Szanowni Państwo!

Zapraszam do wypełnienia ankiety, która stanowi narzędzie do pozyskania informacji w zakresie przyjętych modeli organizacyjnych w obszarze bezpieczeństwa informacji w jednostkach samorządu terytorialnego. Pozyskane informacje zostaną wykorzystane w pracy magisterskiej pt. „Porównanie modeli organizacyjnych stosowanych w dużych jednostkach samorządu terytorialnego w Polsce w zakresie wykonywania zadań z obszaru Bezpieczeństwa Informacji. Wpływ funkcjonującego Systemu Zarządzania zgodnego z normą ISO 9001 na budowanie kompetencji w ramach Systemu Zarządzania Bezpieczeństwem Informacji."

Definicje używanych słów przywołanie w ankiecie:

Audit - w rozumieniu audytu prowadzonego zgodnego z normą ISO 19011.
SZJ – system zarządzania zgodny z wymaganiami normy ISO 9001.
SZBI – system zarządzania bezpieczeństwem informacji zgodnego z ISO 27001 lub innymi dobrymi praktykami.
ABI – Administrator Bezpieczeństwa Informacji.
uodo – ustawa o ochronie danych osobowych.

Pytania zawarte w ankiecie mają charakter zamknięty (proszę o zaznaczenie właściwej odpowiedzi) oraz otwarty (wszędzie tam gdzie umieszczono pole tekstowe, proszę o wpisanie do nich Państwa odpowiedzi).

System zarządzania bezpieczeństwem informacji – część ogólna

1. Czy Urząd podjął pracę nad wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji (zgodnie z wymaganiem zawarty w §20. 1 rozdziału IV 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)?
    a. Nie
    b. Tak, zgodnie z normą ISO 27001. (przejdź do pytania 2).
    c. Tak, zgodnie z wypracowanymi dobrymi praktykami. (przejdź do pytania 4).

Jakie to praktyki:

Miejsce na odpowiedź:

2. Czy wdrożony system zarządzania bezpieczeństwem informacji zgodny z normą ISO 27001 jest zintegrowany z systemem zgodnym z normą 9001?
    a. tak.
    b. nie
    c. nie, jednostka funkcjonuje w oparciu o standardy kontroli zarządczej.
3. Czy Urząd certyfikował system zarządzania bezpieczeństwa informacji zgodny z normą ISO 27001?
    a. tak
    b. nie
4. Jaki jest zakres działania Systemu Zarządzania Bezpieczeństwem Informacji?
    a. Urząd.
    b. Większy zakres.

Jeśli większy zakres to jaki? (np. Urząd i miejskie jednostki organizacyjne lub niektóre miejskie jednostki organizacyjne)

Miejsce na odpowiedź:

5. W jaki sposób realizuje się zarządzanie ryzykiem w kontekście bezpieczeństwa informacji? Proszę o wskazanie jaką metodykę przyjęto w ramach identyfikacji i oceny ryzyk z obszaru bezpieczeństwa informacji.
    a. wspólna metodyka zarządzania ryzykiem w organizacji.
    b. inna metodyka do zarządzania ryzykami do zadań bieżących oraz inna dla identyfikowania ryzyk z obszaru bezpieczeństwa informacji .

Miejsce na komentarz:

6. W jaki sposób jednostka dąży do zrealizowania normatywu z rozporządzenia wykonawczego do uodo (ws. trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji), aby w terminie 5 lat sprawdzeniem objąć wszystkie zbiory danych osobowych przetwarzanych w jednostce?

Miejsce na odpowiedź: w okresie ok. 15 m-cy wykonano analizę przetwarzanych zbiorów, aktualizację dokumentacji bezpieczeństwa (PBI i Instrukcji) oraz weryfikację zgłoszeń do rejestracji zbiorów u GIODO

System zarządzania bezpieczeństwem informacji – część szczegółowa dotycząca integracji

