Zarządzenie nr 124/17
Wójta Gminy Żurawica
z dnia 30.11.2017

w sprawie podjęcia i przeprowadzenia Analizy identyfikacji zagrożeń, szacowania oraz sposobu postępowania z ryzykiem dla bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy Żurawica

Na podstawie: art. 20 ust.2 pkt 3 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jednolity Dz. U. z 2016 r., poz. 113, z późn. zm.) oraz art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, (tekst jednolity Dz. U. z 2016 r., poz. 922) i rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024) oraz zarządzam, co następuje:

§1. Wprowadzam w życie wyniki i sposób postępowania z ryzykiem w oparciu o Analizę identyfikacji zagrożeń, szacowania oraz sposobu postępowania z ryzykiem dla bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy Żurawica stanowiącą załącznik do niniejszego zarządzenia.

§2. Wykonanie zarządzenia w zakresie wprowadzenia w życie wyników i postępowania z ryzykiem w oparciu o Analizę identyfikacji zagrożeń, szacowania oraz sposobu postępowania z ryzykiem dla bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy Żurawica powierza się Komitetowi Bezpieczeństwa Informacji (KBI).

§3. Zarządzenie wchodzi w życie z dniem jego podjęcia.

Wójt Gminy Żurawica
Krzysztof Składowski

Załącznik nr 1 do zarządzenia
Wójta Gminy Żurawica nr 124/17
z dnia 30.11.2017 r.

ANALIZA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW INFORMATYCZNYCH POD KĄTEM IDENTYFIKACJI ZAGROŻEŃ, SZACOWANIA ORAZ SPOSOBU POSTĘPOWANIA Z RYZYKIEM

zwana dalej:

ANALIZĄ IDENTYFIKACJI ZAGROŻEŃ, SZACOWANIA ORAZ SPOSOBU POSTĘPOWANIA Z RYZYKIEM DLA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH w Urzędzie Gminy Żurawica

zgodnie z:

art. 20 ust.2 pkt. 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, (tekst jednolity Dz. U. z 2016 r., poz. 113, z późn. zm.) zwanym dalej rozporządzeniem KRI, oraz art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, (tekst jednolity Dz. U. z 2016 r. poz. 922) i rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024),

wprowadza się dokument o nazwie:

ANALIZA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW INFORMATYCZNYCH POD KĄTEM IDENTYFIKACJI ZAGROŻEŃ, SZACOWANIA ORAZ SPOSOBU POSTĘPOWANIA Z RYZYKIEM

zwany dalej:

ANALIZĄ IDENTYFIKACJI ZAGROŻEŃ, SZACOWANIA ORAZ SPOSOBU POSTĘPOWANIA Z RYZYKIEM PRZY PRZETWARZANIU INFORMACJI I DANYCH OSOBOWYCH w Urzędzie Gminy Żurawica

1. Wstęp

Administrator danych ze względu na ciążący na nim obowiązek przeprowadzania okresowych analiz i szacowania ryzyka dla bezpieczeństwa informacji i ochrony danych osobowych, a wynikający z wymogów § 20 ust 2 pkt 3 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku 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) zwanym dalej rozporządzeniem KRI, oraz ustawy o ochronie danych osobowych, w szczególności z art. 36 ustawy, zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych, adekwatnie do występujących zagrożeń, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W związku z tym Administrator danych podejmuje i realizuje działania w zakresie analizy identyfikacji zagrożeń i ryzyka w celu stosowania odpowiednich standardów bezpieczeństwa informacji i danych osobowych oraz wspiera przedsięwzięcia i inicjatywy związane z ich rzeczywistą ochroną i zabezpieczaniem.

