Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych

Czy wszystko jest jasne ???

Janusz Czauderna
Tel. 505 328 100
jczauderna@volvox.pl

Podstawy prawne

- 15 grudnia 2015 roku
- W wytycznych uwzględniono:
- Ustawę o informatyzacji
- Rozporządzenie Rady Ministra z dnia 12.04.2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
- **Ustawę z dnia 15.07.2011 o kontroli w administracji rządowej**
- Standardy kontroli rządowej [1]

Cel dokumentu

- Wskazanie jednolitych kryteriów merytorycznych realizacji obowiązku dotyczącego przeprowadzania kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych albo realizacji **obowiązku wynikającego z art.13 ust2. ustawy o informatyzacji**

- **interoperacyjność** – zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych. Osiąganie interoperacyjności następuje poprzez ciągłe doskonalenie w zakresie współdziałania systemów teleinformatycznych;

Słownik .....

Kto może prowadzić kontrolę:

- w jednostkach samorządu terytorialnego i ich związkach oraz w tworzonych lub prowadzonych przez te **jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych** – właściwy wojewoda,
- w podmiotach publicznych podległych lub nadzorowanych przez organy administracji rządowej – organ administracji rządowej nadzorujący dany podmiot publiczny,
- w podmiotach publicznych niewymienionych w lit. a i b – minister właściwy do spraw informatyzacji.

Kontrola

Obszary kontroli

» Kontrola powinna objąć następujące **3 główne obszary:**

1. Wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami/rejestrami informatycznymi i wspomagania świadczenia usług drogą elektroniczną. **(interoperacyjność)**

2. Zarządzania bezpieczeństwem informacji w systemach teleinformatycznych. **(SZBI)**

3. Zapewnienia dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych. **(WCGA 2.0)**

Konstrukcja wytycznych:

- Opis przedmioty wymagania kontrolnego
- Zakres kontroli on-site
- Wymagania dowodowe dla każdego wymagania

Obszary kontroli

» W celu przygotowania kontroli zaleca się pozyskanie:

- Dokumentów ustanawiających SZBI : polityki, instrukcje, procedury;

- Dokumentacji analizy ryzyka związanego z BI;

- Dokumentacji przeglądów SZBI;

- Dokumentacji audytów wewnętrznych SZBI.

- Dokumentacji systemu zarządzania jakością usług świadczonych przez system teleinformatyczny

- **załącznik nr 1 i 2 do wytycznych**

Przygotowanie kontroli

CEL główny kontroli :

» **Legalność –** zgodność z prawem powszechnie obowiązującym oraz regulacjami wewnętrznymi dotyczącymi SZBI **w trzech obszarach kontroli**

Kryteria kontroli

- ocenę pozytywną
- ocenę pozytywną z uchybieniami
- ocenę pozytywną z nieprawidłowościami
- ocena negatywna

Kryterium oceny

Kryterium oceny negatywnej

- Ocena negatywna w obszarze 1
- Ocena negatywna w obszarze 2
- Ocena negatywna w obszarze 3

Ocena w obszarach 1 i 2 powinna być uzupełniona odpowiednio opisem poziomu/stopnia uzyskania interoperacyjności oraz opisem względnego poziomu zapewnienia BI, a także opisem stopnia osiągnięcia przez jednostkę podejścia systemowego do BI.

Poziomem odniesienia dla danego systemu są wyniki analizy ryzyka uwzględniającej takie czynniki jak m.in. skala i zakres stosowania danego systemu teleinformatycznego, ważność przetwarzanych w nim danych i które mają bezpośrednie odzwierciedlenie w planie postępowania z ryzykiem.

1. Przeprowadzić **AUDYT** stanu zastanego w organizacji najlepiej etapowo: a) urząd , b) jednostki organizacyjne
   - = badając in-site Najwyższe Kierownictwo
   - = badając on-site kierowników i próbę kadrową
   - = badając on-site pion IT
   - = badając stan dokumentacji
   - = przeprowadzając zestaw testów penetracyjnych

1. Na podstawie **raportu audytowego** wprowadzić działania naprawcze, korygujące
2. Przygotować **załącznik nr 1 i załącznik nr 2**

Co w tej sytuacji zrobić?

