WÓJT GMINY
Zbójno
woj.kujawsko-pomorskie

ZARZĄDZENIE NR 36/2018
WÓJTA GMINY ZBÓJNO

z dnia 28 maja 2018 r.

w sprawie ustalenia procedury szacowania ryzyka w Urzędzie Gminy Zbójno

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2017 r. poz. 1875), w związku z motywem 78 i 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE. z dnia 4 maja 2016 r.), zarządzam co następuje:

§1. Ustalam procedurę szacowania ryzyka w Urzędzie Gminy Zbójno stanowiącą załącznik do niniejszego zarządzenia.

§2. Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od dnia 23 maja 2018 r.

WÓJT
mgr Katarzyna Kukielska

Załącznik do zarządzenia nr 36/2018 Wójta Gminy Zbójno z dnia 28 maja 2018 r. w sprawie ustalenia procedury szacowania ryzyka w Urzędzie Gminy Zbójno.

Procedura szacowania ryzyka w Urzędzie Gminy Zbójno

Słowniczek pojęć

Podmiot - Urząd Gminy Zbójno.

Aktywa - zasoby wykorzystywane przez organizację, związane z przetwarzaniem danych osobowych; aktywa można podzielić na:

a) **aktywa podstawowe:**
   — procesy (np. zbieranie danych potrzebnych do wykonania usługi),
   — działania biznesowe (np. zaprojektowanie nowej funkcjonalności na potrzeby klientów),
   — informacje (np. dane osobowe),

b) **aktywa wspierające:**
   — sprzęt (np. laptop),
   — oprogramowanie (np. aplikacja wykorzystywana do wykonywania usług),
   — sieć (np. wewnętrzna sieć administratora),
   — personel (np. wykwalifikowani pracownicy),
   — siedziba (np. budynki),
   — struktura organizacyjna (np. ustanowienie inspektora ochrony danych)

Dostępność - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne,

Integralność - zapewnienie dokładności i kompletności informacji oraz metod przetwarzania danych,

Poufność - zapewnienie, że informacja jest dostępna jedynie dla osób upoważnionych,

Podatność - „słaby punkt", właściwość danego aktywu, które mogą być wykorzystane przez zagrożenie (np. brak systematycznego aktualizowania jest podatnością oprogramowania, która może spowodować realne powstanie zagrożenia w postaci zainstalowania wirusa w komputerze),

Właściciel ryzyka - osoba (osoby) odpowiedzialna za dany aktyw i ryzyko z nim związane (np. kierownik działu),

Zabezpieczenie - środek, który modyfikuje ryzyko naruszenia bezpieczeństwa (np. szyfrowanie, kontrola dostępu, czujniki dymu, szafy ogniotrwałe).

Zagrożenie - potencjalne zdarzenie, które może wywołać szkodę.

OPIS POSTĘPOWANIA

I. SZACOWANIE RYZYKA

1) Identyfikowanie potencjalnych zagrożeń i podatności.

Ocena ryzyka przeprowadzana jest dla każdej operacji przetwarzania danych osobowych, rozpatruje trzy obszary:

1) prawdopodobieństwo wystąpienia zagrożenia;
2) podatność aktywów na zagrożenia;
3) skutki potencjalnych zagrożeń,

biorąc pod uwagę następstwa naruszenia lub utraty:

1) poufności;
2) integralności;
3) dostępności,

które mogą nastąpić w wyniku działań:

1) umyślnych - (U);
2) przypadkowych – (P);
3) naturalnych - (N).

Przyjmuje się, że zagrożenia (U,P) są wynikiem działań ludzkich, natomiast źródła zagrożeń (N) są niezależne od człowieka.

Listę potencjalnych zagrożeń dla podmiotu umieszczono w **Tabeli nr 1**. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa, podatności oraz skutków zdarzeń.

Należy uwzględnić, że podatność, nie powoduje jeszcze szkody, ale należy zgodnie z Tabelą nr 2 oszacować stopień zabezpieczenia aktywa pod kątem zidentyfikowanych zagrożeń.

Identyfikacja zagrożeń.

Tabela nr 1.

Lp.	Rodzaj	Zagrożenie	Źródło
1.	**Zniszczenia fizyczne**	Pożar, zalanie , zanieczyszczenie, poważny wypadek, zniszczenie urządzeń lub nośników, pył, korozja, wychłodzenie.	P,U,N
2.	**Zjawiska naturalne**	Zjawiska klimatyczne, zjawiska pogodowe, powódź.	N
3.	**Naruszenie bezpieczeństwa informacji**	Podsłuch, kradzież nośników lub dokumentów, kradzież urządzenia, szpiegostwo, kopiowanie danych, odtworzenie wyrzuconych nośników.	U
		Ujawnienie informacji, dane z niewiarygodnych źródeł, sfałszowanie oprogramowania, brak spełnienia wymagań prawnych dotyczących archiwizowania dokumentacji.	P,U
4.	**Awarie techniczne**	Awaria urządzenia, niewłaściwe funkcjonowanie urządzenia, niewłaściwe funkcjonowanie oprogramowania.	P
		Umyślne uszkodzenie urządzenia lub oprogramowania.	U
5.	**Utrata usług**	Awaria systemu klimatyzacji, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego.	P,U,N
6.	**Zakłócenia spowodowane promieniowaniem**	Promieniowanie elektromagnetyczne, promieniowanie cieplne, impuls elektromagnetyczny.	P,U,N
7.	**Nieautoryzowanie działania**	Niewłaściwe funkcjonowanie urządzeń, niewłaściwe funkcjonowanie oprogramowania.	P
		Przeciążenie systemu informacyjnego, naruszenie	P,U

