METODYKA SZACOWANIA RYZYKA

Podpis zatwierdzającego	*02.11.2023* */Data zatwierdzenia/*	**Obowiązuje od:**	**06.11.2023**

1. CEL PROCEDURY

Niniejszy dokument zawiera opis zasad szacowania ryzyka związanych ze zidentyfikowanymi w organizacji procesami istotnymi z punku widzenia dla jej funkcjonowania oraz ochroną danych osobowych.

2. IDENTYFIKACJA DANYCH

W celu przeprowadzenia szacowania ryzyka opisaną poniżej metodą niezbędne jest zidentyfikowanie zbiorów danych służących do przetwarzania danych osobowych. W wyniku przeprowadzonej analizy zidentyfikowano zbiory, które określono w załączniku numer 1 do niniejszej procedury.

3. ANALIZA RYZYKA

W celu określenia wpływu czynników zewnętrznych (zagrożeń) na czynności przetwarzania należy je zidentyfikować, przypisać im odpowiednie wartości liczbowe, określić prawdopodobieństwo ich wystąpienia w odniesieniu do konkretnej czynności zasobu oraz oszacować skutek zgodnie z poniższymi tabelami.

Prawdopodobieństwo wystąpienia zagrożenia (Z)		
Oznaczenie	**Opis**	**Wartość liczbowa**
Niskie	Wystąpienie zjawiska jest mało prawdopodobne, jednak z różnych powodów nie należy go ignorować	1
Średnie	Zjawisko występowało już w przeszłości, lub jest prawie pewne, że zjawisko wystąpi podczas realizacji zadań	2
Wysokie	Zjawisko występowało w przeszłości często lub istnieje duże prawdopodobieństwo jego wystąpienia podczas realizacji zadań	3

Skutek wystąpienia zidentyfikowanych zagrożeń (S)		
Oznaczenie	**Opis**	**Wartość liczbowa**
Mały, nieistotny	Wystąpienie zagrożenia spowoduje niewielkie szkody dla organizacji	1
Istotny	Wystąpienie zagrożenia spowoduje szkody istotne tylko dla organizacji	2
Ważny	Wystąpienie zagrożenia spowoduje naruszenie zdolności do działania organizacji, a szkody z tego wynikłe dotyczą nie tylko organizacji ale i osób trzecich (w tym także osób prawnych)	3

Wprowadzono również pojęcie podatności. Podatność oznacza słabość czynności przetwarzania, która może być wykorzystana przez jedno lub więcej zagrożeń.

Podatność (P)	
Opis	**Wartość liczbowa**
Zbiór jest podatny na zagrożenie w niewielkim stopniu	1
Zbiór jest średnio podatny na zagrożenie	2
Zbiór jest podatny na zagrożenie	3

Następnym etapem jest identyfikacja ryzyk, które mogą wystąpić w odniesieniu do określonych w pkt. 2.1 aktywów.

Ryzyko (R) związane z wystąpieniem danego zagrożenia określone jest jako:

$$R=Z \times S \times P$$

gdzie:
R- ryzyko
Z - Prawdopodobieństwo wystąpienia zagrożenia
S - skutek wystąpienia zidentyfikowanych zagrożeń
P - podatność

W wyniku działania określono dalsze postępowanie w stosunku do zagrożenia w zależności od wartości obliczonego ryzyka:

Ryzyko (R)	**Dopuszczalność ryzyka**	**Niezbędne działania**
1 – 8	Pomijalne	Brak działań, monitorowanie zagrożenia
9 – 17	Istotne	Określenie działań zapobiegawczych
18 – 27	Realne	Zmiana zasad działania

Wyniki analizy można przedstawić zgodnie z poniższym schematem:

Zbiór danych:				**Z1 – Zn. Nazwa zbioru**			**Plan minimalizacji ryzyka**		
							działanie	**osoba**	**termin**
Lp.	**Zagrożenie**	**Prawdopodobieństwo wystąp. zagrożenia /Z/**	**Skutek wystąpienia zagrożenia /S/**	**Podatność /P/**	**Obliczone ryzyko /R/**	**Dopuszczalność ryzyka**			

4. Załączniki

Załącznik 1 – identyfikacja zbiorów danych.
Załącznik 2 – identyfikacja zagrożeń.

Załącznik numer 1

L.p	Zbiory zawierające dane osobowe
1	Z-1. Zbiór danych kontaktowych.
2	Z-2. Zbiór dokumentów kadrowych i płacowych
3	Z-3. Zbiór dokumentów księgowych
4	Z-4. Zbiór umów z kontrahentami
5	Z-5. Ewidencja osób upoważnionych do przetwarzania danych osobowych
6	
7	

Załącznik numer 2

L.p	Zagrożenie
1	Pożar
2	Włamanie.
3	Awaria zasilania biura/poradni
4	Awaria infrastruktury teleinformatycznej
5	Kradzież sprzętu informatycznego
6	Nieuprawniony dostęp do informacji wrażliwej przez osoby nieupoważnione
7	Niedobór personelu
8	Nieuprawniona działalność klientów i podwykonawców
9	Nieprzestrzeganie procedur postępowania lub bezpieczeństwa

Arkusz analizy ryzyka DTI Poland

Procesy:				Z1 – Zn. zidentyfikowany proces.			Plan minimalizacji ryzyka		
							działanie	Osoba odpowiedzialna	termin
L.p	Zagrożenie	Prawdopodobieństwo wystąp. zagrożenia /Z/	Skutek wystąpienia zagrożenia /S/	Podatność /P/	Obliczone ryzyko /R/	Dopuszcza-ilość ryzyka			

