Załącznik Nr 23 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Wytyczne dotyczące audytu bezpieczeństwa informacji wykonywane przez podmiot zewnętrzny

§ 1. W Urzędzie przeprowadza audyty Systemu Zarządzania Bezpieczeństwem:

1) audyt bezpieczeństwa informacji,

2) audyt zabezpieczeń systemów informatycznych.

§ 2. Audyty Systemu Zarządzania Bezpieczeństwem Informacji powinny być przeprowadzane co najmniej raz na rok zgodnie z procedurą audytu bezpieczeństwa informacji.

1. Audyty mają na celu niezależną weryfikację należytego zabezpieczenia informacji przetwarzanych przez Urząd.

2. Audyty mogą być dodatkowo przeprowadzane w przypadku zaistnienia okoliczności wskazujących na konieczność niezależnej weryfikacji mechanizmów zarządzania bezpieczeństwem informacji.

§ 3. 1. Audyt bezpieczeństwa informacji wykonywany być może przez uprawnionego pracownika Wydziału Kontroli i Audytu Wewnętrznego.

2. W przypadku podjęcia decyzji o zleceniu usługi podmiotom zewnętrznym decyzję o rozpoczęciu postępowania celem zlecenia audytu zewnętrznego podejmuje AD.

3. Zakres audytu zewnętrznego określany jest przez AD po konsultacjach z WInf i ABI.

4. Wybór podmiotu świadczącego usługę audytu zewnętrznego odbywa się na podstawie przepisów dotyczących zamówień publicznych lub wewnętrznym przepisów w przypadku gdy zamówienie nie podlega wymogom ustawy zamówień publicznych.

5. Umowa zawarta z usługodawcą spełnia wymagania określone w niniejszej polityce.

1. AD wyznacza osobę koordynującą realizację.

§ 4. 1. Audyt przeprowadzany jest na podstawie harmonogramu prac przygotowanego przez usługodawcę i zatwierdzonego przez ADu lub upoważnionego pracownika.

2. Audyt zewnętrzny:

1) nie powinien trwać dłużej niż 6 tygodni.

2) nie powinien powodować utrudnień w realizacji zadań Urzędu.

§ 5. 1. W ramach przeprowadzania audytu usługodawca może otrzymać dokumentację w zakresie niezbędnym do realizacji przedmiotowych prac.

2. Dopuszcza się przekazanie kopii dokumentacji usługodawcy do pracy poza siedzibą Urzędu, o ile dokumentacja nie zawiera informacji prawnie chronionych.

3. Dokumentacja przekazywana jest za pokwitowaniem przez koordynatora audytu po stronie Urzędu.

4. Po zakończeniu audytu dokumentacja w postaci papierowej jest zwracana za potwierdzeniem.

5. Po zakończeniu audytu usługodawca podpisuje oświadczenie zawierające klauzule:

1) potwierdzające zwrot całości dokumentacji papierowej otrzymanej od Urzędu.

2) potwierdzającej zniszczenie wszelkich wykonanych przez siebie kopii dokumentacji papierowej.

3) potwierdzającej zniszczenie wszelkiej podlegającej audytowi dokumentacji elektronicznej otrzymanej od Urzędu oraz ich kopii.

§ 6. 1. Wywiady z pracownikami Urzędu (jeśli są przewidziane w metodyce audytu) powinny odbywać się w obecności koordynatora audytu po stronie Urzędu lub kierownika osoby biorącej udział w wywiadzie.

2. Zakres wywiadu może dotyczyć wyłącznie zagadnień będących przedmiotem audytu i wynikających z umowy z usługodawcą przeprowadzającym audyt.

3. Wywiady podlegają dokumentowaniu przez osoby biorące w nich udział.

§ 7. 1. Wizje lokalne mogą odbywać się wyłącznie w obecności koordynatora audytu po stronie Urzędu, kierownika komórki organizacyjnej, w którego gestii znajduje się dane pomieszczenie lub wyznaczonego przez niego pracownika.

2. Wyniki wizji lokalnych są dokumentowane w postaci protokołu i przekazywane koordynatorowi audytu po stronie Urzędu.

§ 8. Czynności audytowe dopuszczają możliwość rozdysponowania ankiet wśród pracowników Urzędu, celem zapoznania się ze świadomością pracowników w audytowanym obszarze.

§ 9. Audyt zabezpieczeń systemów informatycznych

1. Zakres audytu zabezpieczeń systemów informatycznych, metodyka przeprowadzenia audytu, w tym wykorzystywane narzędzia, oraz terminy realizacji prac podlegają zatwierdzeniu przez AD lub upoważnionego pracownika.

2. Informacje dotyczące konfiguracji systemów informatycznych przekazywane są usługodawcy przez pracownika WInf poprzez prezentowane przez nich na ekranach monitorów albo w postaci wydruku.

3. Komputery usługodawcy i inne urządzenia informatyczne mogą być podłączone do sieci informatycznej Urzędu wyłącznie za zgodą Dyrektora WInf lub upoważnionego pracownika.

§ 10. 1. Wynik audytu dokumentowane są w postaci raportu i przekazywane koordynatorowi audytu po stronie Urzędu.

2. Dopuszcza się odstąpienie od dokumentowania w postaci protokołów jeżeli audyt zabezpieczeń jest przeprowadzany przy pomocy specjalistycznego oprogramowania generującego raporty zawierające wyniki audytu.

3. Raport z audytu podlega zatwierdzeniu przez AD lub upoważnionego pracownika.

4. Wnioski z audytu podlegają zatwierdzeniu i wdrożeniu jako działania korygujące i zapobiegawcze.