętrznymi i wewnętrznymi w zakresie danych osobowych oraz posiadać upoważnienie do przetwarzania danych osobowych – ASI przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie wniosku określającego zakres uprawnień pracownika, z wyłączeniem osób kierujących Urzędem, – przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji; hasło ustanowione podczas przyznawania uprawnień przez ASI należy zmienić na indywidualne podczas pierwszego logowania się w systemie, – w systemie informatycznym stosuje się uwierzytelnianie trójstopniowe: – Wysoki poziom wrażliwości charakteryzowany dla kont użytkownika o administracyjnych uprawnieniach co najmniej w jednym systemie komputerowym Urzędu. – Średni poziom wrażliwości odnosi się do kont użytkownika, które posiadają wyższe niż przeciętne uprawnienia w co najmniej jednym systemie informatycznym Urzędu, w szczególności dla kont z uprawnieniami redakcyjnymi serwisy internetowe.

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
				– Niski poziomi wrażliwości odnosi się do kont użytkownika, które nie posiadają żadnych szczególnych uprawnień w żadnym systemie informatycznym. – bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła, – hasło użytkownika powinno być zmieniane co najmniej raz na miesiąc, – identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie, – pracownicy są odpowiedziami za zachowanie poufności swoich haseł, hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, – hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie, w sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła, – przy wyborze hasła obowiązują następujące zasady: a) <u>minimalna długość hasła – 8 znaków,</u> b) należy unikać haseł, które użytkownik stosował uprzednio w okresie 10 miesięcy, swojej nazwy użytkownika w jakiejkolwiek formie, przewidywalnych sekwencji znaków z klawiatury np.: "ANNA11", "12345678", itp. c) należy stosować hasła zwierające kombinacje liter i cyfr; hasła, które można zapamiętać bez zapisywania, łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim, – zmiany hasła nie wolno zlecać innym osobom, – w systemach, które umożliwiają opcje zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia, – hasło użytkownika o prawach administratora powinno znajdować się w zapieczętowanej kopercie w zamykanej na klucz szafie metalowej. 3) W zakresie przetwarzania danych księgowych procedura nadawania i zmiany uprawnień, posługiwania się hasłami jest zbieżna z procedurą określoną dla danych osobowych.
	b) Kto ustanowił zasady kontroli dostępu?	X		Burmistrz Miasta i Gminy Łagów – Paweł Marwicki.
	c) Czy zostały ustanowione zasady rejestracji uprawnień użytkowników?	X		TAk

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
	d) Czy dokonuje się okresowych przeglądów uprawnień użytkowników i kto je przeprowadza?	X		ABI, ASI – przeglądy w zależności od potrzeb (nie są to dokumentowane działania).
5.	Czy dokonuje się bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji?	X		Stosownie do uregulowań: – odebranie uprawnień pracownikowi następuje na wniosek przełożonego, któremu pracownik podlega; – identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym, w którym są one przetwarzane oraz unieważnić jej hasło.
6.	Czy zapewnione są szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowania minimalizujące ryzyko błędów ludzkich?	X		Tak. Potwierdzeniem odbytych szkoleń posiadają pracownicy oraz ABI. W celu usystematyzowania wiedzy z zakresu bezpieczeństwa informacji odbywają się szkolenia dla pracowników oraz radnych Rady Miasta w Łagowie. Ostatnie szkolenia odbyły się w listopadzie 2018 roku. Ponadto dla osób rozpoczynających pracę w Urzędzie przeprowadzane są szkolenia z zakresu przepisów dot. ochrony tajemnicy zawodowej i innych tajemnic chronionych (ochrona danych osobowych, ochrona informacji niejawnych) oraz z zakresu informatycznego, w tym z funkcjonującego systemu i obsługi sprzętu komputerowego. Z zakresu ochrony danych osobowych, każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z: przepisami ustawy o ochronie danych osobowych oraz obowiązującymi regulacjami wewnętrznymi: Polityką bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją przetwarzania danych osobowych w Urzędzie Miejskim, co potwierdza na oświadczeniu. Dodatkowo osoby upoważnione do przetwarzania danych osobowych realizują szkolenie w formie samokształcenia na postawie materiałów udostępnionych na stronie GIODO. Zapewnione są także szkolenia zewnętrzne dla osób pełniących funkcje ABI i ASI, oraz dla osób odpowiedzialnych.
7.	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu informacji, b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z	X		1) wewnętrzne monitorowanie sieci przez Informatyka Urzędu, 2) konfiguracja sieci i użytkowników zgodnie z ogólnymi wytycznymi, 3) uwierzytelnianie DWUSTOPNIOWE: na poziomie dostępu do zasobów znajdujących się w sieci lokalnej, oraz na poziomie dostępu do aplikacji (jeśli dana aplikacja taką możliwość udostępnia), 4) stosowanie haseł dostępu, 5) przegląd logów systemowych w miarę możliwości czasowych i potrzeb,