Celem przeprowadzania analizy identyfikacji zagrożeń i ryzyka jest dostarczenie informacji do podjęcia decyzji, co do rodzaju i liczby środków zmniejszających podatność systemu na zagrożenia bezpieczeństwa dla systemu informacyjnego Urzędu Gminy Żurawica. Przyjęta metodyka w zakresie szacowania ryzyka stanowi podstawę do podejmowania decyzji o stosowaniu skutecznych i adekwatnych do potencjalnych zagrożeń zabezpieczeń przez Administratora danych.

Skuteczność zastosowanych środków bezpieczeństwa będzie podlegać cyklicznym badaniom i sprawdzeniom przy współudziale członków KBI. Przy stosowaniu zabezpieczeń powinno się uwzględniać zmieniające się warunki techniczno-organizacyjne oraz postęp informatyczny, co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez Administratora danych systemów bezpieczeństwa.

2. Definicje

a) **Analiza ryzyka** – proces oceny ryzyka, którego zadaniem jest redukcja ryzyka do akceptowalnych poziomów i utrzymanie tego poziomu ryzyka. Systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.

b) **Szacowaniu ryzyka** – proces oceny i analizy ryzyka.

c) **Ocenie ryzyka** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka.

d) **Postępowaniu z ryzykiem** – wdrażanie środków modyfikujących i zmniejszających występowalne ryzyko.

e) **Zarządzaniu ryzykiem** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka.

f) **Akceptowaniu ryzyka** – podjęcie decyzji o zaakceptowaniu ryzyka.

g) **Bezpieczeństwie informacji** – zachowanie poufności, integralności i dostępności informacji.

h) **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

i) **Poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

j) **Rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

k) **Podatność** - słabość zasobów informacyjnych, która może być wykorzystana przez zagrożenie.

l) **Zabezpieczenie** – należy przez to rozumieć środki o charakterze fizycznym, technicznym, lub organizacyjnym zmniejszające ryzyko.

3. Ogólne wymogi i mechanizmy bezpieczeństwa przetwarzanych informacji i danych osobowych, wprowadzone przez Administratora danych;

1) Procedury i dokumentacja tj. System Zarządzania Bezpieczeństwem Informacji wraz z procedurami bezpieczeństwa, System Ochrony Danych Osobowych,

2) Organizacja bezpieczeństwa informacji i danych osobowych (zarządzanie systemami teleinformatycznymi w kontekście ich interoperacyjności, zarządzanie systemami informatycznymi przetwarzającymi dane osobowe),
3) Szkolenia i edukacja osób upoważnionych i uprawnionych do przetwarzania informacji danych osobowych,
4) Bezpieczeństwo fizyczne i środowiskowe,
5) Zarządzanie systemami i sieciami informatycznymi, kontrola dostępu,
6) Pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
7) Zarządzanie incydentami związanymi z bezpieczeństwem informacji i danych osobowych,

W Urzędzie Gminy Żurawica przyjęto, że proces zarządzania ryzykiem dla zapewnienia bezpieczeństwa informacji i ochrony danych osobowych prowadzony będzie w oparciu o poniższe kryteria i polegał będzie on na:

1. Ustanowieniu kontekstu
   (ustaleniu zakresu i granic, osób odpowiedzialnych i uczestniczących oraz przyjęciu metody szacowania ryzyka systemu zarządzania bezpieczeństwem informacji, np. wg kryteriów: oceny ryzyka, skutków, akceptowania ryzyka)
2. Szacowaniu ryzyka
   (zidentyfikowaniu ryzyk dla danych osobowych, przypisaniu im właściciela i wartości oraz odniesieniu do kryteriów oceny)
3. Postępowaniu z ryzykiem
   (zdecydowaniu o sposobie zabezpieczenia: zredukowaniu, zachowaniu, uniknięciu lub transferze ryzyk i określeniu planu postępowania z ryzykiem)
4. Akceptowaniu ryzyka
   (formalnym udokumentowaniu i akceptacji ryzyk)
5. Informowaniu o ryzyku
   (poinformowaniu stron, których ryzyko dotyczy o podjętych decyzjach)
6. Monitorowaniu i przeglądzie ryzyka
   (monitorowaniu i przeglądzie ryzyk i ich czynników, -tj. wartości zbiorów, skutków, zagrożeń, podatności, prawdopodobieństwa wystąpienia przeciwdziałania)

Uwzględniono aspekty bezpieczeństwa w niektórych, newralgicznych obszarach działalności urzędu.

