Załączniki do zarządzenia
Wojewody Mazowieckiego z dnia 01 kwietnia 2025 r.

Załącznik nr 1

Matryca ryzyka

Prawdopodobieństwo wystąpienia

Bardzo Wysokie	**4**	**4**	**8**	**12**	**16**
Wysokie	**3**	**3**	**6**	**9**	**12**
Średnie	**2**	**2**	**4**	**6**	**8**
Niskie	**1**	**1**	**2**	**3**	**4**
Prawdopodobieństwo / Wpływ		**1** **Niski**	**2** **Średni**	**3** **Wysoki**	**4** **Bardzo Wysoki**

wpływ/ siła oddziaływania

Legenda

kolor:	zielony	żółty	pomarańczowy	czerwony
przedział zaszeregowania:	1-3	4-6	8-9	12-16
poziom ryzyka:	**Niski**	**Średni**	**Wysoki**	**Bardzo Wysoki** **(nieakceptowalny)**

1. Identyfikacja aktywów				2. Zagrożenie oraz współczynnik prawdopodobieństwa wystąpienia zagrożenia		3. Podatności	4. Określenie wpływu zagrożenia oraz poziomu zabezpieczeń								5. Przeprowadzenie analizy / Jakościowa analiza czynników ryzyka		6. Działania minimalizujące ryzyko wystąpienia zagrożeń
							Wpływ / skutek zagrożenia na:										
lp	Grupa aktywu	Nazwa aktywu	Istotność aktywu (I)	Zagrożenie	Współczynnik prawdopodobieństwa wystąpienia zagrożenia	Podatności	Poufność	Dostępność	Integralność	Autentyczność	Niezaprzeczalność	Niezawodność	Rozliczalność	Poziom zabezpieczeń	Wpływ na funkcjonowanie Urzędu (wyliczana jest średnia z wpływu/skutku zagrożenia na poufność/dostępność/integralność	Poziom ryzyka	Sposób minimalizacji ryzyka
1	Dokumenty (wersja papierowa, wersja elektroniczna)	Dane osobowe przetwarzane w formie tradycyjnej - papierowej	0	Zniszczenie	0	Niechronione przechowywanie	0	0	0	0	0	0	0	0	0	0	
2		Dane osobowe przetwarzane w formie elektronicznej	0		0		0	0	0	0	0	0	0	0	0	0	
3		Bazy danych umiejscowione poza Jednostką	0		0		0	0	0	0	0	0	0	0	0	0	
4		Bazy danych umiejscowione w Jednostce	0		0		0	0	0	0	0	0	0	0	0	0	
5	Pracownicy i współpracownicy	Stażyści, praktykanci, wolontariusze	0		0		0	0	0	0	0	0	0	0	0	0	
6		Pracownicy i współpracownicy na umowach cywilno-prawnych	0		0		0	0	0	0	0	0	0	0	0	0	
7	Know-how, Outsourcing, dostawcy (wiedza, usługi i produkty od firm zewnętrznych)	Usługi serwisowe, gwarancyjne oraz wsparcia merytorycznego / organizacyjnego	0		0		0	0	0	0	0	0	0	0	0	0	
8	Oprogramowanie komputerowe do przetwarzania danych	Oprogramowanie webowe przetwarzające dane osobowe	0		0		0	0	0	0	0	0	0	0	0	0	
9		Oprogramowanie desktopowe przetwarzające dane osobowe	0		0		0	0	0	0	0	0	0	0	0	0	
10	Media	Internet	0		0		0	0	0	0	0	0	0	0	0	0	
11	Infrastruktura IT (serwery, stanowiska robocze, sieć komputerowa, Internet)	Serwery	0		0		0	0	0	0	0	0	0	0	0	0	
12		Komputery	0		0		0	0	0	0	0	0	0	0	0	0	
13		Urządzenia sieciowe (switche, firewall, router)	0		0		0	0	0	0	0	0	0	0	0	0	
14		Okablowanie strukturalne	0		0		0	0	0	0	0	0	0	0	0	0	
15		Urządzenia mobilne	0		0		0	0	0	0	0	0	0	0	0	0	
16		Urządzenia peryferyjne (drukarka, kserokopiarka)	0		0		0	0	0	0	0	0	0	0	0	0	
17		Zasilacze UPS	0		0		0	0	0	0	0	0	0	0	0	0	
18	Infrastruktura (budynki, pomieszczenia własne i wynajmowane, transport)	Serwerownia	0		0		0	0	0	0	0	0	0	0	0	0	
19		Pomieszczenia biurowe	0		0		0	0	0	0	0	0	0	0	0	0	
20		Archiwum zakładowe	0		0		0	0	0	0	0	0	0	0	0	0	
21	Prawa osób, któych dane dotyczą	Przejrzyste informowanie i przejrzystą komunikację z osobami, których dane dotyczą, na podstawie art. 12-13 RODO	0		0		0	0	0	0	0	0	0	0	0	0	
22		Spełnienie uzasadnionych żądań osób, których dane dotyczą, na podstawie art. 15-21 RODO	0		0		0	0	0	0	0	0	0	0	0	0	