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
	przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji?			6) ograniczenie praw dostępu do zasobów; poprzez nadanie uprawnień na wniosek przełożonego, 7) oprogramowanie antywirusowe, 8) automatyczne wygaszanie ekranu oraz odłączenie od sesji po wyznaczonym czasie nieaktywności; ponowne podłączenie możliwe jest załogowaniu użytkownika, 9) stosowania zasady „czystego biurka" po zakończeniu pracy, zabezpieczanie dokumentów w szafach, 10) zabezpieczenia fizyczne, w tym zabezpieczenie serwerowni, 11) monitoring wizyjny Urzędu. –
8.	Czy dokonano ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość?		X	W urzędzie Miasta i Gminy w Łagowie nie ma możliwości pracy w systemie zdalnym.
9.	Czy dokonuje się zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie?			– wykonywanie kopii zapasowych, – kontrola dostępu fizycznego (system kamer, zamykanie dokumentów w szafach), – kontrola dostępu logicznego (logowanie tylko za wpisaniem prawidłowego loginu/ identyfikatora użytkowania i podania hasła), – zabezpieczenia przez atakiem z zewnątrz (router z firewall-em), – oprogramowanie antywirusowe, pracujące w trybie monitora (ikona dostępna na pasku),
10.	Czy umowy serwisowe podpisane ze stronami trzecimi zawierają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji?	X		Umowy serwisowe podpisane ze stronami trzecimi zawierają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.
11.	Czy dokonano ustalenia zasad postępowania z informacjami, zapewniających minima'izację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych?	X		W regulacjach wewnętrznych opisane zostały zabezpieczenia fizyczne i logiczne, w tym m. in: – w Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Miasta i Gminy w Łagowie – określono zasady ochrony danych przetwarzanych w formie elektronicznej (środki ochrony w zakresie zabezpieczenia sprzętowego, środki ochrony w ramach oprogramowania urządzeń teletransmisji, środki ochrony w ramach oprogramowania systemu), zasady ochrony fizycznej pomieszczeń, w których przetwarzane są dane osobowe. – 1. Dane osobowe zapisane w postaci elektronicznej na dyskach twardych nie są wynoszone poza siedzibę Urzędu.

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
				– 2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych. – 3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. – 4. Urządzenia, dyski lub inne elektroniczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych. – 5. Urządzenia, dyski lub inne nośniki, zawierające dane osobowe, przeznaczone do naprawy, zostają naprawiana na miejscu w Urzędzie pod nadzorem osoby upoważnionej. – 6. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym w zamkniętych szafach. – 7. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy. – 8. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie. – 9. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora. – 10. Dodatkowa kontrola antywirusowa przeprowadzana jest na komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania. – 11. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym. – 12. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną. – 13. Pracownik Urzędu użytkujący komputer przenośny zawierający dane osobowe powinien zachować szczególną ostrożność podczas jego transportu i przechowywania poza obszarem przetwarzania danych osobowych, w tym stosuje środki ochrony kryptograficznej.
12.	Czy dokonano zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinfo.·matycznych,	X		