1.0 Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.	
1.1.1 Usługi elektroniczne	
Ustawa o informatyzacji, art.16 ust. 1a	Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę
Norma PN ISO 27001:2014-12	A.18.1.1 Określenie stosownych wymagań prawnych i umownych
Opis realizacji:	• Czy podmiot publiczny udostępnia elektroniczną skrzynkę podawczą (ESP)? Podać adres ?(•!) 1. Czy adres ESP wskazuje bramkę ESP.2 2. Czy został określony magazyn umożliwiający gromadzenie dokumentów elektronicznych, przyjmowanie i wysyłanie dokumentów elektronicznych ?
Dowody:	1. Wydruk strony internetowej, na której jest ESP. 2. 3.
Uwagi – ewentualne przyczyny braku realizacji	
Ocena:	

Przygotowanie kontroli- audyt

Osiągniecie zgodności poprzez:

- Znajomość wymagań kontroli
- Realizacja zadań prawnych

jako potwierdzenie

Legalności – czyli stwierdzenia zgodności z prawem powszechnie obowiązującym oraz regulacjami wewnętrznymi dotyczącymi SZBI (**w trzech obszarach kontroli)**

Osiągnięcie zgodności

Ankieta
dotycząca działania systemów teleinformatycznych używanych do realizacji zadań publicznych

Poz.	Obszar / Obszar szczegółowy / Wymaganie	Podstawa prawna	Kontroli podlegają	Dokumenty potwierdzające spełnienie wymagania*)	Uwagi i wyjaśnienia*)	Samoocena spełnienia wymagania*) S/N/CS/ND	Komórka i osoba udzielająca odpowiedzi*	nr telefonu do osoby udzielającej odpowiedzi*)
1	2	3	4	5	6	7	8	
1	**Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną**							
1.1	**Usługi elektroniczne**							
1.1.1	Czy Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę? Czy interoperacyjność na poziomie organizacyjnym osiągana jest przez: - informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty, - publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną?	*art. 16 ust. 1a ustawy o informatyzacji* *§5 ust. 2 pkt 1 rozporządzenia KRI* *§ 5 ust. 2 pkt 4 rozporządzenia KRI*	• Świadczenie usług w formie elektronicznej z wykorzystaniem ESP • Zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP podmiotu), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw.					
1.2	**Centralne repozytorium wzorów dokumentów elektronicznych**							

Załącznik nr 1

Zestawienie systemów teleinformatycznych używanych do realizacji zadań publicznych

Lp.	Nazwa systemu	Rejestr publiczny	Cel stosowania	Główne funkcje	Przedmiotowy zakres stosowania	Podmiotowy zakres stosowania	Skala systemu	Powiązania z innymi systemami	Krytyczność dla organizacji	Warstwa techniczna	Właściciel	Administrator	Producent	Umowy serwisowe	Termin uruchomienia produkcyjnego	Terminy istotnych zmian
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1																
2																
3																

Opisy kolumn zestawiania:

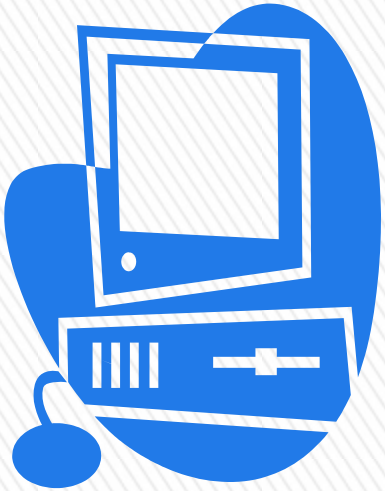
1. Nazwa systemu
2. Rejestr publiczny – czy system teleinformatyczny jest rejestrem publicznym? jeżeli tak, proszę o podanie podstawy prawnej prowadzenia rejestru publicznego
3. Cel stosowania
4. Główne funkcje użytkowe – jakie główne funkcje użytkowe realizuje system
5. Przedmiotowy zakres stosowania - jakie dane i informacje system przetwarza
6. Podmiotowy zakres stosowania – kto jest użytkownikiem systemu (wewnętrznym, zewnętrznym, ilu jest użytkowników)
7. Skala systemu – jaki jest zasięg terytorialny systemu (lokalny, krajowy, międzynarodowy)
8. Powiązania z innymi systemami - jakie dane system przekazuje do innych systemów i do których, jakie dane pobiera z innych systemów i z których