Załącznik nr 2

Załącznik nr 3

					Aktywa (P-Prawdopodobieństwo incydentu / S-Skutki wystąpienia incydentu/ R-Ryzyko wystąpienia incydentu) Formuła: R=P*S																																																																
					Grupa dokumenty												Grupa media			Grupa usługi			Grupa oprogramowanie						Grupa Infrastruktura IT (sieć, sprzęt, poczta, internet)																					Grupa Infrastruktura (obiekty, transport)									Grupa Pracownicy i współpracownicy						Prawa osób, których dane dotyczą					
					Dane osobowe przetwarzane w formie tradycyjnej - papierowej			Dane osobowe przetwarzane w formie elektronicznej			Bazy danych umiejscowione poza Jednostką			Bazy danych umiejscowione w Jednostce			Internet			Usługi serwisowe, gwarancyjne oraz wsparcia merytorycznego /			Oprogramowanie webowe przetwarzające dane osobowe			Oprogramowanie desktopowe przetwarzające dane osobowe			serwery			komputery			Urządzenia sieciowe (switche, firewall, router)			Okablowanie strukturalne			Urządzenia mobilne			Urządzenia peryferyjne (drukarka, kserokopiarka)			Zasilacze UPS			Serwerownia			Pomieszczenia biurowe			Archiwum			Stażyści, praktykanci, wolontariusze			Pracownicy i współpracownicy na umowach cywilno-prawnych			Przejrzyste informowanie i przejrzysta komunikacja z osobami, których dane			Spełnienie uzasadnionych żądań osób, których dane dotyczą		
zagrożenia		P	U	N	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R	P	S	R
zniszczenie fizyczne	Pożar						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Zalanie						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Zanieczyszczenie						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Zniszczenie						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
zjawiska naturalne	Zjawiska klimatyczne (np. mroźna zima)						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Zjawiska pogodowe (np. ulewny deszcz)						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
utrata podstawowych usług	Awaria systemu klimatyzacji lub dostaw wody						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Utrata ładu informatycznego						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Utrata dostaw prądu						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Awaria urządzenia telekomunikacyjnego						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
naruszenie bezpieczeństwa	Przechwycenie sygnałów na skutek zjawiska interferencji						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Szpiegostwo zdalne						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Podsłuch						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Kradzież nośników lub dokumentów						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Kradzież urządzenia						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Dane z niewiarygodnych źródeł						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Manipulowanie urządzeniem						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Sfałszowanie oprogramowania						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Wyrzucenie dokumentów lub nośników danych						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Nie wywiązanie się z umowy						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
awarie techniczne	Awaria urządzenia						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Niewłaściwe funkcjonowanie urządzeń						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Przeciążenie systemu informatycznego						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Niewłaściwe funkcjonowanie oprogramowania						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
nieautoryzowane działania	Nieautoryzowane użycie urządzeń						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Nieuprawnione kopiowanie oprogramowania						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Użycie fałszywego lub skopiowanego oprogramowania						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Wykorzystanie jednego punktu dostępu przez kilku pracowników						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Dostęp do danych bez upoważnienia						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
naruszenie bezpieczeństwa	Błąd użytkowania						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Nie wykonanie rocznego planu kontroli						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Naruszenie praw						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Fałszowanie praw						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Agresywny/pijany petent						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Odmowa działania (np. niestosowanie się do SZBI)						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
haker, cracker	Haking wiążący się z uszkodzeniem						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Wtargnięcie do systemu, włamania						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Złośliwy kod (np. wirus, bomba logiczna, koń trojański)						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Przekupstwo informacyjne						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Atak sieciowy polegający na sfałszowaniu adresu źródłowego						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
terroryzm, szpiedzy przemysłowi, wywiad	Penetracja systemu						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Atak na system (np. rozproszona odmowa usługi)						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Naruszenie bezpieczeństwa systemu						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
Klienci/petenci, pracownicy (osoby niezadowolone, złośliwe, niedbałe, źle wyszkolone)	Napaść na pracownika						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Szantaż						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Korupcja						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Przeszukiwanie informacji stanowiących własność						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Przekupstwo informacyjne						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Wprowadzanie fałszywych, zniekształconych danych						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Sprzedaż danych osobowych						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Sabotaż systemu						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0
	Nieautoryzowany dostęp						0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0			0

Załącznik nr 4

Plan postępowania z ryzykiem bardzo wysokim

Stan na dzień …… r.

Lp.	Ryzyko	Dział lub proces	Dotyczy zagrożenia	Opis postępowania	Osoba odpowiedzialna za realizację	Planowane koszty realizacji	Planowana data zakończenia realizacji	Data zakończenia realizacji	Skuteczność (wg skali 1-4)