Zarządzenie nr 25/2024
Wójta Gminy Regnów
z dnia 22 listopada 2024 roku

w sprawie wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Regnowie

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2024 r., poz.1465 i poz.1572) 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 systemów teleinformatycznych (Dz.U. z 2024r., poz.773) zarządza się, co następuje:

§1. Wprowadza się do stosowania w Urzędzie Gminy w Regnowie dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, zwanej dalej: dokumentacja SZBI, stanowiącą załącznik do niniejszego Zarządzenia.

§2. Dokumentacja SZBI ma zastosowanie do wszystkich stanowisk pracy w Urzędzie, stanowi wewnętrzną regulację i nie podlega publikacji, chyba, że co innego wynika z treści poszczególnych dokumentów.

§3. Funkcję Administratora Systemu Informatycznego (ASI), o której mowa w politykach i procedurach Systemu Zarządzania Bezpieczeństwem Informacji pełni Pan Artur Wąsiewicz, prowadzący obsługę informatyczną w Urzędzie Gminy w Regnowie.

§4. Zobowiązuję pracowników Urzędu Gminy w Regnowie do zapoznania się z dokumentacją SZBI oraz przestrzegania i realizowania określonych w niej postanowień.

§5. Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi Systemu Zarządzania Bezpieczeństwem Informacji.

§6. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Mariusz Cheba

WYKAZ OBOWIĄZUJĄCEJ DOKUMENTACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI
URZĄD GMINY W REGNOWIE

Stan na: 22.11.2024 r.

SYMBOL	NAZWA DOKUMENTU	PODSTAWA NORMATYWNA Z ISO/IEC 27001:2022	DATA OSTATNIEJ AKTUALIZACJI DOKUMENTU
SZBI - 0.WD	**Wykaz obowiązującej Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji**	Nie dotyczy	22.11.2024 r.
SZBI - O.WD – załącznik 1	**Lista osób zapoznanych z dokumentacją SZBI**	5.2 f)	22.11.2024 r.
SZBI - 1.KS	**Księga SZBI** (kontekst organizacji; potrzeby i oczekiwania stron; zakres sytemu; system; przywództwo i zaangażowanie; role, odpowiedzialność i uprawnienia; odpowiedzialność za zarządzanie; planowanie zmian, zasoby; kompetencje; świadomość; komunikacja)	4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.3, A.1.5.2, A.1.5.3, A.1.5.4, 6.3, 7.1, 7.2, 7.3, 7.4,	22.11.2024 r.
SZBI - 1.KS – załącznik 1	**Cele bezpieczeństwa informacji na określony rok**	6.2	22.11.2024 r.
SZBI - 2.PZD	**Procedura Zarządzania Dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji**	7.5.2,7.5.3	22.11.2024 r.
SZBI - 3.PBI	**Polityka Bezpieczeństwa Informacji**	5.2, 6.2, A.1.5.1	22.11.2024 r.
SZBI - 4.DS	**Deklaracja Stosowania**	6.1.3 d)	22.11.2024 r.
SZBI - 5.PZA	**Polityka Zarządzania Aktywami** (Procedura Inwentaryzacji Aktywów; procedura postępowania z informacjami i innymi powiązanymi aktywami; zwrot aktywów)	A.1.5.9, A.1.5.10, A.1.5.11, A.1.7.9	22.11.2024 r.
SZBI - 5.PZA - załącznik 1	**Ewidencja Rodzajów Aktywów**	A.1.5.9	22.11.2024 r.
SZBI - 5.PZA - załącznik 2	**Szczegółowa Ewidencja sprzętu IT**	A.1.5.9	22.11.2024 r.
SZBI - 6.MZR	**Metodyka Zarządzania Ryzykiem Bezpieczeństwa Informacji**	6.1.2	22.11.2024 r.
SZBI - 6.MZR - załącznik 1	**Analiza Ryzyka i Plan postępowania z ryzykiem w Bezpieczeństwie Informacji**	6.1.3 e), 6.2, 8.2, 8.3	22.11.2024 r.
SZBI - 7.POW	**Polityka Oceny Wyników SZBI** (Monitorowanie, Pomiar, Analizy i Ocena SZBI; audyty wewnętrzne SZBI; przegląd Zarządzania)	9.1, 9.2, 9.3	22.11.2024 r.
SZBI - 7.POW - załącznik 1	**Program Audytów Wewnętrznych SZBI (wzór)**	9.2	22.11.2024 r.
SZBI - 7.POW - załącznik 2	**Plan audytu wewnętrznego SZBI (wzór)**	Nie dotyczy	22.11.2024 r.
SZBI – 7. POW - załącznik 3	**Raporty z audytów wewnętrznych SZBI (wzór)**	9.2	22.11.2024 r.
SZBI - 7.POW - załącznik 4	**Raporty z przeglądów Zarządzania SZBI (wzór)**	9.3	22.11.2024 r.
SZBI - 8.PNN	**Polityka Nadzorowania Niezgodności i Działań Naprawczych**	10.2	22.11.2024 r.
SZBI - 8.PNN - załącznik 1	**Karta Niezgodności i raporty z działań naprawczych i korygujących (wzór)**	10.2	22.11.2024 r.
SZBI - 8.PNN - załącznik 2	**Rejestr Niezgodności (wzór)**		22.11.2024 r.
SZBI - 9.PPI	**Polityka Postepowania z Informacjami** (klasyfikacja informacji; oznakowanie informacji; przekazywanie informacji)	A.1.5.12, A.1.5.13, A.1.5.14	22.11.2024 r.
SZBI - 10.PBIRD	**Polityka Bezpieczeństwa Informacji w Relacjach z Dostawcami**	A.1.5.19, A.1.5.20 A.1.5.22	22.11.2024 r.
SZBI - 11.PZI	**Polityka Zarządzania Incydentami Bezpieczeństwa Informacji**	A.1.5.24, A.1.5.25, A.1.5.26, A.1.5.27, A.1.5.28	22.11.2024 r.
SZBI - 11.PZI – załącznik 1	**Notatka Służbowa z naruszenia BI (wzór)**	A.1.5.24, A.1.5.25, A.1.5.26, A.1.5.27, A.1.5.28	22.11.2024 r.
SZBI - 11.PZI – załącznik 2	**Rejestr Incydentów Bezpieczeństwa Informacji**	A.1.5.24, A.1.5.25, A.1.5.26, A.1.5.27, A.1.5.28	22.11.2024 r.
SZBI - 12.PCD	**Polityka Ciągłości Działania**	A.1.5.29, A.1.5.30	22.11.2024 r.
SZBI - 12.PCD - załącznik 1	**Rejestr Planów Ciągłości Działania**	A.1.5.30	22.11.2024 r.
SZBI - 13.PRWP	**Polityka Realizacji Wymagań Prawnych i Umownych**	A.1.5.31	22.11.2024 r.
SZBI -14.PZO	**Polityka Zabezpieczeń Organizacyjnych Bezpieczeństwa Informacji** (kontakt z władzami; kontakt z zainteresowanymi grupami; wywiad o zagrożeniach; zarządzanie projektami; kontrola dostępu; zarządzanie tożsamością; uwierzytelnianie; prawa dostępu; zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT; bezpieczeństwo informacji w korzystaniu z usług chmurowych; prawa własności intelektualnej; ochrona zapisów; ochrona informacji umożliwiających	A.1.5.5, A.1.5.6, A.1.5.7, A.1.5.8, A.1.5.9, A.1.5.10, A.1.5.11, A.1.5.15, A.1.5.16, A.1.5.17, A.1.5.18, A.1.5.21, A.1.5.23, A.1.5.25, A.1.5.26, A.1.5.27, A.1.5.28, A.1.5.32,	22.11.2024 r.