Załącznik nr 2

Osiągnięcie interoperacyjności

- **Osiąganie interoperacyjności jest procesem ciągłym, wymagającym przeprowadzania analizy aktualnego stanu i podejmowania decyzji, co do działań zmierzających do poszerzania jej zakresu.**
- Kontrola powinna :

- określić i ocenić aktualny stan interoperacyjności urzędu,
- ocenić skuteczność procesu osiągania interoperacyjności w obszarach, w których nie jest ona w pełni osiągnięta.



» Świadczone wg jednolitych, standardowych procedur, jasno komunikowanych obywatelowi/podmiotowi

» CEL stosowania: -ułatwienie w dostępie do usług poprzez:

- wyeliminowanie korespondencji papierowej obywatela/podmiotu z urzędem,
- zastąpienie druków i formularzy papierowych ich odpowiednikami elektronicznymi dostępnymi do wypełnienia na platformie usług elektronicznych urzędu,
- wyeliminowanie papierowych dokumentów kierowanych do obywatela/podmiotu i zastąpienie ich odpowiednikami elektronicznymi przesyłanymi na adres elektroniczny

Usługi elektroniczne

» KONTROLA:

- Świadczenie usług w formie elektronicznej z wykorzystaniem ESP, w tym udostępnionej na platformie ePUAP,

» DOWODY:

- Dokumentacja usług elektronicznych podmiotu publicznego, w tym: lista usług świadczonych w formie elektronicznej, dokumentacja (wydruki) stron internetowych, itp.

Usługi elektroniczne

Centralne repozytorium wzorów dokumentów elektronicznych

- Uruchomienie przez podmiot publiczny usługi elektronicznej, gdy usługa funkcjonuje na koncie innego podmiotu- dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych z CRWDE.
- Uruchomienie usługi, dla której nie ma wzorów dokumentów w CRWDE- podmiot zobowiązany jest do przekazania do CRWDE procedury obsługi i wzory dokumentów elektronicznych z nią związanych.

Centralne repozytorium wzorów dokumentów elektronicznych

» KONTROLA:

- Wykorzystanie wzorów dokumentów elektronicznych z CRWDE
- Przekazanie CRWDE oraz udostepnienie w BIP wzorów dokumentów elektronicznych podmiotu publicznego

» DOWODY:

- Dokumentacja związana z wykorzystaniem przez podmiot publiczny wzorów dokumentów elektronicznych przechowywanych w CRWDE
- Wnioski przekazania wzorów dokumentów elektronicznych do CRWDE *art. 19b ust. 3 ustawy o informatyzacji.*

» To model, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji (inaczej: system zorientowany na usługi). *§ 2 pkt 8 rozporządzenia KRI*

Model usługowy

» KONTROLA:

- Poziom wspierania modelu usługowego
- Weryfikacja sposobu zarządzania usługami w oparciu o ustalone procedury
- Ustalenie odpowiedzialności za utrzymanie usług
- Określenie poziomu świadczenia usług
- Monitorowanie poziomu świadczenia usług

» DOWODY:

- Dokumentacja usług elektronicznych świadczonych przez podmiot publiczny [1]

Model usługowy

Współpraca systemów teleinformatycznych z innymi systemami

- Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.
- Aby możliwa była współpraca pomiędzy systemami urzędów dany system powinien być wyposażony w odpowiednie składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI.

