ZARZĄDZENIE NR ORG.120.31.2025

Wójta Gminy Baboszewo

z dnia 12 listopada 2025 r.

w sprawie powołania Pełnomocnika Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Baboszewo.

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r., poz. 1153 t. j.), w związku z § 19 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r., poz. 773) zarządza się, co następuje:

§ 1

Powołuje się na Pełnomocnika Systemu Zarządzania Bepieczeństwem Informacji w Urzędzie Gminy Baboszewo Panią Kingę Mak – Pracownika Urzędu Gminy Baboszewo.

§ 2

Do obowiązków Pełnomocnika SZBI należy w szczególności:

1) Budowa Systemu,
2) Utrzymanie Systemu,
3) Doskonalenie Systemu,
4) Koordynowanie audytów wewnętrznych,
5) Nadzorowanie przestrzegania przez pracowników postanowień normy oraz utworzonych w przyszłości dokumentów systemowych,
6) Przekazywanie do Kierownictwa Urzędu informacji o postępach we wdrożeniu oraz późniejszym utrzymaniu Systemu.

§ 3

Szczegółowy wykaz zadań Pełnomocnika stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 4

Wykonanie Zarządzenia powierza się Sekretarzowi Gminy Baboszewo.

§ 5

Traci moc Zarządzenie NR ORG.120.28.2025 r. Wójta Gminy Baboszewo z dnia 31 października 2025 r.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr inż. Bogdan Janusz Pietruszewski

Załącznik
Nr 2 do Zarządzenia Nr ORG.120.31.2025
Wójta Gminy Baboszewo
z dnia 12 listopada 2025 r.

Zakres czynności wykonywanych przez Pełnomocnika ds. SZBI

1. Opracowanie i wdrożenie i aktualizowanie SZBI

   1) tworzenie i aktualizacja polityki bezpieczeństwa informacji,
   2) definiowanie celów SZBI i nadzorowanie ich realizacji,
   3) rozstrzyganie sporów dotyczących stosowania i interpretacji wymagań zawartych w dokumentacji SZBI oraz wydawania wiążących decyzji w tym zakresie,
   4) identyfikacja kluczowych aktywów informacyjnych i wdrażanie odpowiednich zabepieczeń,
   5) integrację SZBI z innymi systemami zarządzania (np. ISO 9001, ISO 22301).

2. Zarządzanie ryzykiem w bezpieczeństwie informacji

   1) kierowanie pracami Zespołu ds. Bezpieczeństwa Informacji, w tym przedstawianie opracowanych dokumentów do zaopiniowania i nadzorowanie wdrażania zabezpieczeń,
   2) przeprowadzanie analizy ryzyka zgodnie z wymaganiami ISO,
   3) opracowanie Planu postępowania z ryzykiem i monitorowanie jego realizacji,
   4) zapewnienie skuteczności działań minimalizujących ryzyko.

3. Monitorowanie i audytowanie SZBI

   1) organizowanie audytów wewnętrznych SZBI w celu oceny zgodności z normą ISO 27001,
   2) czuwanie nad przestrzeganiem postanowień Polityki Zarządzania Bezpieczeństwem Informacji oraz dokumentów powiązanych,
   3) nadzór nad prawidłowością funkcjonowania i doskonalenia SZBI, w tym nadzór nad przestrzeganiem wymagań procedur, weryfikowanie wdrożonych rozwiązań i zabezpieczeń, inicjowanie i koordynowanie działań zmierzających do usunięcia niezgodności SZBI z wymaganiami normy PN ISO/IEC 27001,
   4) współpracę z audytorami zewnętrznymi podczas audytów,
   5) weryfikację dopuszczenia użytkowników do przetwarzania informacji,
   6) tworzenie raportów dla kierownictwa na temat stanu bezpieczeństwa informacji.

4. Zarządzanie incydentami bezpieczeństwa informacji

   1) wdrażanie procedur reagowania na incydenty bezpieczeństwa,

2) organizację zespołu do obsługi incydentów oraz analiza ich skutków.

