Kwestionariusz
dotyczący działania systemów teleinformatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej

Poz.	Obszar / Zagadnienie	Podstawa prawna	Odpowiedź*			Uwagi
			T	N	ND	
1	*2*	*3*	*4*			*5*
1.	**Projektowanie, wdrażanie i eksploatacja systemu teleinformatycznego**					
a	Czy system teleinformatyczny został zaprojektowany, wdrożony i eksploatowany z uwzględnieniem jego **funkcjonalności** przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk? *Funkcjonalność rozumiana jako zdolność do zapewnienia funkcji odpowiadających zdefiniowanym i przewidywanym potrzebom, gdy oprogramowanie jest używane w określonych warunkach.* *Bibliografia:ISO 9126*	*par. 15 ust. 1 rozporządzenia* ***W przypadku systemów centralnych tylko w zakresie eksploatacji***				
b	Czy system teleinformatyczny został zaprojektowany, wdrożony i eksploatowany z uwzględnieniem jego **niezawodności** przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk? *Niezawodność rozumiana jako zdolność do wykonywania wymaganych funkcji w określonych warunkach przez określony czas lub dla określonej liczby operacji.* *Bibliografia:ISO 9126*	*par. 15 ust. 1 rozporządzenia* ***W przypadku systemów centralnych tylko w zakresie eksploatacji***				
c	Czy system teleinformatyczny został zaprojektowany, wdrożony i eksploatowany z uwzględnieniem jego **używalności** przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk? *Używalność rozumiana jako zdolność do bycia używanym, zrozumiałym, łatwym w nauce i atrakcyjnym dla użytkownika, gdy system jest używany w określonych warunkach.* *Bibliografia:ISO 9126*	*par. 15 ust. 1 rozporządzenia* ***W przypadku systemów centralnych tylko w zakresie eksploatacji***				
d	Czy system teleinformatyczny został zaprojektowany, wdrożony i eksploatowany z uwzględnieniem jego **wydajności** przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk? *Wydajność rozumiana jako stopień, w jaki system lub moduł realizuje swoje wyznaczone funkcje w założonych ramach czasu przetwarzania i przepustowości.* *Wg:IEEE 610*	*par. 15 ust. 1 rozporządzenia* ***W przypadku systemów centralnych tylko w zakresie eksploatacji***				
e	Czy system teleinformatyczny został zaprojektowany, wdrożony i eksploatowany z uwzględnieniem jego **przenoszalności i pielęgnowalności** przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk? *Przenaszalność rozumiana jako łatwość z jaką system lub moduł może być przeniesiony z jednego środowiska sprzętowego lub programowego do innego środowiska.* *Bibliografia:ISO 9126* *Pielęgnowalność rozumiana jako łatwość, z którą system lub moduł może być modyfikowane w celu naprawy defektów, dostosowania do nowych wymagań, modyfikowane w celu ułatwienia przyszłego utrzymania lub dostosowania do zmian zachodzących w jego środowisku.* *Bibliografia:ISO 9126*	*par. 15 ust. 1 rozporządzenia* ***W przypadku systemów centralnych tylko w zakresie eksploatacji***				
2.	**Zarządzanie usługami realizowanymi przez systemy teleinformatyczne**					
a	Czy ustalono deklarowany poziom dostępności usług?	*par. 15 ust. 2 rozporządzenia*				

