Polskie Towarzystwo Informatyczne **Warszawa, 16 lutego 2011 r.**
Zarząd Główny

Uwagi do projektu Rozporządzenia RM w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

1.
§1 pkt 3d)
Sugerujemy użycie liczby mnogiej: „sposoby”

2.
§2 pk 1)
Słowo „podmiot” użyte w definicji aktywów jest niejednoznaczne. Z racji zakresu Rozporządzenia sugerujemy użyć „podmiot publiczny”

3.
§2 pkt 2)
„Ogół składników systemu teleinformatycznego” jest pojęciem niejasnym, sugerujemy pominięcie słowa „Ogół”.

4.
§2 pkt 9)
Sugerujemy zmianę gramatyczną:
9) nieodpłatne oprogramowanie – oprogramowanie udostępniane przez właściciela autorskich praw majątkowych na warunkach określonych przez tego właściciela, jednakże bez pobierania opłaty za ~~jego~~ użytkowanie tego oprogramowania ~~a warunkach określonych przez tego właściciela~~;

5.
§2 pkt 10)
Definicja jest nielogiczna: właściwość nie może być „brakiem”
Sugerujemy definicję z ISO/IEC 27000:2009:

“niezaprzeczalność – zdolność wykazania wystąpienia określonego zdarzenia lub przypisania działania podmiotowi, który to działania rzeczywiście wykonał, w celu rozstrzygnięcia sporu dotyczącego wystąpienia lub niewystąpienia zdarzenia lub działania oraz uczestnictwa podmiotu w zdarzeniu”

6.
§2 pkt 13)

Sugerujemy adaptację definicji z normy ISO/IEC 27000:2009:
„Podatność [systemu teleinformatycznego] – słabość aktywów [systemu teleinformatycznego] lub zabezpieczeń, która może być wykorzystana przez zagrożenie;”

7.
§2 pkt 14)
Sugerujemy konsekwentnie stosować pojecie „podmiot publiczny” tym bardziej, ze w definicjach (np. w definicji niezaprzeczalności”) pojęcie „podmiot” występuje w innym kontekście.
„podmiot publiczny” – podmiot w rozumieniu art. 2 ust. 1 ustawy;
Sugerujemy przejrzenie całości Rozporządzenia i zamianę pojęć „podmiot” oraz „podmiot realizujący zadanie publiczne” określeniem z ustawy „podmiot publiczny”.

8.
§2 pkt 16)
Repozytorium nie może być adresem internetowym. Sugerujemy zmianę definicji:
„repozytorium rekomendacji interoperacyjności –część ePUAP przeznaczona do udostępniania rekomendacji interoperacyjności pod adresem ~~internetowy~~ elektronicznym wskazującym zasoby ePUAP;”~~, pod którym udostępnia się, do zapoznania lub pobrania, rekomendacje interoperacyjności;~~

9.
§3 ust. 1
Rozporządzenie w żadnym miejscu nie odnosi się do procedur. Sugerujemy wykreślić „procedur”

10.
§3 ust. 2 pkt 1 lit e)
Literówka „publicznymi”

11.
§3 ust. 2 pkt 1 lit f)
Zdanie niegramatyczne. Sugerujemy modyfikację:

f) zapewnienie swobody gospodarczej i równego dostępu do rynku informatycznego dla wszystkich jego uczestników w zakresie przedmiotu Rozporządzenia; ~~zamówieo publicznych realizowanych przez podmioty realizujące zadania publiczne w zakresie systemów teleinformatycznych~~;

12.
§8 ust. 4
„teletransmisja” jest pojęciem nadmiarowym. Sugerujemy użycie słowa „transmisja”

13.
§10. Ust 2 i 3

a) Wprowadzenie norm ISO/IEC 20000-1 w odniesieniu do systemu teleinformatycznego jest niepoprawne. Normy serii 20000 odnoszą się do dostawcy usług IT. Z tego względu, jeśli – przykładowo – podmiot publiczny korzysta całkowicie z outsourcingu, to sam ISO/IEC 20000 nie wdraża! Warto podkreślić, że w przypadku

ISO/IEC 27001 podmiotowo właściwa jest organizacja (nasz podmiot publiczny), zatem wymagania zarządzania bezpieczeństwem można odnosić do tego podmiotu.

b) Przywoływanie normy ISO/IEC 20000-2 jako wymagania nie powinno mieć miejsca. Ta część to tylko zalecenia.
c) Nie widzimy racjonalności przywołania w ust. 2 - nie wszystkich zresztą procesów opisanych w ISO 20000-1 (przykładowo, brakuje budżetowania oraz rozliczania usług), aby potem powołać) wprost wymagania normy ISO/IEC 20000-1.

