Załącznik do Zarządzenia Nr 16/2021
Wójta Gminy Grunwald
z dnia 10 lutego 2021 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

I. WSTĘP

Miarą skuteczności działania każdej jednostki jest stopień osiągania zamierzonych celów. Ogólny cel Urzędu (jego rola), a nade wszystko ogólny kierunek, w którym zmierza Urząd został określony w postaci misji.

„Misją Urzędu Gminy Grunwald jest zapewnienie należytego, sprawnego i fachowego realizowania zadań własnych, zleconych i powierzonych Gminie oraz tworzenie warunków do rozwoju gospodarczego Gminy”

Istotnym elementem sprawnej realizacji przez Urząd Gminy Grunwald zadań publicznych jest właściwe zabezpieczenie informacji przed istniejącymi zagrożeniami, w tym systemów w których informacje są przetwarzane.
Bezpieczeństwo informacji ma zagwarantować wdrożony System Zarządzania Bezpieczeństwem Informacji, zapewniający poufność, dostępność i integralności informacji.

II. DEKLARACJA KIEROWNICTWA

Wójt Gminy zobowiązuje się podejmować wszelkie działania związane z wdrożeniem oraz doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Grunwald.

W związku z powyższym Wójt, deklaruje zapewnienie optymalnych warunków i niezbędnych środków dla realizacji celów Systemu Zarządzania Bezpieczeństwem Informacji oraz stałą współpracę z osobami odpowiedzialnymi, w celu opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI.

III. POJĘCIA I SKRÓTY

l) informacja - dowolny komunikat (przekaz treści), któremu można przypisać określone znaczenie, aby móc go wykorzystać do różnych celów. Informacja może przybierać różne formy np. pisemną (wydruku), elektroniczną, ustną oraz audio i wideo;
2) bezpieczeństwo informacji należy przez to rozumieć zachowanie poufności, integralności i dostępności informacji;
3) poufność - właściwość informacji polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom lub procesom;
4) integralność - właściwość informacji polegająca na tym, że informacja nie jest poddawana nieautoryzowanym modyfikacjom lub została usunięta (zniszczona) w sposób nieautoryzowany oraz jest przetwarzana w kontrolowany sposób;

5) dostępność - właściwość informacji polegająca na byciu dostępnym i użytecznym na żądanie upoważnionego podmiotu w danym miejscu i w danym czasie;
6) ryzyko - prawdopodobieństwo wystąpienia zdarzenia niepożądanego i jego konsekwencji, wpływ niepewności na cele bezpieczeństwa informacji;
7) zarządzanie ryzykiem - proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowanego poziomu;
8) aktywa - zasób - wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania);
9) SZBI - System Zarządzania Bezpieczeństwem Informacji - część całościowego systemu zarządzania, oparty na szacowaniu ryzyka, odnoszący się do ustanowienia, wdrożenia, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji;
10) PBI - Polityka Bezpieczeństwa Informacji Urzędu Gminy Grunwald, jako element SZBI.

IV. POLITYKA BEZPIECZEŃSTWA INFORMACJI JAKO GŁÓWNY ELEMENT SZBI

Polityka Bezpieczeństwa Informacji obejmuje wszystkie obszary funkcjonowania Urzędu Gminy, pracowników i podmioty współpracujące i ma zastosowanie do wszystkich zasobów informacyjnych Urzędu, niezależnie od formy przechowywania informacji (papierowej lub elektronicznej).

PBI nie obejmuje swoim zakresem informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 z późn. zm.) oraz nie ma zastosowania dla gminnych jednostek organizacyjnych.

V. CELE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Opracowany, ustanowiony, wdrożony i eksploatowany SZBI podlega bieżącemu monitorowaniu, przeglądowi, utrzymaniu i doskonaleniu.