Poz.	Obszar / Zagadnienie	Podstawa prawna	Odpowiedź*			Uwagi
			T	N	ND	
1	*2*	*3*		*4*		*5*
b	Czy deklarowany poziom dostępności usług jest dochowany? *Pojęcie dostępności oznacza czas bezawaryjnego działania usługi w stosunku do całości czasu, w którym usługa ta powinna być klientom świadczona. Dostępność 90% znaczy więc, że na 100 jednostek czasu 90 przypadło na czas, w którym system działał bezawaryjnie. Pozostałe 10 jednostek to czas, w którym system był w stanie awarii bądź odzyskiwania pełnej funkcjonalności po niej.*	*par. 15 ust. 2 rozporządzenia*				
c	Czy zarządzanie usługami jest dokonywane w oparciu o ustalone procedury?	*par. 15 ust. 2 rozporządzenia*				
3.	**Wymogi WCAG 2.0**					
a	Czy system teleinformatyczny spełnienia wymagania Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia? *Należy wypełnić, jeżeli system ma "Front Office" dla klienta zewnętrznego - np. moduł Internetowy*	*par. 19 rozporządzenia*				
4.	**System zarządzania bezpieczeństwem informacji**					
a	Czy opracowano, ustanowiono i wdrożono system zarządzania bezpieczeństwem informacji?	*par. 20 ust. 1 rozporządzenia*				
aa	decyzja o wdrożeniu SZBI					
ab	polityka bezpieczeństwa informacji					
ac	inne procedury					
ad	aktualizacja polityki, procedur, innych dokumentów	*par. 20 ust. 2 pkt 1 rozporządzenia*				
b	Czy system zarządzania bezpieczeństwem informacji jest monitorowany, poddawany przeglądom oraz doskonalony?	*par. 20 ust. 1 rozporządzenia*				
ba	audyt / audit wewnętrzny co najmniej raz w roku	*par. 20 ust. 2 pkt 14 rozporządzenia*				
bb	okresowa samoocena / ocena systemu					
c	Czy dokonano inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację?	*par. 20 ust. 2 pkt 2 rozporządzenia*				
d	Czy wykaz sprzętu i oprogramowania jest aktualizowany? Jak często?	*par. 20 ust. 2 pkt 2 rozporządzenia*				
e	Czy wdrożono zarządzanie ryzykiem utraty integralności, dostępności lub poufności informacji?	*par. 20 ust. 2 pkt 3 rozporządzenia*				
f	Czy podejmowane są działania minimalizujące ryzyko, stosownie do wyników analizy ryzyka? *Czynności zapisane w Planach działania, dokumentacji zarządzania ryzykiem minimalizujące naruszenia bezpieczeństwa IT w organizacji (np. procedury reagowania na incydenty IT)*	*par. 20 ust. 2 pkt 3 rozporządzenia*				
g	Czy osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia? *Uprawnienia wynikające z: zakresu obowiązków, nadanych uprawnień, upoważnień.*	*par. 20 ust. 2 pkt 4 rozporządzenia*				
h	Czy osoby zaangażowane w proces przetwarzania informacji uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji?	*par. 20 ust. 2 pkt 4 rozporządzenia*				
i	Czy zakres uprawnień osób zaangażowanych w przetwarzanie danych jest bezzwłocznie zmieniany, w przypadku zmiany zadań tych osób?	*par. 20 ust. 2 pkt 5 rozporządzenia*				

Poz.	Obszar / Zagadnienie	Podstawa prawna	Odpowiedź*			Uwagi
			T	N	ND	
1	*2*	*3*		*4*		*5*
j	Czy zapewniono szkolenie 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?	*par. 20 ust. 2 pkt 6 rozporządzenia*				
k	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez **monitorowanie dostępu do informacj**i?	*par. 20 ust. 2 pkt 7 rozporządzenia, par. 20 ust. 2 pkt 9 rozporządzenia, par. 20 ust. 2 pkt 12 lit. c rozporządzenia*				
l	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez **czynności zmierzające do wykrycia nieautoryzowanych działań** związanych z przetwarzaniem informacji?	*par. 20 ust. 2 pkt 7 rozporządzenia, par. 20 ust. 2 pkt 9 rozporządzenia, par. 20 ust. 2 pkt 12 lit. c rozporządzenia*				
m	Czy zapewniono ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez **zastosowanie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji**?	*par. 20 ust. 2 pkt 7 rozporządzenia, par. 20 ust. 2 pkt 9 rozporządzenia, par. 20 ust. 2 pkt 12 lit. c rozporządzenia*				
n	Czy ustanowiono podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość? *Bezpieczne metody połączenia (np. VPN) i metody uwierzytelniania*	*par. 20 ust. 2 pkt 8 rozporządzenia*				
o	Czy umowy serwisowe podpisane ze stronami trzecimi zawierają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji? *Zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu / oprogramowania* *Czy są krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system);* *Oświadczenie producenta prowadzącego support.*	*par. 20 ust. 2 pkt 10 rozporządzenia*				
p	Czy ustalono zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych?	*par. 20 ust. 2 pkt 11 rozporządzenia*				
q	Czy zapewniono aktualizację oprogramowania? *Dotyczy to zarówno oprogramowania pracującego na stacjach roboczych (np. java, flash czy adobe reader), jak również oprogramowania serwerowego*	*par. 20 ust. 2 pkt 12 rozporządzenia*				
r	Czy ustanowiono środki minimalizujące ryzyko utraty informacji w wyniku awarii? *Zapisy wynikające z Polityki zachowania ciągłości działania*	*par. 20 ust. 2 pkt 12 rozporządzenia*				

