ZARZĄDZENIE NR 148/14
WÓJTA GMINY GRÓDEK

z dnia 3 lipca 2014 r.

w sprawie zatwierdzenia dokumentu „Szacowanie ryzyka i analiza poziomu zagrożeń dla systemu ochrony informacji niejawnych Urzędu Gminy Gródek”

Na podstawie § 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012, poz. 683), zarządzam, co następuje:

§ 1. W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego, zatwierdzam opracowany przez Pełnomocnika do spraw Ochrony Informacji Niejawnych dokument „Szacowanie ryzyka i analiza poziomu zagrożeń dla systemu ochrony informacji niejawnych Urzędu Gminy Gródek”, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Nadzór nad realizacją niniejszego zarządzenia powierzam Pełnomocnikowi do spraw Ochrony Informacji Niejawnych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do Zarządzenia Nr 148/14
Wójta Gminy Gródek
z dnia 3 lipca 2014 r.

Urząd Gminy Gródek

ul. A. i G. Chodkiewiczów 2

16-040 Gródek

Zatwierdzam:

SZACOWANIE RYZYKA I ANALIZA POZIOMU ZAGROŻEŃ DLA SYSTEMU OCHRONY INFORMACJI NIEJAWNYCH URZĘDU GMINY GRÓDEK

OPRACOWAŁ:

Pełnomocnik ds. ochrony
informacji niejawnych
Dorota Bójko

Gródek, lipiec 2014 r.

Niniejszy dokument został opracowany na podstawie § 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012, poz. 683).

Celem opracowania jest określenie poziomu zagrożeń dla systemu ochrony informacji niejawnych w Urzędzie Gminy Gródek oraz dokonanie oceny zastosowanych środków bezpieczeństwa w przedmiotowym systemie, pod kontem wymagań określonych w wyżej wymienionym rozporządzeniu. Analizą objęto budynek Urzędu Stanu Cywilnego, zlokalizowany pod adresem: 16-040 Gródek, ul. Fabryczna 8, w którym zlokalizowana jest Kancelaria Materiałów Niejawnych, będąca głównym miejscem przetwarzania informacji niejawnych oraz przechowywania materiałów i dokumentów niejawnych.

I. Analiza poziomu zagrożeń

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego, określa się poziom zagrożeń związanych z utratą poufności, dostępności lub integralności, z ujawnieniem lub utratą informacji niejawnych, zwany „poziomem zagrożeń”. Poziom zagrożeń określa się dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

W celu określenia poziomu zagrożeń przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, a w szczególności:

1. klauzule tajności przetwarzanych informacji niejawnych;
2. postać i ilość informacji niejawnych;
3. sposób przechowywania informacji niejawnych;
4. otoczenie i strukturę budynków lub obszarów, w których przetwarzane są informacje niejawne;
5. ilość osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzyskaną potrzebę dostępu do informacji niejawnych;
6. inne czynniki wynikające ze specyfiki jednostki organizacyjnej, nie wykazane powyżej, a mogące mieć wpływ na ochronę informacji niejawnych, np.: działalnie obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działalnie sił przyrody (np. obszar zagrożony powodzią) lub szkody górnicze.

Poziom zagrożeń ustala się na podstawie wyboru "oceny istotności czynnika" mającego wpływ na ujawnienie lub utratę informacji niejawnych w jednostce organizacyjnej. Z uzasadnienia oceny (sporządzonej według wskazań przedstawionych w "Tabeli oceny istotności czynników zagrożeń") powinno wynikać, jakie znaczenie dla jednostki organizacyjnej ma konkretny czynnik (czy jest bardzo istotny, czy mało istotny), a nie to, w jaki sposób czy za pomocą, jakich środków bezpieczeństwa fizycznego zabezpieczono informacje niejawne. Wynik analizy dokonanej w konkretnej jednostce organizacyjnej ma znaczenie dla określenia poziomu zagrożeń w zależności od tego, czy wskazane w "Tabeli oceny istotności czynników zagrożeń" czynniki bierze się pod uwagę jako: "bardzo istotne", "istotne" albo "mało istotne" dla zagrożenia ujawnieniem lub utratą informacji niejawnych.

TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROŻEŃ

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)		
1	2	3	4	5	6	7
1.	**Klauzula tajności przetwarzanych informacji niejawnych**			**1**	*W jednostce przetwarzane są jedynie informacje o klauzuli „zastrzeżone”.*	Analizie podlegają wszystkie klauzule tajności wszystkich przetwarzanych informacji niejawnych. Przy ocenie istotności czynnika stosuje się zasadę: im wyższe klauzule tajności przetwarzanych informacji tym czynnik ma istotniejsze znaczenie. Dla informacji niejawnych o klauzuli „ściśle tajne” wartość oceny jest stała i wynosi 8 pkt (czynnik ma „bardzo istotne” znaczenie). W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
2.	**Liczba materiałów niejawnych**			**1**	*W jednostce przetwarza się stosunkowo małą liczbę dokumentów zawierających informacje niejawne. Przetwarzane informacje dotyczą głównie spraw zarządzania kryzysowego, spraw obronnych i wojskowych.*	Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urządzeniach ewidencyjnych, pozostające w faktycznej dyspozycji jednostki organizacyjnej. W uzasadnieniu należy odnieść się do przybliżonej, ogólnej liczby wszystkich materiałów, stosując zasadę: im więcej informacji niejawnych o najwyższych klauzulach tajności tym czynnik ma istotniejsze znaczenie. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

3.	**Postać informacji niejawnych**		**4**		*W jednostce przetwarzane są informacje niejawne w postaci papierowej oraz na elektronicznych nośnikach informacji. Informacje przetwarzane są w akredytowanym przez Wójta Gminy systemie teleinformatycznym.*	Przy ocenie należy brać pod uwagę ogólną liczbę przetwarzanych informacji niejawnych, stosując zasadę, że im więcej informacji przetwarzanych w systemach teleinformatycznych (w stosunku do ogólnej liczby materiałów) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
4.	**Liczba osób**			**1**	*Mała liczba pracowników upoważnionych do dostępu do informacji niejawnych w stosunku do wszystkich zatrudnionych.*	Przy ocenie istotności tego czynnika należy uwzględnić pracowników jednostki organizacyjnej mających lub mogących mieć dostęp do informacji niejawnych, tj. osoby zajmujące stanowiska, wykonujące zadania lub prace zlecone związane z dostępem do takich informacji, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych. Im więcej osób (w stosunku do liczby zatrudnionych) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
5.	**Lokalizacja**		**4**		*Budynek USC, w którym przetwarzane są informacje niejawne mieści się w wolnostojącym, dwukondygnacyjnym, ogrodzonym budynku. W budynku znajdują się inne jednostki organizacyjne i instytucje. USC ma oddzielne wejście, nie jest połączone z pozostałymi podmiotami.*	Na wzrost oceny istotności tego czynnika ma wpływ np. to, że budynek użytkowany jest wspólnie z innymi podmiotami lub budynek jest w zabudowie zwartej (np. budynek, którego ściany przylegają do innego budynku). Na wzrost oceny istotności czynnika ma wpływ także najbliższe sąsiedztwo np.: obiekty przedstawicielstw i podmiotów zagranicznych, hotele, obiekty sportowe i hale widowiskowe, ogólnodostępne parkingi, garaże, zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia lub zdrowia.

6.	**Dostęp osób do budynku**		**4**		*W nocy budynek jest zamknięty i zabezpieczony systemem alarmowym. W godzinach urzędowania powszechnie dostępny.*	Na wzrost oceny istotności tego czynnika ma wpływ możliwość swobodnego poruszania się po budynku osób nie będących pracownikami jednostki organizacyjnej, np. goście, interesanci (w obiektach użyteczności publicznej).
7.	**Zagrożenia kradzieżą, włamaniem i napadem**			**1**	*Solidna konstrukcja ścian, zabezpieczenia drzwi, system alarmowy połączony z Policją.*	Poziom zagrożeń powinien uwzględniać inne czynniki wynikające ze specyfiki jednostki organizacyjnej, nie wykazane powyżej, a mogące mieć wpływ na ochronę informacji niejawnych np.: działanie obcych służb specjalnych**,** sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działanie sił przyrody (np. obszar zagrożony powodzią) lub szkody górnicze.
Suma punktów		**16**				

TABELA DO OKREŚLANIA POZIOMU ZAGROŻEŃ

POZIOM ZAGROŻEŃ		
NISKI	ŚREDNI	WYSOKI
7 pkt - 16 pkt	17 pkt - 32 pkt	powyżej 32 pkt

Po analizie wyżej wymienionych czynników możemy określić poziom zagrożenia dla systemu ochrony informacji niejawnych w Urzędzie Gminy Gródek jako **NISKI.**

II. Dobór środków bezpieczeństwa fizycznego

II.1. Podstawowe wymagania bezpieczeństwa fizycznego dla informacji niejawnych o klauzuli „ZASTRZEŻONE”

	Poziom zagrożeń
	NISKI
ZASTRZEŻONE	
Obowiązkowo: kategorie K1+K2+K3	**2**
Dodatkowo: kategoria K4, K5 lub K6	**-**
Łącznie suma punktów:	**2**

