Zarządzenie Nr 207/16
Burmistrza Miasta Międzyrzec Podlaski
z dnia 22 lutego 2016 r.

w sprawie ustanowienia i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Międzyrzec Podlaski

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2015 r., poz. 1515, z późn. zm.) w związku z § 20 Rozporządzenia 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 (Dz.U z 2016, poz. 113) zarządzam, co następuje:

§ 1.

Ustanawiam i wdrażam System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Międzyrzec Podlaski.

§ 2.

1. System Zarządzania Bezpieczeństwem Informacji zapewnia poufność, dostępność i integralność informacji wytwarzanych i przetwarzanych w Urzędzie Miasta Międzyrzec Podlaski z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. System Zarządzania Bezpieczeństwem Informacji wprowadzony w Urzędzie Miasta w uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa w tym:
   1) zarządzanie ryzykiem;
   2) zarządzenie dostępem do zasobów;
   3) monitorowanie poziomu bezpieczeństwa;
   4) zarządzanie incydentem;
   5) nadzoru nad dokumentacją Systemu Bezpieczeństwa Informacji.

§ 3.

Zapewnienia się warunki umożliwiające realizację i egzekwowanie następujących działań:
1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienie szkoleń osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

§ 4.

Sposób realizacji działań, o których mowa w § 3 określa Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Międzyrzec Podlaski, stanowiąca załącznik do niniejszego zarządzenia, będąca integralną częścią Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Międzyrzec Podlaski.

§ 5.

Zobowiązuję pracowników Urzędu Miasta Międzyrzec Podlaski do zapoznania się Polityką Bezpieczeństwa Informacji w Urzędzie Miasta Międzyrzec Podlaski.

§ 6.

Nadzór nad wykonaniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji oraz Przewodniczącemu Zespołu ds. Bezpieczeństwa Informacji.

§ 7.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ MIASTA

Zbigniew Kot