Załącznik Nr 4
do Zarządzenia Rektora Nr …….... z dnia……

METODYKA SZACOWANIA RYZYKA DLA SYSTEMÓW IT

Uniwersytet Przyrodniczy we Wrocławiu

Spis treści

Rozdział 1. Cel i zakres opracowania

§ 1

1. Klasyfikacja krytyczności Zasobów IT, definiuje minimalne akceptowalne poziomy ochrony informacji przetwarzanych w Zasobach IT i samych Zasobów, poprzez określenie klasy bezpieczeństwa posługując się metodyką szacowania ryzyka bezpieczeństwa dla Zasobów IT.
2. Niniejszy dokument opisuje metodykę szacowania ryzyka bezpieczeństwa dla danego Zasobu i służy jako narzędzie do nadania i weryfikowania klasyfikacji bezpieczeństwa.
3. Metodyka ta, uwzględnia ocenę wpływu informacji przetwarzanej w Zasobie IT, oraz poziomu jego bezpieczeństwa na następujące cechy bezpieczeństwa informacji:
    3.1. poufność,
    3.2. integralność,
    3.3. dostępność.

Rozdział 2. Rozumienie słów kluczowych

§ 2

1. Kluczowe słowa i zwroty występujące w niniejszym dokumencie: „MUSI", „NIE WOLNO", „BĘDZIE", „ NIE BĘDZIE", „POWINNO", „NIE POWINNO", „REKOMENDOWANE", „MOŻE", mają być interpretowane zgodnie z poniższym kluczem:
    1.1. „MUSI", „BĘDZIE", „NIE BĘDZIE", „NIE WOLNO": Te słowa kluczowe oznaczają bezwzględne wymaganie. Takie wymaganie musi być zaimplementowane wszędzie tam gdzie zapisy niniejszego standardu obowiązują. Wszystkie odstępstwa od tego wymagania są dopuszczalne jedynie w wyjątkowych przypadkach, i muszą być uzgodnione z Rektorem posługując się procedurą odstępstw.
    1.2. „POWINNO", „NIE POWINNO", „REKOMENDOWANE": Te słowa oznaczają silną rekomendację. Rezygnacja z wdrożenia takich wymagań musi być uzasadniona, a dokumentacja potwierdzająca uzasadnienie takiej rezygnacji będzie udostępniona Rektorowi.
    1.3. „MOŻE": Te słowa kluczowe oznaczają możliwość opcjonalnego wdrożenia zalecenia. Takie rekomendacje nie muszą być wdrożone, a decyzje o nie wdrażaniu zaleceń nie muszą być uzasadnione, ani dokumentowane.

Rozdział 3. Klasyfikacja bezpieczeństwa Zasobu IT

§ 3

1. Dla każdego Zasobu IT wyznaczony ASI przeprowadza ocenę krytyczności i klasyfikuje Zasób IT, definiując poziom ochrony oraz kryteria ich oceny, które zatwierdza właściwy kompetencyjnie Prorektor.
2. Dla danego Zasobu IT, wpływ każdej z wymienionych w §1 ust. 3 cech może mieć znaczenie odpowiadające jednemu z trzech przyjętych poziomów:

	POUNOŚĆ	**INTEGRALNOŚĆ**	**DOSTĘPNOŚĆ**
POZIOM	wysoki	wysoki	wysoki
	średni	średni	średni
	niski	niski	niski

3. Dla cechy POUFNOŚĆ, poziom bezpieczeństwa ustalany jest w zależności od klasyfikacji i rodzaju informacji przetwarzanej przez dany Zasób IT:

POUFNOŚĆ		
POZIOM	WYSOKI	informacje sklasyfikowane jako chronione lub dane osobowe
	ŚREDNI	informacje do użytku służbowego
	NISKI	informacje niepodlegające ochronie

4. Dla cechy INTEGRALNOŚĆ, poziom bezpieczeństwa ustalany jest według następujących kryteriów:

INTEGRALNOŚĆ		
POZIOM	WYSOKI	skutki naruszenia integralności informacji w kluczowych i krytycznych procesach, które mogą dotknąć każdą jednostkę organizacyjną w Uczelni
	ŚREDNI	skutki naruszenia integralności dla pozostałych procesów, ograniczone do części jednostek org. Uczelni, w której naruszenie wystąpiło
	NISKI	skutki naruszenia są ograniczone do pojedynczej jednostki organizacyjnej, w której naruszenie wystąpiło

5. Dla cechy DOSTĘPNOŚĆ, poziom bezpieczeństwa powinien zostać ustalony na podstawie analiz właściwych dla oceny potrzeb planów zapewnienia ciągłości działania Zasobów IT. Jeśli nie przeprowadzono takich analiz, przyjmuje się poziomy dostępności określone w wymiarze czasu odtworzenia danego Zasobu IT (lub Usługi, której Zasób jest częścią) tj. RTO.

DOSTĘPNOŚĆ		
POZIOM	WYSOKI	RTO poniżej 8 godzin
	ŚREDNI	RTO powyżej 8 godzin i poniżej 24 godzin
	NISKI	RTO powyżej 24 godzin

Rozdział 4. Zastosowanie poziomów poszczególnych cech – końcowa klasyfikacja

§ 4

1. Ocena krytyczności i klasyfikacja Zasobu IT dokonywana jest w oparciu o oceny poszczególnych cech według opisu z rozdziału 3

Poufność – Poziom: WYSOKI		**Integralność** – poziom:		
		WYSOKI	ŚREDNI	NISKI
Dostępność – poziom:	WYSOKI	WYSOKI	WYSOKI	ŚREDNI
	ŚREDNI	WYSOKI	WYSOKI	NISKI
	NISKI	ŚREDNI	NISKI	NISKI

Poufność – poziom: ŚREDNI		**Integralność** – poziom:		
		WYSOKI	ŚREDNI	NISKI
Dostępność – poziom:	WYSOKI	WYSOKI	WYSOKI	ŚREDNI
	ŚREDNI	WYSOKI	ŚREDNI	NISKI
	NISKI	ŚREDNI	NISKI	NISKI

Poufność – poziom: NISKI		**Integralność** – poziom:		
		WYSOKI	ŚREDNI	NISKI
Dostępność – poziom:	WYSOKI	WYSOKI	ŚREDNI	ŚREDNI
	ŚREDNI	ŚREDNI	NISKI	NISKI
	NISKI	NISKI	NISKI	NISKI

2. Ocena krytyczności i klasyfikacja Zasobu IT , o której mowa w ust. 1 powinna być wykonywana w następujących przypadkach:

   2.1. nie rzadziej niż raz na rok, bądź w związku z istotną zmianą funkcjonalną danego Zasobu IT,

   2.2. na etapie wstępnej analizy wymagań dla projektowanych istotnych zmian w Zasobie IT lub projektowania nowego Zasobu IT,

   2.3. w innych sytuacjach, uzasadnionych decyzjami ASI danego Zasobu IT lub Dyrektora CSK.

Rozdział 5. Postanowienia końcowe

§ 5

1. Zatwierdzona przez właściwego kompetencyjnie Prorektora informacja o klasyfikacji bezpieczeństwa danego Zasobu IT powinna być archiwizowana w jednostce, w której analiza jest przeprowadzana, a kopia u Dyrektora CSK.