5. Szkolenia i podnoszenie świadomości w zakresie bezpieczeństwa informacji

1) organizowanie i prowadzenie szkoleń pracowników organizacji w ramach Systemu Zarządzania Bezpieczeństwem Informacji, w tym na temat zasad postępowania zgodnych z założeniami Polityki Zarządzania Bezpieczeństwem Informacji – informacje mogą być przekazywane poprzez mailing, przekazywanie prezentacji, szkolenia oraz inne przyjęte standardy w Urzędzie,
2) promowanie zasad bezpiecznego przetwarzania informacji,
3) tworzenie procedur raportowania incydentów i zarządzania hasłami,
4) kształtowanie kultury bezpieczeństwa informacji w organizacji.

6. Współpraca z kierownictwem Urzędu i Kierownikami referatów

1) wsparcie kierownictwa organizacji i kierowników komórek organizacyjnych w podejmowaniu decyzji dotyczących bezpieczeństwa IT,
2) współpracę z kierownictwem Urzędu Gminy oraz z Kierownikami referatów bądź stanowiskami równorzędnymi na wszystkich etapach opracowania, wdrożenia i doskonalenia SZBI,
3) współpracę z działami IT, prawnymi, kadrami oraz Inspektorem Ochrony Danych,
4) uczestnictwo w projektach wdrażających nowe technologie i ocena ich wpływu na bezpieczeństwo informacji,
5) dostęp do wszystkich dokumentów, których treść może być istotna z punktu widzenia funkcjonowania SZBI,
6) uzyskanie wyjaśnień od pracowników Urzędu w zakresie działań realizowanych w ramach SZBI,
7) nadzorowanie prawidłowości prowadzonej w ramach SZBI inwentaryzacji i wyceny zasobów oraz inicjowanie i nadzorowanie wykonania analizy ryzyka przez poszczególne referaty,
8) współdziałanie z Administratorem Systemów Informatycznych w zakresie opracowywania lub modyfikacji dokumentów polityk bezpieczeństwa systemów przetwarzania informacji, procedur bezpieczeństwa i standardów zabezpieczeń, projektów rozwoju systemów teleinformatycznych,

7. Tworzenie i aktualizacja dokumentacji SZBI

1) wydawanie zaleceń pracownikom zatrudnionym w komórkach organizacyjnych Urzędu w zakresie związanym z wdrożeniem, utrzymaniem i doskonaleniem SZBI,
2) nadzór nad prowadzeniem rejestru zdarzeń i incydentów,

3) monitorowanie opracowania polityk, procedur i instrukcji dotyczących bezpieczeństwa informacji przez Właścicieli Aktywów i Właścicieli Procesów,
4) dokumentowanie wszystkich działań zgodnych z wymaganiami ISO 27001.

8. Zapewnienie zgodności z przepisami prawnymi i regulacjami

1) monitorowanie zmian w przepisach dotyczących ochrony informacji i cyberbezpieczeństwa,
2)wdrażanie wymagań RODO, KSC (Krajowego Systemu Cyberbezpieczeństwa), NIS2 w zakresie bezpieczeństwa informacji,
3) zapewnienie zgodności organizacji z obowiązującymi standardami i regulacjami branżowymi.

9. Nadzór nad bezpieczeństwem systemów IT

1) weryfikację skuteczności wdrożonych środków ochrony,
2) testowanie podatności i ocena ryzyka technologicznego,
3) współpracę z zespołami IT w zakresie cyberbezpieczeństwa,
4) współpracę z konsultantami i ekspertami zewnętrznymi oraz pracownikami kompetentnymi w zagadnieniach bezpieczeństwa.

10. Raportowanie do kierownictwa i rekomendowanie działań

1) przedstawianie Wójtowi sprawozdań dotyczących przebiegu prac oraz funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji, działania i wszelkich potrzeb związanych z jego doskonaleniem (zasoby ludzkie, finansowe, wiedzy i inne konieczne do wdrożenia i zachowania zaplanowanego poziomu bezpieczeństwa),
2) proponowanie działań usprawniających system zarządzania,
3) rekomendowanie inwestycji w nowe technologie zwiększające poziom bezpieczeństwa.

WÓJT
mgr inż. Bogdan Janusz Pietruszewski