

ZARZĄDZENIE Nr 37/2014
WÓJTA GMINY SOMONINO
z dnia 07.07.2014r.

W sprawie wdrożenia w Urzędzie Gminy w Somoninie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z wymaganiami normy ISO 27001:2007.

Na podstawie art. 33 ust. 1 i 3 Ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2013r. poz.594 z późn. zm.) oraz § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. 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 2012r. poz. 525), zarządzam co następuje:

§ 1.

Jako Administrator Bezpieczeństwa Informacji polecam zespołowi ds. wdrożenia SZBI w składzie jak niżej dostosowanie ustanowionych w Urzędzie Gminy w Somoninie metod i technik zarządzania bezpieczeństwem informacji do wymagań międzynarodowej normy ISO 27001:2007 i utworzenie na ich bazie Systemu Zarządzania Bezpieczeństwem Informacji.

§ 2.

Powołuję Zespół ds. wdrożenia SZBI w składzie:

- 1) Przewodniczący Zespołu – Jerzy Kowalewski – Zastępca Wójta Gminy Somonino,
- 2) Koordynator systemów i zasobów informatycznych – Marcin Singer – insp. ds. informatycznych,
- 3) Członek Zespołu – Sabina Reclaw – Drewna – Sekretarz Gminy,
- 4) Członek Zespołu – Izabela Wysocka – podinspektor ds. opłat za odpady komunalne,
- 5) Audytor wewnętrzny SZBI – Patryk Richert – referent ds. podatków i opłat

§ 3.

Przewodniczącemu Zespołu polecam przeprowadzenie projektu wdrożeniowego, w zakresie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Somoninie i uzyskaniu niezależnego potwierdzenia zgodności z międzynarodową normą ISO 27001:2007.

§ 4.

Zakres zadań Zespołu ds. wdrożenia SZBI obejmuje:

- 1) w zakresie analizy ryzyka i implementacji zabezpieczeń:
 - a) identyfikację wymagań prawnych związanych z ochroną informacji,
 - b) określenie zasobów informacyjnych wymagających zastosowania mechanizmów zabezpieczających,
 - c) klasyfikację ryzyk i oszacowanie prawdopodobieństwa lub częstości ich występowania,
 - d) identyfikację podatności zasobów na ryzyko,
 - e) oszacowanie ryzyka,
 - f) ocenę możliwych zabezpieczeń pod względem bezpieczeństwa, ekonomicznym i użytkowym,
 - g) wybór i wdrożenie zabezpieczeń optymalnych,
- 2) w zakresie organizacji bezpieczeństwa informacji:
 - a) opracowanie systemowych mechanizmów klasyfikacji informacji (klauzul), zmierzających do zapewnienia bezpieczeństwa informacji oraz kontroli nad dostępem i przepływem informacji,
 - b) opracowanie systemowych mechanizmów zarządzania klauzulami,
 - c) opracowanie mechanizmów bezpieczeństwa osobowego,
 - d) opracowanie programów szkoleń dla pracowników Urzędu, w tym osób odbywających służbę przygotowawczą oraz personelu wykonującego pracę z wykorzystaniem zasobów Urzędu na podstawie umów innych niż umowa o pracę,
 - e) opracowanie systemowych mechanizmów zarządzania zmianami.
- 3) w zakresie technicznego bezpieczeństwa informacji:
 - a) opracowanie systemowych mechanizmów zarządzania oprogramowaniem,

- b) opracowanie systemowych mechanizmów zarządzania kopiami zapasowymi,
 - c) opracowanie mechanizmów utrzymywania gotowości i reagowania na incydenty w środowisku elektronicznym,
 - d) opracowanie mechanizmów bezpieczeństwa sieci i okablowania,
 - e) opracowanie systemowych mechanizmów nadzoru nad konserwacją i serwisem sieci, sprzętu teleinformatycznego i okablowania,
 - f) określenie wymagań technicznych i procedur zarządzania mechanizmami kryptograficznymi,
 - g) ustanowienie i przeprowadzenie walidacji bezpieczeństwa informacji.
- 4) w zakresie dokumentacji bezpieczeństwa informacji:
- a) weryfikację Polityki Bezpieczeństwa,
 - b) opracowanie Planu ciągłości działania,
 - c) weryfikację wdrożonych i opracowanie nowych regulaminów i wytycznych w zakresie bezpieczeństwa informacji,
 - d) weryfikację procedur Systemu Zarządzania Bezpieczeństwem Informacji pod kątem zgodności z dokumentem odniesienia – normą ISO 27001:2007,
 - e) opracowanie procedur i instrukcji Systemu Zarządzania Bezpieczeństwem Informacji,
 - f) opracowanie systemowych mechanizmów ewidencjonowania i zapisu działań związanych z bezpieczeństwem informacji.

§ 5.

Wszystkim pracownikom Urzędu polecam aktywne uczestnictwo w pracach nad Systemem Zarządzania Bezpieczeństwem Informacji i wsparcie jego implementacji. Wsparcie to powinno obejmować co najmniej następujące działania:

- a) przygotowywanie danych wejściowych niezbędnych do opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji,
- b) aktywny udział w szkoleniach i instruktażach prowadzonych w ramach projektu wdrożeniowego,
- c) wykonanie czynności związanych ze skutecznym wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji na swoich stanowiskach pracy.

§ 6.

Wykonanie zarządzenia powierzam Sekretarzowi Gminy Somonino

§ 7.

Zarządzenie wchodzi w życie z dniem podpisania.

z up. WÓJTA
Jerzy Kowalewski
Z-CA WÓJTA