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
	polegającego w szczególności na:			
	a) dbałości o aktualizację oprogramowania?	X		System i program antywirusowy aktualizowany jest automatycznie na każdym stanowisku. Systemy płacowe i księgowe są aktualizowane w momencie pojawienia się aktualizacji. Aktualizacja baz programów geodezyjnych jest realizowana na zgłoszenie pracowników.
	b) minimalizowaniu ryzyka utraty informacji w wyniku awarii?	X		– wykonywanie kopii bezpieczeństwa, które przechowywane są na nośnikach informatycznych w pokoju poza serwerownią. Kopie bezpieczeństwa wykonywane są codziennie na NAS i streamer, po zakończeniu pracy wszystkich użytkowników w sieci komputerowej. – utrzymanie sprawności technicznej sprzętu i oprogramowania, proces konserwacji sprzętu, w szczególności serwerów jest nadzorowany przez osobę odpowiedzialną.
	c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,	X		– określenie środków bezpieczeństwa na poziomie podwyższonym dla przetwarzanych danych osobowych w systemie, o których mowa w przepisach wykonawczych dot. ochrony danych osobowych, – określenie środków bezpieczeństwa dla przetwarzanych informacji niejawnych w systemie, o których mowa w przepisach dot. ochrony informacji niejawnych, – uwierzytelnianie dwustopniowe, – ograniczenie dostępu do zasobów sytemu do osób wyłącznie uprawnionych
	d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa?	X		– logowanie jest zabezpieczeniem haseł dostępu (brak wizualizacji na ekranie), które jest cyklicznie zmieniane, zmiana jest wymuszana przez system,
	e) zapewnieniu bezpieczeństwa plików systemowych?	X		– wykonywanie kopii bezpieczeństwa, – program antywirusowy, – przegląd logów systemowych,
	f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych?	X		aktualizacja zapewniona przez serwer poprawek do Microsoft.
	g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa?	X		aktualizacja zapewniona przez serwer poprawek do Microsoft.

Lp.	Działania w zakresie zarządzania bezpieczeństwem informacji	Określenie stanu faktycznego		Uwagi dotyczące stanu faktycznego *(uzasadnienie udzielonej odpowiedzi, ze wskazaniem na dowody, w tym regulacje wewnętrzne)*
		TAK	NIE	
	h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa?	X		W aktualizowanych regulacjach z zakresu bezpieczeństwa informacji doprecyzowana będzie ścieżka dotycząca monitorowania stanu zabezpieczenia danych osobowych. W zakresie ochrony przetwarzanych w systemie teleinformatycznym informacji niejawnych kontrole zgodności prowadzi wyznaczona osoba.
13.	Czy bezzwłocznie zgłaszane są incydenty naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących?	X		Zapisy dotyczy postępowania w sytuacji naruszenia bezpieczeństwa danych uregulowane w obowiązującej polityce bezpieczeństwa danych osobowych. - w odniesieniu do laptopów uregulowano postępowanie w przypadku zaginięcia lub kradzieży komputera przenośnego, a mianowicie fakt ten należy niezwłocznie zgłosić Burmistrzowi (ADO). Ponadto w przypadku utraty sprzętu należy powiadomić policję i administratora.

3. Sposób klasyfikowania wyników

Kryteriami badania przyjętymi w takcie audytu są zgodność i adekwatność funkcjonujących w Urzędzie rozwiązań w obszarze bezpieczeństwa informacji. Zgodność i adekwatność rozumiane jako zgodność z obowiązującymi przepisami prawa i regulacjami wewnętrznymi oraz adekwatność przyjętych rozwiązań, czy przyjęte rozwiązania są dostosowane do jednostki.

Sposób klasyfikowania wyników dla przyjętych kryteriów	Istotne	Średnie	Mało istotne
Opis	Ustalenia, które w istotny sposób wpływają na prawidłową organizację systemu bezpieczeństwa informacji w jednostce oraz prawidłowe funkcjonowanie wybranych narzędzi tego systemu **powodując**, że nie są one realnymi narzędziami zarządzania. Powinny zostać niezwłocznie usunięte.	Ustalenia, które w istotny sposób wpływają na prawidłową organizację systemu bezpieczeństwa informacji w jednostce oraz prawidłowe funkcjonowanie wybranych narzędzi tego systemu **nie powodując,** że nie są one realnymi narzędziami zarządzania w jednostce.	Ustalenia, które nie wpływają na organizację systemu bezpieczeństwa informacji oraz prawidłowe funkcjonowanie wybranych narzędzi tego systemu, a dotyczą spełnienia wybranych wymogów formalnych.

4.Opinia audytora wewnętrznego w sprawie adekwatności i zgodności kontroli zarządczej w audytowanym obszarze.