Dobór środków zabezpieczenia informacji i danych osobowych powinien być adekwatny do potrzeb. Powinien wynikać z przeprowadzanej analizy ryzyka i być uwzględniony w okresowym zarządzaniu ryzykiem.

4. Zagrożenia występujące w systemach informatycznych

Celem zarządzania incydentami w ramach informacji i ochrony danych jest zminimalizowanie potencjalnych ryzyk i negatywnych skutków niepożądanych zdarzeń w procesie przetwarzania danych, będących następstwem działań na szkodę tego procesu (w systemie informatycznym i w systemie tradycyjnym).

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności, rozliczalności i dostępności danych w systemie informatycznym:

- utrata usługi[1], urządzenia lub funkcjonalności,
- przeciążenie lub niepoprawne działanie systemu,
- błędy ludzkie,
- niezgodność z politykami, procedurami lub zaleceniami,
- naruszenie ustaleń związanych z bezpieczeństwem fizycznym,
- niekontrolowane zmiany systemu,
- niepoprawne działanie oprogramowania lub sprzętu,
- naruszenia dostępu,

Szczególnie: w systemach informatycznych:

- atak oprogramowania szkodliwego *(np. wirus, koń trojański)*,
- uszkodzenie systemu informatycznego,
- luki zabezpieczeń w systemie teleinformatycznym *(np. pliki na kopiach awaryjnych tracą zabezpieczenie wynikające z praw dostępu określonych w systemie operacyjnym)*,
- niewłaściwe skonfigurowanie systemu, którego skutkiem jest udostępnienie zasobów podmiotowi nieuprawnionemu *(np. brak hasła, brak aktywowanej funkcji blokady klawiatury czy wygaszacza ekranowego, czy obecność trwale aktywnych standardowych haseł)*,
- świadoma lub nieświadoma nieuprawniona ingerencja w system teleinformatyczny osób trzecich, tj.:
  - nieświadome – wynikające z braku wiedzy użytkownika dotyczącej obsługi,
  - nieświadome – wynikające z nieświadomego przekazania *(np. podpatrzenie przez osobę trzecią, atak socjotechniczny)* uprawnień dostępu podmiotowi nieuprawnionemu,
  - świadome – udostępnienie podmiotowi nieuprawnionemu dostępu do zasobów,

[1] Np.: utrata dostępności, np. do katalogu sieciowego.

- świadome – naruszenia poufności lub integralności systemu informatycznego *(udostępnienie plików, wydruków, lub ich uszkadzanie)*.

- ujawnienie osobom nieupoważnionym informacji lub objętych tajemnicą procedur ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.
- niewylogowanie się z systemu informatycznego przed opuszczeniem stanowiska pracy,
- nie wykonanie w określonym terminie kopii bezpieczeństwa,
- nieprawidłowości w zakresie zabezpieczenia nośników i miejsc przechowywania informacji i danych osobowych,

4. Analiza ryzyka

Administrator danych, aby poprawnie przeprowadzić analizę ryzyka, powinien określić:

1. ZASOBY - które trzeba chronić np.;
    1) sprzęt komputerowy, na którym przetwarzane są informacje i dane osobowe,
    2) zbiory danych osobowych, które przetwarzane są w formie papierowej i elektronicznej,
    3) zasoby sieciowe i programowe, w których przetwarzane są informacje,
    4) obszary przetwarzania informacji i danych osobowych,
2. ZAGROŻENIA - czynnik, który może powodować wystąpienie incydentu,
3. PODATNOŚĆ - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie,
4. SKUTKI - jaki wpływ będzie miał zaistniały incydent na utratę informacji i danych osobowych,

Analizę ryzyka przeprowadza się w poszczególnych kategoriach zagrożeń zgodnie z tabelą nr 1, w której określono typowy wykaz zagrożeń i związanych z nimi podatności. Wykaz zagrożeń i podatności może zostać rozszerzony w miarę powstania nowych zagrożeń dla systemu informacyjnego.

