ZARZĄDZENIE NR 18/2020
STAROSTY ŁÓDZKIEGO WSCHODNI9EGO
z dnia 25 lutego 2020 roku

w sprawie przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji w Starostwie Powiatowym w Łodzi

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz. U. z 2019 r. poz. 511, poz. 1571 i poz. 1815) i § 20 ust. 2 pkt 14 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 2017 r. poz. 2247) w związku z Zarządzeniem Nr 16/2011 Starosty Łódzkiego Wschodniego z dnia 21 marca 2011 r. w sprawie ustalenia Regulaminu funkcjonowania kontroli zarządczej w Starostwie Powiatowym w Łodzi, zarządza się co następuje:

§ 1.1. Przeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji na podstawie § 20 ust. 2 pkt 14 z 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, w Starostwie Powiatowym w Łodzi.

2. W ramach realizacji zadania, o którym mowa w ust. 1. określa się zakres czynności, których wykaz stanowi załącznik do niniejszego zarządzenia.

§ 2. Termin realizacji zadania o którym mowa w § 1. w pierwszym półroczu 2020 roku.

§ 3. Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Andrzej Opala

Załącznik
do Zarządzenia Nr 18/2020
Starosty Łódzkiego Wschodniego
z dnia 25 lutego 2020 r.

WYKAZ ELEMENTÓW AUDYTU

Usługa polegająca na przeprowadzeniu w 2020 roku okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji w Starostwie Powiatowym w Łodzi określonego w § 20 ust. 2 pkt 14 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 2017 r. poz. 2247), w Starostwie Powiatowym w Łodzi.

L.p.	PODSTAWA PRAWNA	ELEMENT / OBSZAR AUDYTU
1	§ 15 ust. 1 KRI	Audyt działań projektowych, wdrożeniowych oraz eksploatacyjnych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
2	§ 20 ust. 1 KRI	Audyt Systemu Zarządzania Bezpieczeństwem Informacji pod kątem poufności, dostępności i integralności.
3	§ 20 ust. 2 pkt 1 KRI	Audyt regulacji wewnętrznych w zakresie zmieniającego się otoczenia pod kątem aktualizacji.
4	§ 20 ust. 2 pkt 2 KRI	Audyt utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
5	§ 20 ust. 2 pkt 3 KRI	Audyt okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
6	§ 20 ust. 2 pkt 4 KRI	Audyt 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.
7	§ 20 ust. 2 pkt 6 KRI	Audyt procesów zapewniających szkolenia 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.
8	§ 20 ust. 2 pkt 7 KRI	Audyt ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, pod kątem: a) monitorowania dostępu do informacji, b) czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.
9	§ 20 ust. 2 pkt 8 KRI	Audyt ustanowionych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

10	§ 20 ust. 2 pkt 9 KRI	Audyt zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
11	§ 20 ust. 2 pkt 10 KRI	Audyt umów serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji.
12	§ 20 ust. 2 pkt 11 KRI	Audyt zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.
13	§ 20 ust. 2 pkt 12 KRI	Audyt 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.
14	§ 20 ust. 2 pkt 12 lit. b KRI	Audyt poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.
15	§ 20 ust. 2 pkt 13 KRI	Audyt komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
16	§ 20 ust. 2 pkt 14 KRI	Audyt ciągłości wykonywania audytu wewnętrznego.
17	§ 20 ust. 4 KRI	Audyt występowania dodatkowych zabezpieczeń, niezależnych od zakresu, o którym mowa w § 20 ust. 2 pkt 1÷14, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne.
18	§ 21 ust. 2 KRI	Audyt prowadzenia / występowania dzienników systemowych odnotowujących działania użytkowników lub obiektów systemowych, polegających na dostępie do: a) systemu z uprawnieniami administracyjnymi, b) konfiguracji systemu, w tym konfiguracji zabezpieczeń, c) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
19	21 ust. 3 KRI	Audyt występowania procedur spoza zakresu § 20 ust. 2 pkt 1÷14, mogących stanowić odnotowywanie działań użytkowników lub obiektów systemowych, a także innych zdarzeń związanych z eksploatacją systemu w postaci: a) działań użytkowników nieposiadających uprawnień administracyjnych, b) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, c) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny, – w zakresie wynikającym z analizy ryzyka
20	§ 21 ust. 4 KRI	Audyt procedur związanych z dziennikami systemowymi.