7. Integracja systemu zarządzania zgodnego z normą ISO 9001 z systemem zarządzania bezpieczeństwem informacji. (ta część dotyczy Urzędu, który w pyt. 2 odpowiedział „tak", pozostałe Urzędy proszone są o przejście do pyt. 8)
    a. W jaki sposób Urząd podszedł do obowiązku powołania Pełnomocnika ds. Systemu Zarządzania?
        i. Wspólny Pełnomocnik – SZJ (ISO 9001) i SZBI(np. ISO 27001)
        ii. Dwóch niezależnych Pełnomocników.

    b. Integracja dokumentacji zintegrowanego systemu zarządzania
    (proszę o wstawienie „x" w odpowiedniej komórce w poniższej tabeli)

Element systemu	**Wspólne**	**Niezależne**	**Komentarz**
Księga Systemu Zarządzania			
Polityka Systemu Zarządzania			
Plan jakości			
Przegląd systemu zarządzania			
Procedura monitowania celów			
Procedura auditów wewnętrznych			
Procedura nadzoru nad dokumentacją			
Procedura działań doskonalących			

    c. Czy oprócz wymienionych we wcześniejszym pytaniu procedur zidentyfikowano inne wspólne procedury w ramach zintegrowanego systemu?

Miejsce na odpowiedź:

    d. Czy opisywanie procesów/procedur dotyczących SZBI odbywa się w ramach jednego narzędzia informatycznego(np. Aris, BIC Platform, MS Office itp.).
        i. Wspólne narzędzie do opisywania procedur
        ii. różne systemy informatyczne.

    W jakich narzędziach informatycznych odbywa się opracowywanie przebiegów procesów i procedur w ramach systemu zarządzania

Miejsce na odpowiedź: (proszę o wskazanie w jakim narzędziu opracowuje Państwo procesy/procedury z zakresu systemu zarządzania ISO 9001 i SZBI)

e. Tryb planowania auditów wewnętrznych / planowanie sprawdzeń planowych w zakresie wykonywania przepisów ochrony danych osobowych (za realizację których odpowiada ABI). Czy procedura planowania auditów zakłada wspólne planowanie auditów i sprawdzeń?
   i. Połączone
   ii. Niezależne od siebie

f. Kto jest odpowiedzialny za opracowanie raportów z auditów / sprawdzeń z zakresu SZBI?
   i. Auditorzy wewnętrzni systemu zarządzania
   ii. Administrator Bezpieczeństwa Informacji
   iii. Inna rola w systemie zarządzania - kto jest odpowiedzialny za opracowanie raportu?

Miejsce na odpowiedź:

g. Jaką rolę odgrywają auditorzy wewnętrzni systemu zarządzania w kontekście bezpieczeństwa informacji – w jakim stopniu są angażowani w weryfikację funkcjonowania elementów Bezpieczeństwa Informacji?
   i. W ramach auditu systemu zarządzania dokonują weryfikacji celu z zakresu SZBI.
   ii. W ramach sprawdzeń dokonują weryfikacji elementów zabezpieczeń zbiorów danych osobowych.
   iii. Inne niż wyżej wymienione:

Miejsce na odpowiedź:

h. Przegląd systemu zarządzania.
   i. Jak często odbywają się przeglądy (np. raz w roku, dwa razy do roku)?

Miejsce na odpowiedź: raz w roku

   ii. Czy połączono przegląd systemu zarządzania zgodnego z normą ISO 9001 z przeglądem systemu zarządzania bezpieczeństwem informacji?
      A. tak
      B. nie
   iii. Jakie punkty omawiane są podczas przeglądu systemu zarządzania? (dotyczy agendy dwóch ostatnich przeglądów systemu zarządzania)
      A. wymagania z pkt. 5.6. systemu zarządzania zgodnego z normą ISO 9001 stanowiące materiał wejściowy.
      B. punkty wymagane przez normy ISO 9001 , ISO 27001 oraz innych wymagań innych norm w ramach zintegrowanego systemu zarządzania.
      C. wszystkie powyższe oraz inne tematy omawiane są podczas przeglądu

Miejsce na komentarz:

   iv. Jakie elementy podczas przeglądu systemu zarządzania omawiane są z obszaru systemu zarządzania bezpieczeństwem informacji? (zaznaczyć kółkiem elementy, które omawiane są podczas przeglądu)
      A. wyniki audytów i przeglądów SZBI,
      B. informacje zebrane od zainteresowanych stron,
      C. techniki i procedury możliwe do zastosowania w organizacji w celu udoskonalenia SZBI,
      D. informacje na temat działań korygujących i naprawczych,
      E. podatności lub zagrożenia nieobjęte poprzednim oszacowaniem ryzyka,

F. działania podjęte w ramach wdrażania rekomendacji z poprzednich przeglądów wykonanych przez kierownictwo,
G. zmiany w zakresie SZBI,
H. zalecenia dotyczące doskonalenia SZBI.