Analizę ryzyka prowadzi się okresowo (nie rzadziej niż raz na rok). Źródła potencjalnych ryzyk mogą być zgłoszone osobie odpowiedzialnej za szacowanie ryzyka w każdym momencie, przez każdego interesariusza systemu.

Analizy ryzyk dokonuje np. zespół KBI wyznaczony przez Administratora danych posiadający stosowną wiedzę i doświadczenie z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

Na analizę ryzyka składają się:

a) szacowanie skutków,
b) analiza podatności na dane zagrożenie,
c) analiza zabezpieczeń,

4. Szacowanie skutków

Ocena skutków (konsekwencji) w przypadku wystąpienia zagrożeń dla bezpieczeństwa informacji tj. utraty poufności, integralności, dostępności - dokonywana jest w oparciu o poniższe kryteria:

Skutki utraty poufności, integralności, dostępności	**Opis**
pomijalne (0 pkt)	ewentualne szkody w przypadku przełamania, zniszczenia lub awarii zabezpieczeń są ograniczone i pomijalne
niskie (1pkt)	niewielki wpływ negatywny na realizację zadań jednostki lub możliwe niewielkie utrudnienia w realizacji zadań służbowych pracowników
wysokie (2 pkt)	znaczący negatywny wpływ na realizację zadań jednostki, konsekwencje prawne lub istotne utrudnienia w realizacji zadań służbowych pracowników lub widoczny wpływ na wizerunek jednostki
bardzo wysokie (3pkt)	brak możliwości realizacji zadań jednostki, istotne konsekwencje prawne lub istotny negatywny wpływ na wizerunek jednostki

5. Szacowanie podatności (słabości) systemu informacyjnego;

Podatność systemu na zagrożenia może wynikać np. z:

- braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę jak obsługiwać system,
- dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych,

- możliwości celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych,
- możliwości awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję,
- przesyłania informacji przez niezabezpieczone łącza telekomunikacyjne.

Szacowanie podatności zasobów, która może być wykorzystana przez zagrożenie dokonywana jest zgodnie z poniższymi kryteriami:

Podatność	Opis
brak podatności (0pkt)	wdrożono kompleksowe mechanizmy zabezpieczające
niski poziom podatności (1pkt)	istnieją wady w strukturze zabezpieczeń fizycznych i informatycznych, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym - skutkują naruszeniem polityki bezpieczeństwa
średni poziom podatności (2pkt)	istnieją istotne wady lub luki w sprzęcie lub oprogramowaniu lub w zabezpieczeniach fizycznych, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym - skutkuje złamaniem zabezpieczeń
wysoki poziom podatności (3 pkt)	brak odpowiednich środków zabezpieczających w tym niska świadomość personelu

6. Określanie poziomu ryzyka

Określanie poziomu ryzyka polega na ustaleniu wpływu wystąpienia zagrożenia na:

1) dostępność systemu lub informacji,
2) integralność systemu lub informacji,
3) poufność informacji przetwarzanej w systemie,

a następnie wyznaczeniu poziomu ryzyka, które stanowi zależność:

Ryzyko = iloczyn wartości skutków i podatności zasobów systemu

Skala poziomu oszacowanego ryzyka dla danego zasobu zawarta jest w poniższej tabeli. Do oceny ryzyka zastosowano 3 stopniową skalę. W stosunku do ryzyk ocenianych, jako

„Duże” i **„Bardzo duże”** niezbędne jest podjęcie działań redukujących ich poziom – do poziomu akceptowalnego.