Urząd stawia przed SZBI następujące cele :

1) osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa aktywów informacyjnych Urzędu poprzez - zapewnienie poufności, dostępności i integralności informacji;
2) zapewnienie ochrony wizerunku Urzędu;
3) zapewnienie sprawnej realizacji zadań Urzędu;
4) spełnienie wszelkich wymogów obowiązującego prawa odnośnie ochrony informacji przetwarzanych w Urzędzie;
5) zapewnienie odpowiedniego zaangażowania pracowników w utrzymanie bezpieczeństwa informacji;
5) zidentyfikowanie wszelkich aktywów informacyjnych w rozumieniu SZBI;
6) zarządzanie ryzykiem i wdrożenie odpowiednich zabezpieczeń;
7) zarządzanie incydentami naruszającymi bezpieczeństwo informacji.

VI. ZESPÓŁ DO SPRAW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

1. W Urzędzie Gminy Grunwald powołuje się Zespół do Spraw Zarządzania Bezpieczeństwem Informacji, który wspiera Wójta Gminy w zarządzaniu bezpieczeństwem informacji, w szczególności poprzez :

l) doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji, w tym definiowanie potrzeb w zakresie poprawy bezpieczeństwa informacji;

2) nadzór nad dokumentacją Systemu, w tym monitorowanie i doskonalenie Polityki Bezpieczeństwa Informacji;

3) analizę incydentów naruszenia bezpieczeństwa informacji i określanie działań korygujących;

4) identyfikację aktywów i zarządzanie ryzykiem.

2. W skład Zespołu wchodzą:

1) Sekretarz Gminy — jako koordynator;
2) Inspektor Ochrony Danych (IOD);
3) Administrator Systemu Informatycznego;
4) Pracownik Urzędu wykonujący zadania w zakresie informatyzacji.

VII. ODPOWIEDZIALNOŚĆ ZA OCHRONĘ INFORMACJI ORAZ KONSEKWENCJE ZA NARUSZENIE BEZPIECZEŃSTWA INFORMACJI

Właściciele merytorycznych informacji (bez względu na formę przetwarzania) są zobowiązani do zapewnienia optymalnego bezpieczeństwa informacji.

Do stosowania zasad określonych w dokumentacji SZBI zobowiązani są wszyscy pracownicy Urzędu, stażyści, praktykanci oraz inne osoby i podmioty mające dostęp do zasobów informacyjnych.

Nieprzestrzeganie zasad określonych w dokumentacji SZBI, stanowi naruszenie obowiązków pracowniczych, co może skutkować odpowiedzialnością dyscyplinarną określona przepisami Kodeksu pracy lub inną wynikająca z odpowiednich przepisów prawa.

VIII. UTRZYMANIE ODPOWIEDNIEGO POZIOMU BEZPIECZEŃSTWA INFORMACJI

1. Rozwijany SZBI powinien zawierać elementy pozwalające utrzymać odpowiedni poziom bezpieczeństwa, w tym:

1) Politykę zarządzania ryzykiem;
2) Politykę Ochrony Danych;
3) Rejestr czynności przetwarzania danych osobowych;
4) monitorowanie poziomu bezpieczeństwa, w tym audyt wewnętrzny w zakresie bezpieczeństwa informacji;
5) nadzór nad dokumentacją SZBI;
6) zapewnienie ciągłości działania systemów teleinformatycznych;
7) Politykę antymobbingową.

2. Nakłady ponoszone na zabezpieczenia powinny być poprzedzone analizą ryzyka i oceną kosztów związanych z ich wdrożeniem w celu zastosowania zabezpieczeń, adekwatnie do wymagań prawnych i potencjalnych strat spowodowanych naruszeniem bezpieczeństwa.

3. W celu doskonalenia i utrzymania odpowiedniego poziomu bezpieczeństwa informacji ważne jest systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników Urzędu.

IX. ZARZĄDZANIE RYZYKIEM

Zarządzanie ryzykiem odnosi się do aktywów Urzędu. Aktywa są zidentyfikowane, a następnie poddane analizie, jakim zagrożeniom podlegają oraz jakie to niesie ze sobą skutki. Na tej podstawie, w oparciu o metodykę szacowania ryzyka szacowane jest ryzyko, a następnie podejmowane decyzje mające na celu obniżenie ryzyka do poziomu akceptowalnego.

X. ZABEZPIECZENIA

Urząd powinien dobierać cele stosowania zabezpieczeń i zabezpieczenia adekwatne do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.