Miejsce na komentarz:

8. Czy w Urzędzie powołano Administratora Bezpieczeństwa Informacji?
   a. Tak
   b. Nie
   c. Korzysta się z usług zewnętrznego podmiotu.
9. W jaki sposób realizowany jest wymóg z art. 36 a ust. 8 uodo tj. administrator danych zapewnia środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań?

Miejsce na odpowiedź: w strukturze UM utworzono komórkę organizacyjną **Administrator Bezpieczeństwa Informacji** podlegającą zgodnie z przepisami ustawowymi bezpośrednio kierownikowi jednostki organizacyjnej

10. Jaki model organizacyjny zastosowano w przypadku nieobecności ABI?
    a. Powołano w tym celu zastępcę
    b. Upoważniono do pełnienia tej roli pracownika w przypadku nieobecności ABI.
    c. ABI nie ma zastępstwa
    d. Inny model organizacyjny. Jaki?

Miejsce na odpowiedź:

11. Struktura zarządzania poszczególnymi zagadnieniami z obszaru Bezpieczeństwa Informacji (dotyczy przyjętego przez Urząd modelu organizacyjnego):
    a. kadra pracowników odpowiedzialna za funkcjonowanie (lub wdrożenie) systemu zarządzania bezpieczeństwem informacji zgodnego z Krajowymi Ramami Interoperacyjności lub innymi standardami (np. ISO 27001)
       i. proszę o wskazanie stanowisk,

Miejsce na odpowiedź: Dyrektor oraz administratorzy Wydziału Informatyki i ABI

       ii. proszę o wymienienie podstawowych zadań w ramach SZBI wskazanych stanowisk,

Miejsce na odpowiedź: jak 11e

       iii. jakie jest jakie umiejscowienie w strukturze organizacyjnej jednostki wskazanych stanowisk (wydział, oddział)?

Miejsce na odpowiedź: jak 11e

       iv. jaka jest podległość merytoryczna (pod kierownikiem jednostki, kierownikiem komórki organizacyjnej)?

Miejsce na odpowiedź: jak 11e

    b. Ochrona danych osobowych (np. ABI i z-cy ABI oraz ewentualny personel wspierający pracę ABI),
       i. proszę o wskazanie stanowisk,

Miejsce na odpowiedź: ABI

ii. proszę o wymienienie podstawowych zadań w ramach SZBI wskazanych stanowisk?

Miejsce na odpowiedź: (w odniesieniu do wymienionych stanowisk) **Zadaniem ABI jest zapewnianie przestrzegania przepisów o ochronie danych osobowych** (zgodnie z art. 36a ust. 2 pkt 1 u.o.d.o.), w szczególności przez:

1. **sprawdzanie zgodności przetwarzania danych osobowych** z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie **sprawozdania dla administratora danych**,
2. **nadzorowanie opracowania i aktualizowania dokumentacji** opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzegania zasad w niej określonych,
3. **zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych** z przepisami o ochronie danych osobowych.

iii. jakie umiejscowienie w strukturze organizacyjnej jednostki wskazanych stanowisk (wydział, oddział)?

Miejsce na odpowiedź: samodzielna komórka organizacyjna ABI

iv. jaka jest podległość merytoryczna (pod kierownikiem jednostki, kierownikiem komórki organizacyjnej)?