Ryzyko	Opis
Akceptowalne (0-3pkt)	podjęte działania zabezpieczające są wystarczające
Duże (4-6pkt)	niezbędne podjęcie działań redukujących duży poziom ryzyka do poziomu akceptowalnego
Bardzo duże (pow.6pkt)	niezbędne podjęcie działań redukujących bardzo duży poziom ryzyka do poziomu akceptowalnego

7. Ograniczanie ryzyka

Podstawowym sposobem postępowania z ryzykiem jest stosowanie zabezpieczeń w oparciu o wyniki analizy ryzyka. Zastosowane zabezpieczenia powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, oraz wymagania wynikające z analizy ryzyka dla działania i funkcjonowania urzędu. W przypadku zastosowania określonego typu zabezpieczenia powinno ono powodować obniżenie skutków (konsekwencji) zagrożenia w szczególności dla bezpieczeństwa teleinformatycznego urzędu.

ARKUSZ OKRESOWEJ ANALIZY RYZYKA wg. STANU NA DZIEŃ 30.11.2017r.

Zasoby	Źródła zagrożeń	Rodzaje zagrożeń	Wpływ na utratę			Skutki waga (a)	Podatność (b)	Ryzyko (a x b)	Zabezpieczenia	Zabezpieczenia wdrożone T/N	Właściciel ryzyka
			Poufności	Dostępności	Integralności						
Sprzęt komputerowy	Siły wyższe	(czynnik zewnętrzny-losowy) pożar		x		3	2	**6**	• System sygnalizacji przeciwpożarowej, • Ochrona kopii bezpieczeństwa	• Budynek spełnia wymagania przeciwpożarowe/ gaśnice wolno-stojące • Kopie bezpieczeństwa dla systemu IT	Administrator Systemu Informatycznego (ASI)
		(czynnik zewnętrzny-losowy) zalanie wodą		x		2	2	**4**	• Ochrona fizyczna zabezpieczeń obszarów bezpieczeństwa np. serwerownia/procedury kontrolne • Umieszczenie kopii bezpieczeństwa w innej lokalizacji	• Przeglądy i konserwacje instalacji • Sygnalizacja alarmowa • Kopie bezpieczeństwa dla systemu IT	Administrator Systemu Informatycznego (ASI)
		(czynnik zewnętrzny-losowy) awarie (zanik) zasilania		x	x	2	2	**4**	• Ciągłość zasilania urządzeń sieciowych (UPS-y) • Zbudowanie stabilnej sieci zasilającej • backupy	• Przeglądy sieci zasilającej • Zastosowanie UPS w serwerowni • Kopie zapasowe serwerów	Administrator Systemu Informatycznego (ASI)
		(czynnik zewnętrzny-losowy) kradzież	x	x		3	2	**6**	• Kontrola dostępu, system monitoringu wizyjnego	• Przeglądy i konserwacje instalacji alarmowej, monitoringu • Zastosowano procedury bezpieczeństwa (zamykanie pomieszczeń na klucz)	Kadra kierownicza, (kierownicy komórek organizacyjnych) pracownicy
Personel	Błędy personelu	Błędy administratora	X	x	x	2	2	**4**	• Serwisowanie sprzętu komputerowego	• Konserwacja i serwisowanie sprzętu komputerowego	Administrator Systemu Informatycznego (ASI)

