Urząd Miejski
ul.Kościuszki 27
89-650 Czersk

BR.0050.115.2014

ZARZĄDZENIE NR 736/14
BURMISTRZA CZERSKA

z dnia 14 lipca 2014 r.

w sprawie wdrożenia w Urzędzie Miejskim w Czersku Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO 27001:2007.

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (t. j. - Dz. U. z 2013 r., poz. 594 ze 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. 526), zarządzam co następuje:

§ 1.

Panu Bogdanowi Daneckiemu – Administratorowi Bezpieczeństwa Informacji polecam dostosowanie ustanowionych w Urzędzie Miejskim w Czersku 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 – Grzegorz Zabrocki,

2) Koordynator systemów i zasobów informatycznych - Opiekun sieci komputerowej - Wiesław Kononowicz - działający zgodnie z umową nr WO-272-1/6/2014 z dnia 2 stycznia 2014 r.,

3) Członek Zespołu – Administrator Bezpieczeństwa Informacji – Bogdan Danecki,

4) Audytor wewnętrzny SZBI – Joanna Blumowska- Hatta,

5) Audytor wewnętrzny SZBI – Agnieszka Gliniecka.

§ 3.

Przewodniczącemu Zespołu polecam przeprowadzenie projektu wdrożeniowego w zakresie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Czersku i uzyskanie 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,

g) ocenę możliwych zabezpieczeń pod kątem ekonomicznym i użytkowym,

h) 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 pełniących 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 Miejskiego w Czersku 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.

§ 7.

Zarządzenie wchodzi w życie z dniem podpisania.

z up. Burmistrza
Zastępca Burmistrza

Jan Gliszczyński

Uzasadnienie

Zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Urząd Miejski w Czersku ma obowiązek przeprowadzania audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Jednocześnie wdrożenie w Urzędzie Miejskim w Czersku Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO 27001:2007 pozwala na spełnienie obowiązków wynikających z przedmiotowego rozporządzenia, w tym obowiązku przeprowadzania audytu, przez najbliższe trzy lata.

Mając na uwadze, że istnieje możliwość wdrożenia w Urzędzie ISO 27001:2007 w ramach projektu systemowego dotyczącego CAF, finansowanego w całości ze środków zewnętrznych, wydanie niniejszego zarządzenia uważa się za uzasadnione i konieczne.