II.2. Środki bezpieczeństwa zastosowane w Urzędzie Gminy Gródek dla ochrony informacji niejawnych o klauzuli „ZASTRZEŻONE”

Kategorie obowiązkowe *- K1+K2+K3:*

- ✓ **K1S1 – konstrukcja szafy** – zastosowano metalową szafę zamykaną na klucz – **1 pkt.**
- ✓ **K1S2 – zamek do szafy** – zamek zastosowany w szafie charakteryzuje się umiarkowaną odpornością na włamanie - **1 pkt.**
- ✓ **K2S1 – konstrukcja pomieszczenia** – pomieszczenie znajduje się wewnątrz budynku, bez okien, o solidnych ścianach, zamykane na kratę z kłódką oraz na drzwi obite blachą. Konstrukcja pomieszczenia Kancelarii Materiałów Niejawnych zapewnia odporność na włamanie ocenioną na - **2 pkt.**
- ✓ **K2S2 – zamek do drzwi pomieszczenia** – trzy zamki zastosowane w drzwiach (dwa standardowe typu Yale i zasuwa) charakteryzują się umiarkowanym stopniem odporności na fachowe działania osoby nieuprawnionej posługującej się wyjątkowymi umiejętnościami i narzędziami - **1 pkt.**
- ✓ **K3 – budynki** - budynek o solidnej konstrukcji, ściany zewnętrzne z cegły o grubości 40 cm + 14 cm docieplenie, okna zabezpieczone kratą, podłoga i strop – konstrukcja żelbetowa – **3 pkt.**

Kategorie dodatkowe - *K4, K5 lub K6:*

- ✓ **K4S1 - systemy kontroli dostępu** – zastosowano system kontroli dostępu oparty na zamkniętych drzwiach z trzema zamkami **– 1pkt.**
- ✓ **K4S2 – kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów) –** do strefy kontrolowanego dostępu mogą wejść bez eskorty jedynie osoby posiadające poświadczenie bezpieczeństwa bądź upoważnienie Wójta do dostępu do informacji niejawnych o klauzuli „zastrzeżone" – **3 pkt.**
- ✓ **K5S1 – personel bezpieczeństwa** – teren budynku w porze wieczornej oraz w weekendy jest sporadycznie odwiedzany i kontrolowany przez Wójta Gminy, pracowników Urzędu Gminy bądź jednostek podległych **– 1pkt.**
- ✓ **K5S2 - systemy sygnalizacji napadu i włamania** – budynek zabezpiecza system alarmowy, włączany po godzinach pracy, z chwilą opuszczenia budynku **– 1pkt.**
- ✓ **K6S1 – ogrodzenie** – teren wokół budynku ogrodzony metalowym ogrodzeniem o wysokości ok. 1,6 m. **– 1pkt.**

II.3. Punktacja zastosowanych środków bezpieczeństwa fizycznego dla informacji niejawnych o klauzuli „ZASTRZEŻONE"

ŚRODEK BEZPIECZEŃSTWA	PKT
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	**1**
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	2
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	**2**

KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3 = 5, 3, 2 lub 1 pkt)	**3**
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	3
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	**4**
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	**2**
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	0
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	**1**
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY=K1+K2+K3+K4+K5+K6	**13**

III. Podsumowanie

Zgodnie z rozporządzeniem Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012, poz. 683), proces doboru środków bezpieczeństwa fizycznego powinien zapewniać elastyczność ich stosowania w zależności od określonego poziomu zagrożeń. W wyniku przeprowadzonej analizy, w celu określenia poziomu zagrożeń, zastosowano odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

- *personel bezpieczeństwa* – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;
- *bariery fizyczne* – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;
- *szafy i zamki* – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
- *system kontroli dostępu* – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;
- *system sygnalizacji napadu i włamania* – elektroniczny system pomocniczy (alarm) stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa.

Na podstawie „Tabeli oceny istotności czynników zagrożeń”, określono poziom zagrożeń w Urzędzie Gminy Gródek jako niski. Minimalna liczba punktów do osiągnięcia dla niskiego poziomu zagrożeń i klauzuli informacji niejawnych „zastrzeżone”, zgodnie z wyżej powołanym rozporządzeniem, wynosi 2 pkt.

W wyniku przeprowadzonej analizy można stwierdzić, iż podstawowe wymagania bezpieczeństwa fizycznego w Urzędzie Gminy Gródek zostały spełnione. Wymagana liczba punktów (2 pkt.) została nie tylko osiągnięta, ale nawet zrealizowana z dużą nadwyżka (13 pkt.).

Powyższe stanowi, iż obecnie zastosowane w Urzędzie Gminy Gródek środki bezpieczeństwa i ochrony, w całości odpowiadają wymaganiom określonym w wyżej powołanym rozporządzeniu.