ZARZĄDZENIE NR 73.2025

Wójta Gminy Raciąż

z dnia 4 czerwca 2025 r.

w sprawie wprowadzenia „Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Raciąż"

Na podstawie: art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. 2024, poz. 1465 ze zm.), art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2024 r. poz. 1557 ze zm.), ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024, poz. 1077 ze zm.) oraz § 19 ust. 1-3 rozporządzenia Rady Ministrów z dnia 21 maja 2014 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. 2024, poz. 773 ze zm.), z uwzględnieniem wymagań normy PN-EN ISO/IEC 27 001:2023, zarządzam, co następuje:

§ 1. Podstawowe zasady

1. Wprowadza się w Urzędzie Gminy Raciąż System Zarządzania Bezpieczeństwem Informacji, zwany dalej "SZBI".
2. SZBI stanowi zbiór procedur i zasad określających sposób postępowania przy przetwarzaniu informacji w Urzędzie Gminy Raciąż w celu zapewnienia ich bezpieczeństwa.
3. SZBI obejmuje swoim zakresem wszystkie informacje przetwarzane w Urzędzie Gminy Raciąż, niezależnie od formy ich przechowywania i przetwarzania.

§ 2. Cel i zakres SZBI

1. Celem SZBI jest zapewnienie poufności, integralności, dostępności i autentyczności informacji przetwarzanych w Urzędzie Gminy Raciąż oraz zapewnienie ciągłości działania jednostki.
2. SZBI obejmuje wszystkie procesy związane z przetwarzaniem informacji w Urzędzie Gminy Raciąż oraz stosowane w tym zakresie rozwiązania organizacyjne i techniczne.
3. SZBI ma na celu minimalizację zagrożeń wynikających z działalności człowieka, przypadkowych zdarzeń oraz zapewnienie bezpieczeństwa przetwarzanych danych.
4. Zarządzenie stosuje się do wszystkich pracowników Urzędu Gminy Raciąż, stażystów, praktykantów oraz osób wykonujących zadania na rzecz Urzędu na podstawie umów

cywilnoprawnych, a także innych osób mających dostęp do informacji przetwarzanych w Urzędzie.

§ 3. Definicje

Ilekroć w zarządzeniu jest mowa o:

1. SZBI – należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji wdrożony w Urzędzie Gminy Raciąż;
2. Bezpieczeństwie informacji – należy przez to rozumieć zachowanie poufności, integralności, dostępności i autentyczności informacji;
3. Poufności – należy przez to rozumieć właściwość zapewniającą, że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom lub procesom;
4. Integralności – należy przez to rozumieć właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w nieautoryzowany sposób;
5. Dostępności – należy przez to rozumieć właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
6. Autentyczności – należy przez to rozumieć właściwość polegającą na tym, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
7. Danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, zgodnie z definicją zawartą w art. 4 pkt 1 RODO;
8. Incydencie bezpieczeństwa – należy przez to rozumieć pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;
9. Ryzyku – należy przez to rozumieć kombinację prawdopodobieństwa wystąpienia zdarzenia oraz jego konsekwencji.

§ 4. Składniki Systemu Zarządzania Bezpieczeństwem Informacji

1. W skład SZBI wchodzą następujące dokumenty:

a) Polityka Bezpieczeństwa Informacji – stanowiąca **Załącznik nr 1** do niniejszego zarządzenia, zawierająca deklarację zasad bezpieczeństwa informacji;

b) Polityka Ochrony Danych Osobowych – stanowiąca **Załącznik nr 2** do niniejszego zarządzenia, uwzględniająca zasady ochrony danych w fazie projektowania i domyślnej ochrony danych;

c) Polityka Bezpieczeństwa Organizacyjnego – stanowiąca **Załącznik nr 3** do niniejszego zarządzenia, określająca zasady organizacji bezpieczeństwa;

d) Polityka Bezpieczeństwa Osobowego – stanowiąca **Załącznik nr 4** do niniejszego zarządzenia, określająca zasady dotyczące pracowników i osób upoważnionych;

e) Polityka Bezpieczeństwa Fizycznego – stanowiąca **Załącznik nr 5** do niniejszego zarządzenia, określająca zasady ochrony fizycznej zasobów i pomieszczeń;

f) Polityka Bezpieczeństwa Technologicznego – stanowiąca **Załącznik nr 6** do niniejszego zarządzenia, określająca zabezpieczenia techniczne i teleinformatyczne;

g) Instrukcja Zarządzania Systemem Informatycznym – stanowiąca **Załącznik nr 7** do zarządzenia;

h) Polityka Szacowania Ryzyka i Oceny Skutków dla Ochrony Danych (DPIA) – stanowiąca **Załącznik nr 8** do zarządzenia;

i) Procedura Zarządzania Incydentami Bezpieczeństwa – stanowiąca **Załącznik nr 9** do zarządzenia;

j) Plan Ciągłości Działania – stanowiący **Załącznik nr 10** do zarządzenia;

k) Rejestr Ryzyk – stanowiący **Załącznik nr** 11 do zarządzenia;

l) Polityka Kontroli Dostępu – stanowiąca **Załącznik nr 12** do zarządzenia;

m) Polityka Zarządzania Aktywami – stanowiąca **Załącznik nr 13** do zarządzenia;

n) Polityka Bezpieczeństwa Komunikacji – stanowiąca **Załącznik nr 14** do zarządzenia;

o) Polityka Relacji z Dostawcami – stanowiąca **Załącznik nr 15** do zarządzenia.