	obsługującego sprzęt komputerowy								• Oprogramowanie antywirusowe	• Zastosowano oprogramowanie antywirusowe na końcówkach klienckich i serwerach	Administrator Systemu Informatycznego (ASI)
									• Przechowywanie i tworzenie kopii zapasowych	• Kopie bezpieczeństwa dla systemu IT	Administrator Systemu Informatycznego (ASI) Użytkownicy
									• Prowadzenie ewidencji sprzętu i oprogramowania wraz z konfiguracją	• Prowadzona jest jedynie ewidencja środków trwałych	Administrator Systemu Informatycznego (ASI) Administrator Bezpieczeństwa Informacji (ABI)
		Nieumiejętne posługiwanie się systemem przez użytkownika	X	x	x	1	1	1	• Szkolenia wstępne dla pracowników nowozatrudnionych	• Plany szkoleń	Administrator Systemu Informatycznego (ASI) Kierownicy komórek organizacyjnych Administrator Bezpieczeństwa Informacji (ABI)
									• Okresowe szkolenia dla pracowników już zatrudnionych • Szkolenia okresowe (wewnętrzne, zewnętrzne)	• Plany szkoleń	Administrator Systemu Informatycznego (ASI) Kierownicy Referatów Administrator Bezpieczeństwa Informacji (ABI)
		Nieuprawniony dostęp do informacji	X	x	x	1	1	1	• Uwierzytelnienie użytkowników w systemie/autoryzacja	• Kontrola dostępu do stanowisk komputerowych • Wdrożenie procedur kontrolnych • Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Ochrony Danych Osobowych	Administrator Systemu Informatycznego (ASI) Kierownicy komórek organizacyjnych Administrator Bezpieczeństwa Informacji (ABI)
									• Autoryzacja i kontrola dostępu do zasobów	• Kontrola dostępu do stanowisk komputerowych • Wdrożenie procedur kontrolnych	Administrator Systemu Informatycznego (ASI) Kierownicy komórek organizacyjnych

									• Wdrożenie Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym oraz procedur bezpieczeństwa w ramach Systemu Zarządzania Bezpieczeństwem Informacji • Wydzielenie stref ochronnych	Administrator Bezpieczeństwa Informacji (ABI)
		Nieuprawniona lub przypadkowa modyfikacja informacji	X	x	x	1	1	1	• Kontrola dostępu do danych	• Kontrola dostępu do stanowisk komputerowych • Wdrożenie procedur kontrolnych • Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Ochrony Danych Osobowych	Administrator Systemu Informatycznego (ASI) Kierownicy komórek organizacyjnych Administrator Bezpieczeństwa Informacji (ABI)
									• Rejestracja operacji na danych	• Użycie specjalistycznego oprogramowania • Zabezpieczanie haseł	Administrator Systemu Informatycznego (ASI) Użytkownicy Administrator Bezpieczeństwa Informacji (ABI)
									• Kontrola antywirusowa	• Zastosowanie oprogramowania antywirusowego	Administrator Systemu Informatycznego (ASI)
		Nieautoryzowany dostęp do informacji	X	x	x	1	1	1	• Stosowanie zasady wiedzy koniecznej (need to know)	• Ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę, jak je obsługiwać	Administrator Systemu Informatycznego (ASI) Administrator Bezpieczeństwa Informacji (ABI)
									• Procedury przeglądania uprawnień w systemach	• Prowadzenie odpowiedniej dokumentacji • Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Ochrony Danych Osobowych	Administrator Systemu Informatycznego (ASI) Kierownicy komórek organizacyjnych Administrator Bezpieczeństwa Informacji (ABI)