» KONTROLA:

- Poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrami referencyjnymi
- Sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami

» DOWODY:

- Umowy z podmiotami prowadzącymi rejestry referencyjne
- Opis interfejsów systemu teleinformatycznego
- Dokumentacja systemu teleinformatycznego

Współpraca systemów teleinformatycznych z innymi systemami

- Celem wdrożenia systemu elektronicznego zarządzania dokumentacją jest wyeliminowanie z obiegu wewnętrznego podmiotu publicznego dokumentów papierowych, co spowoduje dodatkowo obniżenie kosztów związanych ze zużyciem papieru.
- Stosowanie systemu elektronicznego zarządzania dokumentami elektronicznymi :

- Uporządkowanie i usprawnienie przepływu dokumentów,
- Usprawnienie archiwizacji dokumentów ,
- Ułatwienie dostępu do dokumentów archiwalnych

Obieg dokumentów w podmiocie publicznym

» KONTROLA:

- Regulacje wewnętrzne opisujące sposób zarządzania dokumentacją w kontrolowanym podmiocie

» DOWODY:

- Dokumentacja systemu zarządzania dokumentacją-procedury i zasady postępowania z dokumentami [1]

Obieg dokumentów w podmiocie publicznym

» KONTROLA:

- Sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu publicznego
- Sposób udostępniania zasobów informatycznych z systemów teleinformatycznych podmiotu publicznego
- Sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne podmiotu publicznego

» DOWODY:

- Opis formatów danych w systemach podmiotu publicznego
- Dokumentacja systemu teleinformatycznego

Formaty danych udostępniane przez systemy teleinformatyczne

System zarządzania bezpieczeństwem informacji (SZBI)

- Ważne zapewnienie: dostępności, integralności, poufności danych posiadanych i przetwarzanych
- SZBI odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia BI. SZBI zawiera strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby [1]

» DOWODY:

- Polityka bezpieczeństwa teleinformatycznego;
- Polityka bezpieczeństwa fizycznego;
- Polityka bezpieczeństwa danych osobowych.
- Procedura zarzadzania ryzykiem;
- Regulamin korzystania z zasobów informatycznych;
- Procedura zarządzania sprzętem i oprogramowaniem;
- Procedura zarządzania konfiguracją;
- Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Procedura monitorowania poziomu świadczenia usług;
- Procedura bezpiecznej utylizacji sprzętu elektronicznego;
- Procedura zarządzania zmianami i wykonywaniem testów;
- Procedura stosowania środków kryptograficznych;
- Procedura określania specyfikacji technicznych wymagań odbioru systemów IT;
- Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji;
- Procedura wykonywania i testowania kopii bezpieczeństwa;
- Procedura monitoringu i kontroli dostępu do zasobów teleinformatycznych, prowadzenia logów systemowych.
- Dokumentacja z przeglądów SZBI;
- Dokumentacja z szacowania ryzyka BI;
- Dokumentacja postępowania z ryzykiem;
- Dokumentacja akceptacji ryzyka;
- Dokumentacja audytów z zakresu BI;
- Dokumentacja incydentów naruszenia BI;
- Dokumentacja zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
- Dokumentacja zarządzania sprzętem i oprogramowaniem teleinformatycznym;
- Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Dokumentacja SZBI

» Kontrola SZBI powinna wykazać, że SZBI jest:

- Ustanowiony,
- Kompletny,
- Działający w praktyce

» KONTROLA:

- Dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI, Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI
- Działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI
- Stopień zaangażowania kierownictwa podmiotu publicznego w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI

» DOWODY: Dokumentacja : SZBI w tym polityka BI oraz inne stanowiące SZBI, z przeglądów SZBI, z audytów z zakresu BI, zmian wynikających z wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI.