2. Dokumenty wymienione w ust. 1 stanowią integralną część niniejszego zarządzenia.

§ 5. Obowiązki i odpowiedzialności

1. **Wójt Gminy Raciąż**:
    a) ponosi ostateczną odpowiedzialność za bezpieczeństwo informacji w Urzędzie Gminy Raciąż;
    b) zatwierdza dokumentację SZBI;
    c) zapewnia zasoby niezbędne do wdrożenia i utrzymania SZBI;
    d) wyznacza Pełnomocnika ds. Bezpieczeństwa Informacji.
2. **Pełnomocnik ds. Bezpieczeństwa Informacji**:
    a) nadzoruje i koordynuje funkcjonowanie SZBI;
    b) opracowuje i aktualizuje dokumentację SZBI;
    c) przeprowadza analizę ryzyka w zakresie bezpieczeństwa informacji;
    d) monitoruje zgodność SZBI z przepisami prawa i wymaganiami wewnętrznymi;

e) organizuje szkolenia z zakresu bezpieczeństwa informacji;

f) raportuje do Wójta Gminy Raciąż o stanie bezpieczeństwa informacji i incydentach.

3. **Sekretarz Gminy**:

a) wspiera Wójta w zarządzaniu SZBI;

b) nadzoruje wdrażanie i przestrzeganie procedur bezpieczeństwa informacji;

c) zapewnia uwzględnienie wymagań bezpieczeństwa informacji w procesach organizacyjnych Urzędu.

4. **Administrator Systemów Informatycznych**:

a) administruje systemami informatycznymi Urzędu;

b) wdraża zabezpieczenia techniczne zgodnie z wymaganiami SZBI;

c) monitoruje stan bezpieczeństwa infrastruktury informatycznej;

d) reaguje na incydenty bezpieczeństwa w systemach informatycznych;

e) prowadzi dokumentację techniczną systemów informatycznych.

5. **Kierownicy referatów**:

a) nadzorują przestrzeganie zasad SZBI przez podległych pracowników;

b) identyfikują zasoby informacyjne w swoich jednostkach organizacyjnych;

c) zgłaszają potrzeby w zakresie bezpieczeństwa informacji;

d) uczestniczą w procesie analizy ryzyka.

6. **Pracownicy Urzędu**:

a) przestrzegają zasad i procedur SZBI;

b) uczestniczą w szkoleniach z zakresu bezpieczeństwa informacji;

c) zgłaszają incydenty bezpieczeństwa;

d) odpowiadają za bezpieczeństwo informacji w zakresie swoich obowiązków służbowych.

§ 6. Zakres ochrony informacji

1. Ochronie w ramach SZBI podlegają wszystkie informacje przetwarzane w Urzędzie Gminy Raciąż, w tym w szczególności:

a) dane osobowe;

b) informacje niejawne;

c) informacje publiczne;

d) dane podatkowe;

e) dane pracownicze;

f) dane wrażliwe dotyczące mieszkańców gminy;

g) dane dotyczące nieruchomości i infrastruktury;

h) dane finansowe i budżetowe.

2. Zapewnienie poufności informacji polega na:

a) ograniczeniu dostępu do informacji wyłącznie dla osób upoważnionych;

b) stosowaniu mechanizmów uwierzytelniania i autoryzacji;

c) ochronie informacji przed nieuprawnionym ujawnieniem;

d) stosowaniu zasady minimalnych uprawnień.

3. Zapewnienie integralności informacji polega na:

a) ochronie informacji przed nieautoryzowanymi zmianami;

b) stosowaniu mechanizmów kontroli zmian;

c) weryfikacji poprawności wprowadzanych danych;

d) regularnym tworzeniu kopii zapasowych.

4. Zapewnienie dostępności informacji polega na:

a) zapewnieniu ciągłości działania systemów informatycznych;

b) odpowiednim zabezpieczeniu infrastruktury technicznej;

c) zapewnieniu mechanizmów odtwarzania danych;

d) stosowaniu redundantnych rozwiązań dla krytycznych systemów.

§ 7. Zarządzanie ryzykiem

1. W Urzędzie Gminy Raciąż prowadzi się regularną analizę ryzyka związanego z bezpieczeństwem informacji zgodnie z Polityką Szacowania Ryzyka, stanowiącą **Załącznik nr 8** do niniejszego zarządzenia.

2. Analiza ryzyka obejmuje:

a) identyfikację aktywów informacyjnych;

b) określenie zagrożeń i podatności;

c) oszacowanie prawdopodobieństwa wystąpienia zagrożeń;

d) ocenę potencjalnych skutków;

e) określenie poziomu ryzyka;

f) wskazanie sposobów postępowania z ryzykiem.