									• Procedury nadawania i odbierania uprawnień w systemie	• Wdrożenie procedur kontrolnych • Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Ochrony Danych Osobowych	Administrator Systemu Informatycznego (ASI) Administrator Bezpieczeństwa Informacji (ABI)
Oprogramowanie oraz Infrastruktura (stacje robocze, serwery, urządzenia sieciowe, linie transmisji danych)	Konfiguracja serwerów, stacji roboczych, urządzeń sieciowych i aplikacji	Awarie urządzeń i błędy oprogramowania	X	x	x	1	1	1	• Procedury zakupu sprzętu komputerowego i oprogramowania	• Planowanie zakupów w bieżącym roku i na rok następny	Administrator Systemu Informatycznego (ASI)
									• Archiwizacja (backup) danych	• Kopie bezpieczeństwa dla systemu IT	Administrator Systemu Informatycznego (ASI)
									• Kontrola antywirusowa	• Zastosowano oprogramowanie antywirusowe na końcówkach klienckich i serwerach	Administrator Systemu Informatycznego (ASI)
	Działania przestępcze	Kradzieże sprzętu komputerowego i nośników informacji	x	x	x	2	2	4	• Kontrola fizycznego dostępu do obiektów i pomieszczeń (identyfikacja osób)	• Pomieszczenia zamykane na klucz	Kierownicy komórek organizacyjnych Administrator Bezpieczeństwa Informacji (ABI)
									• Zabezpieczenie przeciw włamaniom: konstrukcje antywłamaniowe, urządzenia alarmowe	• Monitoring CCTV, system alarmowy	Administrator Systemu Informatycznego (ASI) Administrator Bezpieczeństwa Informacji (ABI)
		Wniknięcie kodu złośliwego z sieci WAN	x	x	x	1	1	1	• Zapory sieciowe skonfigurowane według zasady „wszystko jest zabronione, z wyjątkiem tego, na co wyrażono zgodę”	• Zastosowano firewall sprzętowy	Administrator Systemu Informatycznego (ASI)
									• Systemy klasy IDS/IRS	• Zastosowano firewall sprzętowy z systemami IPS/IDS	Administrator Systemu Informatycznego (ASI)
									• Wykrywanie i blokowanie spamu	• Filtrowanie realizowane na poziomie usługi poczty	Administrator Systemu Informatycznego (ASI)
									• Oprogramowanie antywirusowe	• Zastosowano oprogramowanie antywirusowe na	Administrator Systemu Informatycznego (ASI)

									końcówkach klienckich i serwerach	
								• Skanery sieciowe	• Wdrożono na poziomie dostępu do sieci urządzenia monitorujące	Administrator Systemu Informatycznego (ASI)
								• Procedury reagowania na wykryte incydenty	• Monitoring aktywności w sieci realizowany przez system, analiza logów systemu • Wsparcie firmy zewnętrznej w ramach umowy.	Administrator Systemu Informatycznego (ASI)
		Wprowadzenie kodu złośliwego z sieci LAN	x	x	x	2	2	4	• Blokowanie możliwości instalowania oprogramowania przez użytkownika	• Kontrola bieżąca uprawnień użytkowników	Administrator Systemu Informatycznego (ASI) Administrator Bezpieczeństwa Informacji (ABI)
									• Blokowanie portów USB na stacjach roboczych	• Realizowane przez oprogramowanie antywirusowe	Administrator Systemu Informatycznego (ASI)
									• Blokowanie możliwości instalowania oprogramowania przez użytkownika	• Kontrola bieżąca uprawnień użytkowników	Administrator Systemu Informatycznego (ASI)
									• Weryfikacja zainstalowanego oprogramowania na stacjach roboczych	• Dedykowane oprogramowanie do zarządzania stacjami roboczymi	Administrator Systemu Informatycznego (ASI)
									• Oprogramowanie antywirusowe	• Zastosowano oprogramowanie antywirusowe na końcówkach klienckich i serwerach	Administrator Systemu Informatycznego (ASI)
									• Procedury uaktualnienia oprogramowania	• Systemy i oprogramowanie antywirusowe automatycznie • Pozostałe oprogramowanie statycznie po przejściu testów	Administrator Systemu Informatycznego (ASI)
		Atak typu DDoS lub DoS		x			1	1	• Monitorowanie ruchu w sieci	• Zastosowano firewall sprzętowy z systemami IPS/IDS	Administrator Systemu Informatycznego (ASI)