System zarządzania bezpieczeństwem informacji (SZBI)

» Zarządzanie ryzykiem:
- Identyfikacja ryzyka,
- Ocena ryzyka
- Sposób postępowania z ryzykiem

» Plan postępowania z ryzykiem jest podstawowym dokumentem wykonawczym do podejmowania wszelkich działań minimalizujących ryzyko stosownie do przeprowadzonej analizy. Po zastosowaniu zabezpieczeń wynikających z planu postępowania z ryzykiem pozostaje ryzyko szczątkowe podlegające akceptacji przez kierownictwo

Analiza ryzyka

» KONTROLA:

- Regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w urzędzie;

- Dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem,

- Działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka

» DOWODY:

- procedura przeprowadzania analizy ryzyka,
- rejestr ryzyk,
- plan postępowania z ryzykiem,
- dowody utrzymywania i doskonalenia systemu zarządzania ryzykiem,
- dokumentacja zmian w zabezpieczeniach związanych z bieżącą analizą ryzyka.

Analiza ryzyka

» KONTROLA:

- Regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych (bazą konfiguracji CMDB);
- Rejestr zasobów teleinformatycznych (baza konfiguracji CMDB) zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych,
- Sposób aktualizacji rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB).

» DOWODY:

- Dokumentacja zarządzania sprzętem i oprogramowaniem

Inwentaryzacja sprzętu i oprogramowania informatycznego

» KONTROLA:

- Regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych;

- Adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień),

- Działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.;

- Sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych,

» DOWODY:

- Dokumentacja zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym procedury nadawania, zmiany i odbierania uprawnień do pracy w systemach teleinformatycznych i dokumentacja wykonywania ww. procedur.

Zarządzanie uprawnieniami

» KONTROLA:

- Regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych;
- Dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń,

» DOWODY: Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji, w tym: programy szkoleń i listy uczestników.

Szkolenia pracowników

» KONTROLA:

- Regulacje wewnętrzne zawierające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość,
- Działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość.

» DOWODY: Dokumentacja dotycząca zarządzania urządzeniami przenośnymi i pracą na odległość

Praca na odległość i mobilne przetwarzanie danych

» KONTROLA:

- Regulacje wewnętrzne, w których określono zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym wymagane klauzule prawne dotyczące BI;

- Umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI,

» DOWODY: Zapisy umów serwisowych oraz umów dotyczących rozwoju systemów teleinformatycznych.

Serwis sprzętu informatycznego i oprogramowania

» KONTROLA:

- Regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji.

- Sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL

» DOWODY: Dokumentacja postępowania z incydentami naruszenia BI w tym rejestr incydentów naruszenia BI, procedury zgłaszania i postępowania z incydentami, dokumentacja wykonywania ww. procedur [1]

Procedury zgłaszania incydentów naruszenia BI

» KONTROLA:

- Regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;

- Sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji

- Działania podjęte w wyniku zaleceń poaudytowych.

» DOWODY: Dokumentacja audytów z zakresu BI. Dokumentacja realizacji zaleceń poaudytowych. [1]

» `

Audyt wewnętrzny z zakresu bezpieczeństwa informacji

» KONTROLA:

- Regulacje wewnętrzne, w których określono zasady tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu publicznego,
- Działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja tych działań.

» DOWODY: Dokumentacja wykonywania kopii zapasowych w tym: procedury wykonywania, przechowywania i testowania kopii zapasowych oraz dokumentacja wykonywania ww. procedur. [1]

Kopie zapasowe

» KONTROLA:

- Zapewnienie warunków dla uzyskania odpowiedniej funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności systemów informatycznych w fazie ich projektowania, wdrażania i eksploatacji,

- Regulacje wewnętrzne opisujące wymagania w zakresie projektowania systemów teleinformatycznych w urzędzie dotyczące architektury systemu, sposób licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. ustawą *o informatyzacji)*, sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągnięcia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu;

- Regulacje wewnętrzne opisujące wymagania w zakresie wdrażania systemów teleinformatycznych w urzędzie dotyczące: sposobu dostarczenia i instalacji systemu teleinformatycznego, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji a także warunków i kryteriów odbioru;

- Regulacje wewnętrzne opisujące sposób przeprowadzania zmian w systemach teleinformatycznych (w trakcie ich eksploatacji) w tym opis: sposobu zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany;

- Regulacje wewnętrzne opisujące proces monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanych wobec wzrostu ilości systemów teleinformatycznych, ilości przetwarzanych danych, ilości użytkowników poprzez podejmowanie działań zapobiegawczych;

- Działania związane z wdrażaniem nowych systemów teleinformatycznych oraz wprowadzaniem zmian w systemach eksploatowanych;

- Działania związane z **monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności;**

- Działania zapobiegawcze będące wynikiem dostrzeżonych problemów podczas monitorowania ich pracy.