		zdolności utrzymania systemu informacyjnego.	
8.	**Naruszenie bezpieczeństwa funkcji**	Błąd użytkowania.	P
		Naruszenie praw.	P,U
		Fałszowanie praw, odmowa działania.	U
		Naruszenie dostępności personelu.	P,U,N

Identyfikacja występujących podatności.

Tabela nr 2.

Rodzaj	Podatności	Zagrożenia
Sprzęt	Niezabezpieczone urządzenie do przechowywania danych.	Kradzież danych lub dokumentów.
	Brak staranności przy pozbywaniu się nośników.	Kradzież nośników lub danych.
	Niekontrolowane kopiowanie.	Kradzież danych.
	Wrażliwość na wilgoć, pył, zanieczyszczenie.	Pył, korozja, wychłodzenie.
	Wrażliwość na zmiany temperatury.	Zjawiska pogodowe.
	Wrażliwość na zmiany napięcia zasilania.	Utrata zasilania.
	Brak planów okresowej wymiany sprzętu.	Zniszczenie lub awaria urządzenia lub nośników.
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej.	Nadużycie praw.
	Błędne przypisanie praw dostępu.	Nadużycie praw.
	Brak mechanizmów identyfikacji i uwierzytelnienia użytkownika.	Fałszowanie praw.
	Złe zarządzanie hasłami.	Fałszowanie praw.
	Brak fizycznej kontroli budynków, drzwi i okien.	Kradzież nośników lub danych.
	Brak skutecznej kontroli zmian.	Zakłócenie procesu.
Sieć	Niezabezpieczone linie telefoniczne.	Podsłuch.
	Złe łączenie kabli.	Awaria urządzenia telekomunikacyjnego.
	Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy.	Fałszowanie praw.

	Niezabezpieczone połączenie z siecią publiczną.	Nieautoryzowane użycie urządzeń.
	Uszkodzenie fizyczne sieci lub kabli.	Zatrzymanie procesu.
Personel	Nieobecność personelu.	Naruszenie danych, brak dostępności.
	Niewystarczające szkolenie z bezpieczeństwa, użycia oprogramowania lub sprzętu.	Błąd użytkowania.
	Brak mechanizmów monitorowania.	Nielegalnie przetwarzanie danych.
	Praca personelu zewnętrznego lub sprzątającego bez nadzoru.	Nieautoryzowane użycie urządzeń.
Siedziba	Lokalizacja na obszarach zagrożonych powodzią.	Powódź.
	Brak fizycznej ochrony budynków, drzwi i okien.	Kradzież, zniszczenie.
Organizacja	Brak procedur regulujących bezpieczeństwo aktywów.	Utrata danych, niezgodność z przepisami prawa, nieautoryzowany dostęp.
	Brak regularnego nadzoru	Nadużycie praw.
	Brak zdefiniowanego postępowania dyscyplinarnego.	Kradzież urządzenia.

2) Szacowanie poziomu ryzyka.

Metodyka oceny ryzyka, została ustanowiona w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w podmiocie oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka. Za dane wejściowe do procesu oceny uważa się wszelkie informacje przedstawione w analizie ryzyka (dane z inwentaryzacji), a w szczególności miejsce, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywa. Ponadto każde szacowanie prawdopodobieństwa, podatności oraz skutków zdarzenia powinno się odbywać w relacji z Tabelą nr 1 i 2 niniejszej procedury według zadanych kryteriów:

Szacowanie prawdopodobieństwa

Tabela nr. 3

Badane kryterium	Ryzyko	Kategoria ryzyka	Wartość
(PO)	Niskie, odległe, mało realne szanse na	małe	1

Prawdopodobieństwo *(możliwość wystąpienia)*	zdarzenie.		
	Może się zdarzyć lub zdarza się sporadycznie.	średnie	2
	Bardzo realne szanse wystąpienia.	duże	3

Szacowanie podatności

Tabela nr. 4

Badane kryterium	Ryzyko	Kategoria ryzyka	Wartość
(PR) Podatność *(słabość aktywa)*	Aktywa bardzo dobrze zabezpieczone.	mała	1
	Aktywa dostatecznie zabezpieczone.	średnia	2
	Aktywa słabo lub nie zabezpieczone.	duża	3