Miejsce na odpowiedź: Prezydent Miasta

c. Informacje niejawne (np. pełnomocnik ds. ochrony informacji niejawnych oraz inspektor bezpieczeństwa teleinformatycznego),
   i. proszę o wskazanie stanowisk,

Miejsce na odpowiedź: pełnomocnik ds. ochrony informacji niejawnych, inspektor bezpieczeństwa teleinformatycznego, administrator systemu

ii. proszę o wymienienie podstawowych zadań w ramach SZBI wskazanych stanowisk,

zadania pełnomocnika o.i.n. - art. 15 ust. 1 pkt 2 ustawy o ochronie informacji niejawnych "zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne"
zadania inspektora b.t.
1. Kontrola przestrzegania realizacji procedur bezpiecznej eksploatacji systemów do przetwarzania informacji niejawnych, zwłaszcza przez personel teleinformatyczno-techniczny.
2. Organizowanie i prowadzenie szkoleń z zakresu bezpieczeństwa przetwarzania informacji niejawnych.
3. Monitorowanie zmian w funkcjonowaniu mechanizmów zabezpieczeń systemów do przetwarzania informacji niejawnych.
4. Reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn, okresowe przeglądanie i dokumentowanie logów systemowych systemów do przetwarzania informacji niejawnych.
5. Przeprowadzanie okresowej analizy zagrożeń.
6. Tworzenie planów awaryjnych i organizowanie treningów w ich realizacji.
7. Uczestnictwo w pracach zespołu opracowującego dokumenty szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji systemów do przetwarzania informacji niejawnych.
8. Opracowywanie instrukcji dla podległych pracowników.

9. Informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu lub sieci teleinformatycznych do przetwarzania informacji niejawnych.
10. Prowadzenie dziennika inspektora bezpieczeństwa teleinformatycznego.

Zadania administratora systemu

1.przydzielanie i odbieranie użytkownikom kont w systemach do przetwarzania informacji niejawnych na polecenie gestora systemu,
2.przydzielanie pierwszych haseł, z możliwością zmiany przez użytkowników na ich własne po pierwszym zalogowaniu się do systemu,
3.szkolenie użytkowników, konfigurowanie urządzeń i oprogramowania, monitorowanie zmian, przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie – tzw. logów systemowych w komputerach do przetwarzania informacji niejawnych,
4. reagowanie na sygnały o incydentach w zakresie bezpieczeństwa i usuwanie ich skutków,
5. prowadzenie ewidencji sprzętu do przetwarzania informacji niejawnych, oprogramowania i nośników danych zawierających informacje niejawne,
6. tworzenie kopii bezpieczeństwa systemów do przetwarzania informacji niejawnych,
7. uczestnictwo w pracach zespołu opracowującego dokumenty szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji systemów do przetwarzania informacji niejawnych,
8. informowanie przełożonych i inspektora bezpieczeństwa teleinformatycznego o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem systemu lub sieci teleinformatycznych do przetwarzania informacji niejawnych,
9. prowadzenie dziennika administratora.

iii. jakie umiejscowienie w strukturze organizacyjnej jednostki wskazanych stanowisk (wydział, oddział)?

Miejsce na odpowiedź: pełnomocnik o.i.n., inspektor b.t.: Biuro ds. Ochrony Informacji Niejawnych, administrator systemu: Wydział Informatyki

iv. jaka jest podległość merytoryczna (pod kierownikiem jednostki, kierownikiem komórki organizacyjnej)?

Miejsce na odpowiedź: pełnomocnik o.i.n. zgodnie z ustawą podlega bezpośrednio kierownikowi jednostki organizacyjnej

d. Informacja publiczna (np. koordynator udostępniania informacji publicznej)
   i. proszę o wskazanie stanowisk,

Miejsce na odpowiedź: w skład Urzędu Miasta Szczecin jako samodzielna jednostka organizacyjna wchodzi Biuro Informacji Publicznej (§ 12 ust. 2 pkt 5 Regulaminu Organizacyjnego Urzędu Miasta Szczecin stanowiącym Załącznik do Zarządzenia Prezydenta Miasta Szczecin Nr 417/15 z dnia 27.11.2016 r. w sprawie Regulaminu Organizacyjnego Urzędu Miasta Szczecin ze zm.).

ii. proszę o wymienienie podstawowych zadań w ramach SZBI wskazanych stanowisk?