» DOWODY**:** Dokumentacja wdrożeń nowych systemów teleinformatycznych, dokumentacja wprowadzanych zmian w systemach eksploatowanych, dokumentacja monitorowania systemów teleinformatycznych oraz działań zapobiegawczych będących wynikiem dostrzeżonych problemów podczas monitorowania

Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

» KONTROLA:

Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem,

- Regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie,

- Działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związane z monitorowaniem ruchu osobowego w urzędzie,

- Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia BI,

- Działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem,

- Działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, zgodne z wynikami analizy ryzyka i planem postępowania z ryzykiem;

- Działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI.

» DOWODY: Dokumenty wprowadzające stosowanie zabezpieczeń, dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń, dokumentacja wykonywania ww. procedur. [1]

Zabezpieczenia techniczno-organizacyjne dostępu do informacji

» KONTROLA:

- Regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem,

- Działania związane z aktualizacją oprogramowania oraz redukcją ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem;

- Działania związane z minimalizowaniem ryzyka utraty informacji w wyniku awarii oraz ochroną przed błędami, utratą i nieuprawnioną modyfikacją a także zapewnienie bezpieczeństwa plików systemowych poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych, w tym np.: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia (ang. load balancing), monitorowania parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem;

- Działania związane z zastosowaniem mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa poprzez stosowanie zabezpieczeń kryptograficznych np.: dla transmisji do urządzeń mobilnych, poczty elektronicznej, a także podpisów kwalifikowanych do autoryzacji dokumentów zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem;

- Działania podejmowane w związku z dostrzeżeniem nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;

- Działania związane z kontrolą zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

» DOWODY: plan postępowania z ryzykiem, dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń i dokumentacja wykonywania ww. procedur. [1]

Zabezpieczenia techniczno-organizacyjne systemów informatycznych

» KONTROLA:

- Regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych,

- Działania związane z zapewnieniem rozliczalności użytkowników, szczególnie posiadających uprawnienia: administrowania systemami użytkowymi, zmiany konfiguracji systemów operacyjnych i ich zabezpieczeń, przetwarzania danych podlegających prawnej ochronie;

- Działania związane z zapewnieniem rozliczalności działań użytkowników lub obiektów systemowych a także rejestracji innych zdarzeń systemowych w zakresie wynikającym z analizy ryzyka;

- Działania związane z regularnym przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych;

- Okres i sposób przechowywania dzienników systemowych

» DOWODY: Dokumenty zawierające analizę ryzyka, dokumentacja dzienników systemowych, w tym: procedury prowadzenia i dostępu do dzienników systemowych oraz dokumentacja wykonywania ww. procedur.

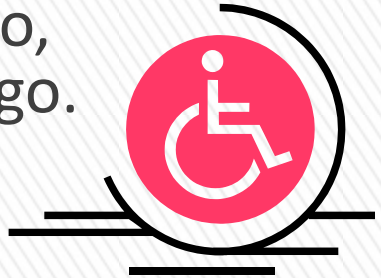
Rozliczalność działań w systemach informatycznych

» KONTROLA:

- Sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu publicznego

DOWODY:

Opis zastosowanych rozwiązań technicznych umożliwiających osobom niedosłyszącym lub niedowidzącym zapoznanie się z treścią informacji na stronach internetowych systemów teleinformatycznych podmiotu publicznego, dokumentacja systemu teleinformatycznego. Wyniki z przeprowadzonych testów razem z ich interpretacją.



Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

Dziękuję za uwagę