3. Analiza ryzyka przeprowadzana jest co najmniej raz w roku oraz w przypadku istotnych zmian w systemach informatycznych lub procesach przetwarzania informacji.

4. Na podstawie wyników analizy ryzyka opracowuje się i aktualizuje Plan postępowania z ryzykiem.

5. Dla procesów przetwarzania danych osobowych mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych przeprowadza się ocenę skutków dla ochrony danych (DPIA), zgodnie z art. 35 RODO.

§ 8. System zarządzania ciągłością działania

1. W ramach SZBI ustanawia się system zarządzania ciągłością działania, którego celem jest zapewnienie nieprzerwanej realizacji zadań Urzędu Gminy Raciąż w przypadku wystąpienia sytuacji kryzysowych.

2. System zarządzania ciągłością działania obejmuje:

a) identyfikację procesów krytycznych;

b) analizę wpływu potencjalnych zakłóceń na działalność Urzędu;

c) opracowanie planów ciągłości działania;

d) ustanowienie procedur odtwarzania po awarii;

e) określenie zasad testowania planów ciągłości działania.

3. Plan Ciągłości Działania, stanowiący **Załącznik nr 10** do zarządzenia, określa szczegółowe procedury postępowania w przypadku wystąpienia:

a) awarii systemów informatycznych;

b) klęsk żywiołowych;

c) aktów terroryzmu;

d) epidemii;

e) innych zdarzeń mogących zakłócić funkcjonowanie Urzędu.

4. Plan Ciągłości Działania podlega regularnemu przeglądowi i testowaniu nie rzadziej niż raz w roku.

§ 9. Postępowanie w przypadku naruszenia bezpieczeństwa informacji

1. Każda osoba, która stwierdzi lub podejrzewa naruszenie bezpieczeństwa informacji, zobowiązana jest do niezwłocznego zgłoszenia tego faktu Pełnomocnikowi ds. Bezpieczeństwa Informacji lub Administratorowi Systemów Informatycznych.

2. Zasady postępowania w przypadku naruszenia bezpieczeństwa informacji określa Procedura Zarządzania Incydentami Bezpieczeństwa, stanowiąca **Załącznik nr 9** do zarządzenia.

3. W przypadku naruszenia ochrony danych osobowych Pełnomocnik ds. Bezpieczeństwa Informacji ocenia, czy zaistniały incydent stanowi naruszenie wymagające zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z art. 33 RODO.

4. Pełnomocnik ds. Bezpieczeństwa Informacji prowadzi rejestr incydentów bezpieczeństwa.

§ 10. Kontrola i doskonalenie SZBI

1. SZBI podlega regularnej kontroli i doskonaleniu w celu zapewnienia jego skuteczności i adekwatności.

2. **Wójt Gminy Raciąż zapewnia przeprowadzanie co najmniej raz w roku audytu wewnętrznego w zakresie bezpieczeństwa informacji.**

3. Pełnomocnik ds. Bezpieczeństwa Informacji przeprowadza **co najmniej raz w roku** przegląd SZBI obejmujący weryfikację:

   a) zgodności SZBI z przepisami prawa;

   b) adekwatności zabezpieczeń w stosunku do zidentyfikowanych ryzyk;

   c) skuteczności wdrożonych zabezpieczeń;

   d) potrzeby wprowadzenia zmian w SZBI.

4. Wyniki przeglądu SZBI są dokumentowane i przedstawiane Wójtowi Gminy Raciąż.

5. Na podstawie wyników przeglądu i audytu opracowuje się działania korygujące i zapobiegawcze.

§ 11. Szkolenia

1. Każdy nowy pracownik Urzędu Gminy Raciąż przed uzyskaniem dostępu do systemów informatycznych przechodzi szkolenie z zakresu bezpieczeństwa informacji.

2. Wszyscy pracownicy Urzędu uczestniczą w szkoleniach okresowych z zakresu bezpieczeństwa informacji co najmniej raz w roku.

3. Pełnomocnik ds. Bezpieczeństwa Informacji opracowuje roczny plan szkoleń z zakresu bezpieczeństwa informacji.

4. Szkolenia obejmują w szczególności:

   a) przepisy prawa dotyczące ochrony informacji;

   b) zasady i procedury SZBI;

c) zagrożenia bezpieczeństwa informacji;

d) środki ochrony informacji;

e) postępowanie w przypadku incydentów bezpieczeństwa.

§ 12. Postanowienia końcowe

1. Zobowiązuje się wszystkich pracowników Urzędu Gminy Raciąż do zapoznania się z niniejszym zarządzeniem i przestrzegania zawartych w nim zasad.
2. Nieprzestrzeganie zasad określonych w niniejszym zarządzeniu może stanowić naruszenie obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.
3. Pełnomocnik ds. Bezpieczeństwa Informacji, we współpracy z Sekretarzem Gminy, opracuje harmonogram wdrożenia SZBI w terminie 30 dni od dnia wejścia w życie zarządzenia.
4. Załączniki do zarządzenia nie podlegają publikacji w Biuletynie Informacji Publicznej ze względu na bezpieczeństwo informacji i poufność danych.
5. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Raciąż

mgr Zbigniew Sadowski