Zdecydowanie sugerujemy zmianę:

a) Skreślić ust. 2.
b) Zmodyfikować ust. 3:

„3. Wymagania określone w ust. 1 ~~i 2~~ uznaje się za spełnione jeśli zarządzanie usługami teleinformatycznymi przez dostawców świadczących te usługi na rzecz podmiotu publicznego odbywa się ~~projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie udoskonalanie systemu teleinformatycznego odbywają się~~ zgodnie z wymaganiami Polskiej Normy PN-ISO/IEC 20000-1:2007 „Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja” wraz z poprawkami lub uzupełnieniami tej normy albo normą ją zastępującą..

c) Dodać ust. 4:

4. Przy wdrażaniu normy wskazanej w ust. 3 zaleca się uwzględnienie wytycznych zawartych w PN-ISO/IEC 20000-2:2007 „Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania” wraz z poprawkami lub uzupełnieniami tej normy albo normą ją zastępującą.

14.

§14. Ust 3 i 4

a) Proponujemy modyfikację ust. 3, która ma na celu odseparowanie normy zawierającej wymagania (27001) ord norm wspierających jej wdrożenie (zawierających wytyczne).

„3. System zarządzania bezpieczeństwem informacji spełnia wymogi, o których mowa w ust. 1 ~~i 2~~, jeżeli jest zgodny z ~~został opracowany na podstawie~~ Polską Normą PN ISO/IEC 27001:2007 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeostwem informacji – Wymagania” wraz ~~z normami uzupełniającymi lub normy go zastępującej,~~ wraz z poprawkami lub uzupełnieniami tej normy albo normą ją zastępującą.

b) Dodać nowy ust 4 z 2. Części ust. 3:

4. Przy wdrażaniu normy wskazanej w ust. 3 zaleca się uwzględnienie wytycznych zawartych w:
1) PN-ISO/IEC 17799:2007 “Technika informatyczna – Techniki bezpieczeostwa – Praktyczne zasady zarządzania bezpieczeostwem informacji”,

2) PN-ISO/IEC 27005:2010 “Technika informatyczna – Techniki bezpieczeostwa – Zarządzanie ryzykiem w bezpieczeostwie informacji”,

~~3) PN-ISO/IEC 27006:2009 “Technika informatyczna – Techniki bezpieczeostwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeostwem informacji”,~~

<Uwaga: norma ta podmiotowo zawiera WYMAGANIA akredytacji dla jednostek certyfikujących SZBI, zatem nie odnosi się do podmiotów publicznych!>

4) PN-ISO/IEC 24762:2010 “Technika informatyczna – Techniki bezpieczeostwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie”.

wraz z poprawkami lub uzupełnieniami tych norm albo normami je zastępującymi.

c) Skreślić ust. 4 – ust. ten nie jest poprawny z punktu widzenia wdrożenia wymagań opisanych w normie 27001. Zabezpieczenia wdrożone w oparciu o model opisany w 27001 uwzględniać muszą wyniki szacowania ryzyka oraz odnośne przepisy prawa.

15.
Załącznik nr 2
Proponujemy wpisać na początku następujące zastrzeżenia:

1. Jeśli norma nie ma oznaczenia daty wydania, to oznacza, że ma zastosowanie ostatnie wydanej normy
2. Jeśli specyfikacja techniczna nie ma oznaczonej wersji lub daty wydania, to ma zastosowanie najnowsza, zalecana przez producenta, wersja specyfikacji

16.
Załącznik nr 2
Kolumna nr 5 - Nagłówek
Nagłówek tej kolumny jest niejasny. Czy oznacza on organizację normalizacyjną, czy firmę, która ma prawo własności intelektualnej?
Sugerujemy nie wprowadzać takiego ograniczenia, natomiast wpisać, czy specyfikacja jest przedmiotem międzynarodowej normalizacji – wtedy podać oznaczenie specyfikacji (nr normy lub jej nazwę), czy jest specyfikacją nieopublikowaną, wewnętrzna - wtedy podać właściciela tej specyfikacji.
Należy zaznaczyć, ze opublikowanie specyfikacji lub algorytmu nie przesądza o prawach własności , w tym licencji za użytkowanie.

17.
Załącznik nr 2
Kolumna nr 6 - Nagłówek
W nagłówku pojawiają się pojęcia niezdefiniowane: (dokument Normalizacyjny, dokument standaryzacyjny). Proponujemy zmienić na:
„Oznaczenie i nazwa normy lub dokumentu zawierającego specyfikację techniczna wskazanego formatu”

18.
Załącznik nr 2, pkt A.1.1.3
Ma zastosowanie norma ISO 19005-1:2005
Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)
Prośba o uwzględnienie bez daty publikacji

19.
Załącznik nr 2, pkt A.1.1.6
Ma zastosowanie norma ISO/IEC 26300 „ISO/IEC 26300:2006
Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0 – prośba o uwzgleднienie bez daty publikacji; na dniach są zatwierdzane techniczne poprawki TechCor 2