Poz.	Obszar / Zagadnienie	Podstawa prawna	Odpowiedź*			Uwagi
			T	N	ND	
1	*2*	*3*		*4*		*5*
s	Czy mechanizmy kryptograficzne są stosowane w sposób adekwatny do zagrożeń i wymogów prawa? *Stosuje się przy systemach mobilnych oraz przy przesyłaniu danych pomiędzy systemami np. poprzez Internet* *Obowiązuje tu na pewno ogólna zasada, że żadne dane wrażliwe nie powinny być przesyłane przez sieć bez odpowiedniej ochrony kryptograficznej (w szczególności podczas przesyłania ich przez Internet).*	*par. 20 ust. 2 pkt 12 rozporządzenia*				
t	Czy zapewniono bezpieczeństwo plików systemowych? *Zapewnienie odpowiednio bezpiecznego dostępu do poczty elektronicznej (dostęp tylko szyfrowany);* *Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?* *Czy dostęp do Internetu jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp);* *wydzielone konta administratora od kont użytkowników*	*par. 20 ust. 2 pkt 12 rozporządzenia*				
u	Czy zapewniono redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych? *Czy wykonywano na bieżąco aktualizację systemów operacyjnych, aplikacji, bibliotek itp. mające wpływ na bepieczeństwo*	*par. 20 ust. 2 pkt 12 rozporządzenia*				
w	Czy w razie dostrzeżenia nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa podejmowane są niezwłocznie działania? *Informacje o incydentach i reakcje na nie*	*par. 20 ust. 2 pkt 12 rozporządzenia*				
x	Czy incydenty naruszenia bezpieczeństwa informacji są bezzwłocznie zgłaszane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących? *Zapisy w Polityce bezpieczeństwa lub procedury zarządzania incydentami*	*par. 20 ust. 2 pkt 13 rozporządzenia*				
5.	**Rozliczalność**					
a	Czy rozliczalność w systemie teleinformatycznym podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach)? *Rozliczalność w rozumieniu przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz.U. Nr 93, poz.545) - właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie, np. włączone logi (test działania logów).*	*par. 21 ust. 1 rozporządzenia*				
b	Czy w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do systemu z uprawnieniami administracyjnymi?	*par. 21 ust. 2 rozporządzenia*				
ab	Czy w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do konfiguracji systemu, w tym konfiguracji zabezpieczeń?	*par. 21 ust. 2 rozporządzenia*				

Poz.	Obszar / Zagadnienie	Podstawa prawna	Odpowiedź*			Uwagi
			T	N	ND	
1	*2*	*3*	*4*			*5*
ac	Czy w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa?	*par. 21 ust. 2 rozporządzenia*				
b	Czy informacje w dziennikach systemów są przechowywane przez 2 lata od dnia ich zapisu lub przez okres wskazany w przepisach odrębnych?	*par. 21 ust. 4 rozporządzenia*				
c	Czy zapisy dzienników systemów są składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji?	*par. 21 ust. 5 rozporządzenia*				
d	W jakich przypadkach dzienniki systemów są prowadzone na nośniku papierowym? Czym jest to uzasadnione?	*par. 21 ust. 5 rozporządzenia*				

Objaśnienia dotyczące wypełniania kwestionariusza:
Proszę zaznaczyć prawidłową odpowiedź w kolumnie 4 "Odpowiedź":
T - Tak,
N - Nie,
ND - nie dotyczy.
W kolumnie 5 "Uwagi" proszę podać dodatkowe informacje, np. w przypadku niespełnienia wymagań, w przypadku spełnienia wymagań tylko przez część systemów, w celu opisania przyczyn itp.