	identyfikację osób; niezależny przegląd bezpieczeństwa informacji; zgodność; udokumentowane procedury operacyjne)	A.1.5.33, A.1.5.34, A.1.5.35, A.1.5.36, A.1.5.37	
SZBI - 15.PPZ	**Polityka Pracy Zdalnej (odrębny dokument)**	A.1.6.7	22.11.2024 r.
SZBI - 16.PZZL	**Polityka Zarządzania Zasobami Ludzkimi w Bezpieczeństwie Informacji**	A.1.6.1, A.1.6.2, A.1.6.3, A.1.6.4, A.1.6.5, A.1.6.6, A.1.6.8	22.11.2024 r.
SZBI - 17.PZF	**Polityka Zabezpieczeń Fizycznych** (granice bezpieczeństwa fizycznego; wejście fizyczne; zabezpieczenie biur, pomieszczeń i obiektów; monitorowanie bezpieczeństwa fizycznego; ochrona przed zagrożeniami fizycznymi i środowiskowymi; czyste biurko i czysty ekran; usytuowanie i ochrona urządzeń; bezpieczeństwo aktywów poza siedzibą podmiotu; nośniki pamięci; narzędzia pomocnicze; bezpieczeństwo okablowania; konserwacja sprzętu; bezpieczna utylizacja sprzętu)	A.1.7.1, A.1.7.2, A.1.7.3, A.1.7.4, A.1.7.5, A.1.7.6, A.1.7.7, A.1.7.8, A.1.7.9, A.1.7.10, A.1.7.11, A.1.7.12, A.1.7.13, A.1.7.14.	22.11.2024 r.
SZBI - 18.PKZ	**Polityka Kopii Zapasowych**	A.1.8.13	22.11.2024 r.
SZBI - 19.PZT	**Polityka Zabezpieczeń Technologicznych Bezpieczeństwa Informacji** (urządzenia punktów końcowych użytkowników; uprzywilejowane prawa dostępu; ograniczenie dostępu do informacji; dostęp do kodu źródłowego; bezpieczne uwierzytelnianie; zarządzanie potencjałem; ochrona przed złośliwym oprogramowaniem; zarządzanie słabościami technicznymi; zarządzanie konfiguracją; usuwanie informacji; maskowanie danych; zapobieganie wyciekom danych; zapas informacji; redundancja urządzeń; rejestrowanie; działania monitorujące; synchronizacja zegara; uprzywilejowane programy; instalacja oprogramowania; bezpieczeństwo sieci; bezpieczeństwo usług sieciowych; segregacja sieci; filtrowanie stron internetowych; stosowanie kryptografii; cykl życia bezpiecznego rozwoju; wymagania dotyczące bezpieczeństwa aplikacji; bezpieczna architektura systemu; bezpieczne kodowanie; rozwój zlecany na zewnątrz; rozdzielenie środowisk rozwojowych, testowych i produkcyjnych; zarządzanie zmianami; informacje o badaniu; ochrona systemów informatycznych podczas badania audytowego)	A.1.8.1, A.1.8.2, A.1.8.3, A.1.8.4, A.1.8.5, A.1.8.6, A.1.8.7, A.1.8.8, A.1.8.9, A.1.8.10, A.1.8.11, A.1.8.12, A.1.8.14, A.1.8.15, A.1.8.16, A.1.8.17, A.1.8.18, A.1.8.19, A.1.8.20, A.1.8.21, A.1.8.22, A.1.8.23, A.1.8.24, A.1.8.25, A.1.8.26, A.1.8.27, A.1.8.28, A.1.8.29, A.1.8.30, A.1.8.31, A.1.8.32, A.1.8.33, A.1.8.34	22.11.2024 r.