Weryfikacja wymagań w zakresie zarządzania bezpieczeństwem informacji wynikających z § 20 Rozporządzenia Rady Ministrów (dalej: Rozporządzenie) 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 2012 r. poz. 526). Zgodnie z tym przepisem, podmiot realizujący zadania publiczne ma obowiązek opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu bezpieczeństwa informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak:

1. Autentyczność (właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane).
2. Rozliczalność (właściwość systemu pozwalająca przypisać określone działania do osoby fizycznej lub procesu oraz umiejscowić je w czasie).
3. Niezaprzeczalność (brak możliwości zanegowania swojego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie).
4. Niezawodność (właściwość oznaczająca spójne, zamierzone zachowanie i skutki).

L.p.	Zakres badania	Opinia audytora	Wnioski
1	Zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;	W Urzędzie systematycznie dokonuje się przeglądów oraz w miarę potrzeby aktualizacji regulacji wewnętrznych. Przyjęte w Urzędzie regulacje w zakresie bezpieczeństwa informacji nie zostały zebrane jednym dokumentem SZBI. **Zgodność i adekwatność.**	Zebrano w jeden dokument poszczególne regulacje wewnętrzne w zakresie bezpieczeństwa informacji zawierają one niezbędne elementy wynikające z rozporządzenia oraz są regularnie przeglądane i aktualizowane. **Mało istotne**
2	Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;	Zorganizowany w Urzędzie system jest sformalizowany, wskazano osobę odpowiedzialną za utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
3	Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;	Przeprowadzane są w Urzędzie okresowe analizy ryzyka w ramach funkcjonującej kontroli zarządczej, działania są zgodne z obowiązującymi w Urzędzie regulacjami. Nie występują dowody wskazujące na ile w ramach okresowej analizy ryzyka były rozważane ryzyka dotyczące utraty integralności, dostępności lub poufności informacji. Należy rozważyć uszczegółowienie. **Zgodność – tak, adekwatność – nie**	Należy rozważyć wprowadzenie do procedur bezpieczeństwa informacji elementów analizy ryzyka związanych z integralnością, dostępnością i poufnością informacji. **Średnie**
4	Podejmowania działań zapewniających, że osoby	Wprowadzono rozwiązania powodujące, że osoby	Nie zachodzi potrzeba poprawy funkcjonującego systemu.

	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;	zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. W Urzędzie obowiązują procedury nadawania uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazuje się osobę odpowiedzialną za te czynności. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych. **Zgodność i adekwatność**	
5	Bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji;	W Urzędzie określono zasady zarządzania uprawnieniami. Określono zasady zarządzania hasłami, użytkownicy zobowiązują się do zachowania haseł w tajemnicy, istnieje zasada wymuszenia zmiany hasła początkowego. Współpraca DZ z DI standard kontroli zarządczej w zakresie komunikacji realizowany. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
6	Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:	Osoby zaangażowane w proces przetwarzania informacji zostały przeszkolone w temacie. Pracownicy Urzędu zostali zapoznani z obowiązującymi procedurami w zakresie bezpieczeństwa informacji. Należy przeprowadzić szkolenia wszystkich pracowników w zakresie bezpieczeństwa informacji. **Zgodność i adekwatność**	W celu usystematyzowania wiedzy z zakresu bezpieczeństwa informacji zaplanowane zostały na 2018r. szkolenia dla wszystkich pracowników.
a) zagrożenia bezpieczeństwa informacji,		**Zgodność i adekwatność**	j.w.
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,		**Zgodność i adekwatność**	j.w.
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;		**Zgodność i adekwatność**	j.w.
7	Zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym	W Urzędzie określono w sposób formalny zasady dotyczące ochrony przetwarzanych informacji, określono zasady	Nie zachodzi potrzeba poprawy funkcjonującego systemu.