									• Blokowanie ruchu sieciowego z określonych adresów IP	• Zastosowano firewall sprzętowy z systemami IPS/IDS	Administrator Systemu Informatycznego (ASI)
									• Umowy z dostawcami usługi dostępu do Internetu zawierające klauzule przenoszące działania przeciw atakowi na dostawcę	• Gwarancja na pasmo dostępu do Internetu	Administrator Systemu Informatycznego (ASI)
									• Procedury postępowania na wypadek wykrycia ataku DDoS/DoS	• Blokada atakujących automatycznie przez firewall, w razie dalszych problemów redundancja łącza i przekierowanie ruchu na routerach, firewall.	Administrator Systemu Informatycznego (ASI)
		Nieuprawnione działania w sieci komputerowej	X	x	x	2	2	**4**	• Blokowanie możliwości instalowania oprogramowania przez użytkownika	• Kontrola uprawnień użytkowników	Administrator Systemu Informatycznego (ASI) Administrator Bezpieczeństwa Informacji (ABI)
									• Weryfikacja, czy na stacji roboczej znajduje się wyłącznie dopuszczalne oprogramowanie	• Kontrola uprawnień użytkowników	Administrator Systemu Informatycznego (ASI)
									• Okresowe przeglądanie logów stacji roboczej przez administratorów	• Osobiście przez uprawnioną osobę	Administrator Systemu Informatycznego (ASI)
									• Działalność szkodliwego oprogramowania (wirusy, trojany, ransomware itp.)	• Centralnie zarządzany system antywirusowy	Administrator Systemu Informatycznego (ASI)

WNIOSKI I DZIAŁANA NAPRAWCZEW ZWIAZKU Z PRZEPROWADZONĄ ANALIZĄ IDENTYFIKACJI ZAGROŻEŃ, SZACOWANIA ORAZ SPOSOBU POSTĘPOWANIA Z RYZYKIEM PRZY PRZETWARZANIU INFORMACJI I DANYCH OSOBOWYCH
w Urzędzie Gminy Żurawica

§1

1. Administrator danych przeprowadził analizę dla wybranych chronionych zasobów informacyjnych i możliwych zagrożeń dla bezpieczeństwa informacji i danych osobowych.
2. Administrator danych jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, informatyczne jak i fizyczne oraz organizacyjne, do wyników, jakie oddała przeprowadzona analiza.
3. Ewentualne zmiany i udoskonalenia związane z pkt 2 należy uwzględnić i określić w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Ochrony Danych Osobowych przyjętych w Urzędzie Gminy Żurawica.

§2

W wyniku przeprowadzonej analizy w Urzędzie Gminy Żurawica, Administrator danych wyróżnił potencjalnie najniebezpieczniejsze zagrożenia, a w szczególności są to:

- system monitoringu wizyjnego wymaga modernizacji
- nie jest prowadzona inwentaryzacja sprzętu, oprogramowania i jego konfiguracji na zgodność z wymaganiami rozporządzenia KRI

§3

Administrator danych w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy, podejmuje działania naprawcze, polegające w szczególności na:

- odebranie uprawnień administratora systemu wszystkim pracownikom, którym takie uprawnienia nie są niezbędne,
- wykonaniu modernizacji systemu zabezpieczeń monitoringu wizyjnego,
- prowadzeniu ewidencji/inwentaryzacji sprzętu i oprogramowania i jego konfiguracji na zgodność z wymaganiami rozporządzenia KRI

PODSUMOWANIE

W Urzędzie Gminy Żurawica po przeprowadzeniu analizy i poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i identyfikacji ryzyka, zwanej dalej analizą identyfikacji zagrożeń, szacowania oraz sposobu postępowania z ryzykiem przy przetwarzaniu informacji i danych osobowych wartość poziom ryzyka przedstawia się następująco:

POZIOM RYZYKA **„Duże"**

Niezbędne jest podjęcie działań redukujących poziom duży – do poziomu akceptowalnego.

(członkowie KBI)

(data i podpis) 30.11.2017

(data i podpis) 30.11.2017

(data i podpis) 30.11.2017

ZATWIERDZIŁ (Administrator danych)

(data i podpis) 30.11.2017 Wójt Gminy Żurawica Krzysztof Składowski