WÓJT
Mariusz Cioch
....
Podpis

Odniesienia – norma ISO/IEC 27001:2022: 5.2, 6.2, A.1.5.1

POLITYKA BEZPIECZEŃSTWA INFORMACJI URZĄD GMINY W REGNOWIE

22.11.2024r.

.....
Data

1. Zapewniając bezpieczeństwo informacji zidentyfikowane zostały procesy jakie są realizowane w Urzędzie Gminy w Regnowie oraz aktywa informacyjne, które wymagają ochrony. W celu skutecznej ochrony informacji powierzonych przez mieszkańców Gminy oraz powstające w procesie realizacji naszych zdań wdrożyliśmy i stosujemy System Zarządzania Bezpieczeństwem Informacji.
2. System zarządzania bezpieczeństwem informacji jaki jest wdrożony w Urzędzie Gminy w Regnowie opiera się na identyfikacji i klasyfikacji informacji, które chcemy chronić. Jesteśmy świadomi, że informacje, niezależnie od nośnika, na którym są gromadzone oraz kanałów informacyjnych, którymi są przekazywane powinny być chronione w taki sposób, aby nie następowało ich nieautoryzowane ujawnienie, przekazanie lub wykorzystanie, które mogłoby prowadzić do naruszenia interesów i praw naszych interesariuszy. Niezmiernie istotne jest, aby wszystkie informacje były właściwie chronione, a także dostępne na czas dla osób upoważnionych oraz aby nie ulegały nieautoryzowanym zniekształceniom na skutek umyślnego lub nieumyślnego działania.
3. Aby spełnić wymagania w zakresie bezpieczeństwa informacji wszyscy pracownicy powinni stosować się do wymagań wynikających z niniejszej Polityki, Deklaracji Stosowania Zabezpieczeń oraz dokumentacji systemu zarządzania bezpieczeństwem informacji.
4. Dla zapewnienia wysokiego poziomu bezpieczeństwa informacji stosujemy następujące zasady:
    1) aktywa informacyjne są poddawane regularnym przeglądom,
    2) regularnie wykonywany jest proces oceny ryzyka w celu coraz lepszej identyfikacji zagrożeń związanych z wykorzystywanymi aktywami,
    3) stale podnosimy świadomość pracowników Urzędu w zakresie bezpieczeństwa informacji,
    4) kładziemy duży nacisk na stosowanie nowoczesnych i bezpiecznych technologii informacyjnych,
    5) zwracamy szczególną uwagę na dobór dostawców oraz odpowiedni nadzór nad powierzonymi im procesami i informacjami,
    6) zbieramy i analizujemy wszelkie incydenty związane z naruszeniem bezpieczeństwa informacji oraz podejmujemy niezwłoczne działania w celu wyeliminowania tych zagrożeń w przyszłości,
    7) identyfikujemy zobowiązania prawne oraz kontraktowe, a także oczekiwania petentów,
    8) stale monitorujemy skuteczność stosowanych zabezpieczeń,
    9) kładziemy duży nacisk na ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji,
5. Wszyscy pracownicy zobowiązani są do przestrzegania wymagań bezpieczeństwa informacji określonych w dokumentacji oraz tych wynikających z wymagań prawnych i innych.
6. Pracownicy Urzędu zobowiązani są do:
    1) dbałości o bezpieczeństwo powierzonych informacji,
    2) stosowania zabezpieczeń w odniesieniu do informacji i sprzętu służącego do tworzenia, przechowywania i przetwarzania informacji,
    3) ochrony danych osobowych,
    4) zgłaszania wszystkich stwierdzonych przypadków naruszenia bezpieczeństwa informacji,
    5) zgłaszania propozycji rozwiązań systemowych i organizacyjnych służących poprawie poziomu bezpieczeństwa informacji.

WÓJT
Mariusz Gleba

.....
Wójt Gminy w Regnowie