	dostępem, uszkodzeniami lub zakłóceniami, przez:	postępowania w sytuacjach naruszenia ochrony danych osobowych. **Zgodność i adekwatność**	
a) monitorowanie dostępu do informacji,		Monitorowanie dostępu realizowane jest poprzez odpowiednie przechowywanie kluczy do budynku (określone Zarządzeniem Burmistrza), stosowaną niepisaną zasadę „czystego biurka", poprzez funkcjonujący w budynku monitoring (kamery umieszczone na korytarzach). Sprawdzania dostępów dokonuje Administrator Bezpieczeństwa Informacji (ABI) w ramach dobrych praktyk. **Zgodność i adekwatność**	Należy doprecyzować sposób postępowania z kluczami do pomieszczeń, w których przetwarzane, przechowywane są dane osobowe. W aktualizowanych regulacjach z zakresu bezpieczeństwa informacji doprecyzowana będzie ścieżka dot. monitorowania stanu zabezpieczenia danych osobowych.
b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,		Administrator Bezpieczeństwa Informacji (ABI) w ramach monitoringu wykonuje czynności zmierzające do wykrycia działań związanych z nieautoryzowanym przetwarzaniem informacji. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;		Zabezpieczenia systemowe **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
8	Ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;	W zakresie pracy na odległość – nie dotyczy **Zgodność i adekwatność**	Nie dotyczy
9	Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;	W Urzędzie podstawowym zabezpieczeniem informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie jest tworzenie kopii zapasowych oraz przestrzeganie zasad dostępu. Dokonano podziału ról i odpowiedzialności w zakresie uprawnień do dostępu do informacji. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
10	Zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;	W umowach serwisowych ze stronami trzecimi, znajdują się klauzule gwarantujące odpowiedni poziom bezpieczeństwa informacji. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
11	Ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;	W Urzędzie ustalono zasady postępowania z informacjami, zasady te zostały zaakceptowane, odpowiednio zakomunikowane oraz wdrożone. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.

12	Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:	Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych zapewnia powierzono Administratorowi Systemu. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
a) dbałości o aktualizację oprogramowania,		Aktualizacja wynika z potrzeb użytkowników. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,		Minimalizuje ryzyko utraty informacji w wyniku awarii codzienne tworzenie kopii zapasowych. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,		Ochronę przed błędami, utratą, nieuprawnioną modyfikacją zapewnia codzienne tworzenie kopii zapasowych **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,		zmiana jest wymuszana przez system **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
e) zapewnieniu bezpieczeństwa plików systemowych,		- wykonywanie kopii bezpieczeństwa - program antywirusowy - przegląd logów systemowych **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,		Redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych zabezpieczają aktualizacje oprogramowania, antywirus. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,		W Urzędzie nie odnotowano podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;		Systemy teleinformatyczne działające w Urzędzie funkcjonują zgodnie z przyjętą polityką bezpieczeństwa informacji. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.
13	Bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.	Urzędzie nie odnotowano incydentów naruszenia bezpieczeństwa informacji. Zasady postępowania w takich przypadkach zostały szczegółowo określone w regulacjach wewnętrznych. **Zgodność i adekwatność**	Nie zachodzi potrzeba poprawy funkcjonującego systemu.

5. Ustalenia audytu

Celem audytu wewnętrznego prowadzonego w formie zadania zapewniającego było zebranie informacji na temat funkcjonującego w Urzędzie systemu bezpieczeństwa informacji oraz weryfikacja wymagań w zakresie zarządzania bezpieczeństwem informacji wynikających z § 20 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 2012 r. poz. 526).

Na podstawie przeprowadzonego zadania zapewniającego, po dokonaniu przeglądu dokumentacji, przeprowadzeniu wywiadów z audytowanymi oraz na podstawie wyników przeprowadzonych testów można uznać, że w Urzędzie Miasta i Gminy w Łagowie obszar bezpieczeństwa informacji jest zarządzany w usystematyzowany sposób, generalnie spełnia wymogi rozporządzenia.

Na tym sprawozdanie zakończono.

6. Zakończenie

Sprawozdanie sporządzono w trzech jednobrzmiących egzemplarzach.
Stosownie do przepisów § 19 ust 1. Kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki.
ust 2. Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie kierownika komórki audytu wewnętrznego i kierownika jednostki.
Rozporządzenia Ministra Finansów z dnia 04 września 2015 r. w sprawie audytu wewnętrznego oraz informacji pracy i wynikach tego audytu (Dz. U. poz. 1480 28 września 2015 r).

mgr Grzegorz Palacz
Audytor Wewnętrzny
Upoważnienie Nr 1679/2009
(data i podpis audytora)
05.11.2018 r.