Miejsce na odpowiedź: pracownicy BIP nie realizują zadań w ramach SZBI.

iii. jakie umiejscowienie w strukturze organizacyjnej jednostki wskazanych stanowisk (wydział, oddział)?

Miejsce na odpowiedź: samodzielna komórka organizacyjna: BIP jest wyodrębnioną organizacyjnie jednostką Urzędu, biurem na prawach referatu (§ 12 ust. 2 pkt 5 Regulaminu Organizacyjnego Urzędu Miasta Szczecin stanowiącym Załącznik do Zarządzenia Prezydenta Miasta Szczecin Nr 417/15 z dnia 27.11.2016 r. w sprawie Regulaminu Organizacyjnego Urzędu Miasta Szczecin ze zm.).

iv. jaka jest podległość merytoryczna (pod kierownikiem jednostki, kierownikiem komórki organizacyjnej)?

Miejsce na odpowiedź: Na podstawie § 3 pkt 6 Zarządzenia nr 410/16 Prezydenta Miasta Szczecin z dnia 31 października 2016 r. w sprawie podziału zadań i kompetencji oraz powierzenia prowadzenia określonych spraw Gminy Miasto Szczecin w imieniu Prezydenta Miasta Szczecin, Sekretarzowi Miasta powierzono nadzór w zakresie udostępniania informacji publicznej.

e. Zagadnienia techniczne (np. informatycy – zabezpieczenia teleinformatyczne oraz pracownicy techniczni – zabezpieczenia fizyczne, których podstawowym obowiązkiem jest zabezpieczanie zasobów informacyjnych jednostki)
   i. proszę o wskazanie stanowisk,

Miejsce na odpowiedź: administratorzy sieci, administratorzy baz danych, administratorzy systemów użytkowych Dyrektor oraz administratorzy Wydziału Informatyki

ii. proszę o wymienienie podstawowych zadań w ramach SZBI wskazanych stanowisk?

Miejsce na odpowiedź: (w odniesieniu do wymienionych stanowisk)

Zadania pielęgnacyjne:
-kontrola wykorzystania zasobów
-archiwizacja systemu plików
-kontrola zajętości przestrzeni dyskowej
-kontrola atrybutów związanych z utrzymaniem bezpieczeństwa systemu
-podejmowanie działań dla utrzymania pożądanego poziomu bezpieczeństwa

Obsługa żądań użytkowników:
-zakładanie i usuwanie kont użytkowników
-ustalenie zezwoleń na korzystanie z wyróżnionych zasobów systemu
-odblokowywanie kont
-powiadamianie użytkowników o zmianach w systemie
-przydzielanie adresów IP, oraz nadzór nad współpracą użytkownika z siecią

Zadania wynikające z potrzeb bieżących:
-uruchamianie i zatrzymywanie systemu
-usuwanie zablokowanych procesów

Usuwanie awarii:
-usuwanie drobnych awarii sprzętu sieciowego
-diagnozowanie poważniejszych awarii przed przekazaniem do serwisu
-usuwanie przyczyn awarii sieci
-rekonstrukcja systemu plików

Działania w ramach ochrony systemu:
-zarządzanie hasłami
-ochrona plików systemowych
-ochrona katalogów systemowych
-ochrona przed wszelkimi zagrożeniami powodowanymi własnymi mechanizmami
Systemowymi

Inne zadania:
-współpraca z Webmasterem w zakresie utrzymania strony internetowej na serwerze
-współpraca z administratorem Firewall'a i serwera VPN w zakresie bezpieczeństwa sieci oraz zarządzania użytkownikami
-kierowanie komisją przetargowa d/s zakupów sprzętu komputerowego
-pomoc w kontaktach z zewnętrznymi firmami w/s napraw gwarancyjnych
-kontrola legalności zainstalowanych systemów operacyjnych i innego oprogramowania

iii. jakie umiejscowienie w strukturze organizacyjnej jednostki wskazanych stanowisk (wydział, oddział)?

Miejsce na odpowiedź: komórka organizacyjna Wydziału Informatyki

iv. jaka jest podległość merytoryczna (pod kierownikiem jednostki, kierownikiem komórki organizacyjnej)

Miejsce na odpowiedź: Sekretarz Miasta