Szacowanie skutków

Tabela nr. 4

Badane kryterium	Ryzyko	Kategoria ryzyka	Wartość
(S) Skutek *(wpływ na organizację i/lub proces)*	Utrata danych nie spowoduje utrudnień w pracy przedsiębiorstwa lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu.	mały	1
	Utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku przedsiębiorstwa , odtworzenie danych jest możliwe ale pracochłonne.	średni	2
	Utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne, odtworzenie danych i reputacji będzie trudne i kosztowne.	duży	3

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:

R = PR · PO · S

gdzie:

PR - Prawdopodobieństwo

PO - Podatność

S - Skutek

Wynik z działania zgodnie z poniższą tabelą należy przypisać ustanowionym kategoriom ryzyka, a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego. W uzasadnionych przypadkach można zaakceptować ryzyko kategorii drugiej lub trzeciej, szczególnie gdy działania profilaktyczne odnoszą się do długoterminowych i kosztownych inwestycji na rzecz bezpieczeństwa danego aktywa.

Wytyczne do postępowania z ryzykiem

Tabela nr. 5

Lp.	Wartość ryzyka	Kategoria (poziom) ryzyka	Akceptacja ryzyka Tak / Nie	Działania zapobiegawcze (postępowanie z ryzykiem)	Właściciel ryzyka
1.	1÷ 7	Mały	TAK	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące.	Dział (wydział, samodzielne stanowisko pracy lub inna wewnętrzna komórka organizacyjna).
2.	8 ÷ 17	Średni	NIE	Należy zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne.	Dział (wydział, samodzielne stanowisko pracy lub inna wewnętrzna komórka organizacyjna).
3.	18 ÷ 27	Duży	NIE	Należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc aktywa w bezpieczniejsze miejsce.	Dział (wydział, samodzielne stanowisko pracy lub inna wewnętrzna komórka organizacyjna)

Szacowanie ryzyka oraz postępowanie z ryzykiem (Tabela nr 6), stanowi załącznik do niniejszej procedury.

3) Działania doskonalące bezpieczeństwo informacji.

Procesy doskonalące bezpieczeństwo informacji prowadzone są w oparciu o podjęte działania zapobiegawcze i/lub korygujące adekwatnie do wagi potencjalnych problemów. W tym celu uruchamia się plan postępowania z ryzykiem.

W wyniku tych działań należy według powyższych zasad powtórnie dokonać szacowania ryzyka w celu sprawdzenia skuteczności i odporności systemu na przypadek zaistnienia zadanych w pierwszej fazie oceny zagrożeń naruszających poufność, dostępność i/lub integralność.

Wynik z powtórnego szacowania ryzyka stanowi o ryzyku szczątkowym, które jest pozostałością po podjęciu wszystkich możliwych kroków zmierzających do unikania ryzyka, jego kontrolowania lub przeniesienia (transferu).

4) Plan postępowania z ryzykiem.

Dla aktywów gdzie ryzyko było nieakceptowalne, formułuje się plan postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu bezpiecznego – akceptowalnego. W tym celu kierownictwo podmiotu wdraża adekwatne do wynikającego ryzyka zabezpieczenia oraz mierzy ich skuteczność.

Ostatecznie zatwierdzone i wdrożone zabezpieczenia należy wpisać w dokument szacowania poziomu ryzyka w kolumnie działań zapobiegawczych i/lub korygujących w celu poddania aktywa ponownej ocenie ryzyka.

5) Wprowadzanie zmian.

Dokonywanie zmian w ocenie ryzyka odbywa się w wyniku każdorazowego podjęcia działań korygujących i/lub zapobiegawczych, zidentyfikowania nowego - realnego zagrożenia oraz dokonanego incydentu naruszającego bezpieczeństwo informacji.

Zapisy sporządzone w ocenie ryzyka nie ulegają przedawnieniu i są trwałe, w związku z czym każde działanie mające na celu ponowną ocenę ryzyka bezwzględnie dokonuje się w kolejnym cyklu analizy.

Szacowanie poziomu ryzyka należy przeprowadzać co najmniej raz w roku.

Załącznik do procedury szacowania ryzyka w Urzędzie Gminy Zbójno ustalonej zarządzeniem nr 36/2018 Wójta Gminy Zbójno z dnia 28 maja 2018 r. w sprawie ustalenia procedury szacowania ryzyka w Urzędzie Gminy Zbójno

Szacowanie ryzyka oraz postępowanie z ryzykiem

Tabela nr 6.

Szacowanie poziomu ryzyka oraz postępowanie z ryzykiem										
Lp.	**Operacja przetwarzania danych**	**Zagrożenie**	**Prawdopodobieństwo**	**Podatność**	**Skutek - koszt**	**Wartość ryzyka**	**Kategoria (poziom) ryzyka**	**Akceptacja ryzyka**	**Działania zapobiegawcze (postępowanie z ryzykiem)**	**Właściciele ryzyka**