Arkusz analizy ryzyka DTI Poland

Procesy:				Z-1. Zbiór danych kontaktowych.			Plan minimalizacji ryzyka		
							działanie	Osoba odpowiedzialna	termin
L.p	Zagrożenie	Prawdopodobieństwo wystąp. zagrożenia /Z/	Skutek wystąpienia zagrożenia /S/	Podatność /P/	Obliczone ryzyko /R/	Dopuszcza-ilość ryzyka			
1	Pożar	1	3	2	6	Pomijalne			
2	Włamanie.	1	2	2	4	Pomijalne			
3	Awaria zasilania biura/poradni	2	1	3	6	Pomijalne			
4	Awaria infrastruktury teleinformatycznej	1	1	1	1	Pomijalne			
5	Kradzież sprzętu informatycznego	1	3	2	6	Pomijalne			
6	Nieuprawniony dostęp do informacji wrażliwej przez osoby nieupoważnione	1	2	2	4	Pomijalne			
7	Niedobór personelu	1	1	1	1	Pomijalne			
8	Nieuprawniona działalność klientów i podwykonawców	1	3	2	6	Pomijalne			
9	Nieprzestrzeganie procedur postępowania lub bezpieczeństwa	2	1	2	4	Pomijalne			

Arkusz analizy ryzyka DTI Poland

				Procesy:	Z-2. Zbiór dokumentów kadrowych i płacowych.		Plan minimalizacji ryzyka		
							działanie	Osoba odpowiedzialna	termin
L.p	Zagrożenie	Prawdopodobieństwo wystąp. zagrożenia /Z/	Skutek wystąpienia zagrożenia /S/	Podatność /P/	Obliczone ryzyko /R/	Dopuszcza-ilość ryzyka			
1	Pożar	1	3	2	6	Pomijalne			
2	Włamanie.	1	2	2	4	Pomijalne			
3	Awaria zasilania biura/poradni	2	1	3	6	Pomijalne			
4	Awaria infrastruktury teleinformatycznej	1	1	1	1	Pomijalne			
5	Kradzież sprzętu informatycznego	1	3	2	6	Pomijalne			
6	Nieuprawniony dostęp do informacji wrażliwej przez osoby nieupoważnione	1	2	2	4	Pomijalne			
7	Niedobór personelu	1	1	1	1	Pomijalne			
8	Nieuprawniona działalność klientów i podwykonawców	1	3	2	6	Pomijalne			
9	Nieprzestrzeganie procedur postępowania lub bezpieczeństwa	2	1	2	4	Pomijalne			

Arkusz analizy ryzyka DTI Poland

Procesy:				Z-3. Zbiór dokumentów księgowych.			Plan minimalizacji ryzyka		
							działanie	Osoba odpowiedzialna	termin
L.p	Zagrożenie	Prawdopodobieństwo wystąp. zagrożenia /Z/	Skutek wystąpienia zagrożenia /S/	Podatność /P/	Obliczone ryzyko /R/	Dopuszcza-ilość ryzyka			
1	Pożar	1	3	2	6	Pomijalne			
2	Włamanie.	1	2	2	4	Pomijalne			
3	Awaria zasilania biura/poradni	2	1	3	6	Pomijalne			
4	Awaria infrastruktury teleinformatycznej	1	1	1	1	Pomijalne			
5	Kradzież sprzętu informatycznego	1	3	2	6	Pomijalne			
6	Nieuprawniony dostęp do informacji wrażliwej przez osoby nieupoważnione	1	2	2	4	Pomijalne			
7	Niedobór personelu	1	1	1	1	Pomijalne			
8	Nieuprawniona działalność klientów i podwykonawców	1	3	2	6	Pomijalne			
9	Nieprzestrzeganie procedur postępowania lub bezpieczeństwa	2	1	2	4	Pomijalne			

Arkusz analizy ryzyka DTI Poland

			Procesy:	**Z-4. Zbiór umów z kontrahentami.**			**Plan minimalizacji ryzyka**		
							działanie	**Osoba odpowiedzialna**	**termin**
L.p	**Zagrożenie**	**Prawdopodobieństwo wystąp. zagrożenia /Z/**	**Skutek wystąpienia zagrożenia /S/**	**Podatność /P/**	**Obliczone ryzyko /R/**	**Dopuszcza-ilość ryzyka**			
1	Pożar	1	3	2	6	Pomijalne			
2	Włamanie.	1	2	2	4	Pomijalne			
3	Awaria zasilania biura/poradni	2	1	3	6	Pomijalne			
4	Awaria infrastruktury teleinformatycznej	1	1	1	1	Pomijalne			
5	Kradzież sprzętu informatycznego	1	3	2	6	Pomijalne			
6	Nieuprawniony dostęp do informacji wrażliwej przez osoby nieupoważnione	1	2	2	4	Pomijalne			
7	Niedobór personelu	1	1	1	1	Pomijalne			
8	Nieuprawniona działalność klientów i podwykonawców	1	3	2	6	Pomijalne			
9	Nieprzestrzeganie procedur postępowania lub bezpieczeństwa	2	1	2	4	Pomijalne			

Arkusz analizy ryzyka DTI Poland

Procesy:				Z-5. Ewidencja osób upoważnionych do przetwarzania danych osobowych.			Plan minimalizacji ryzyka		
							działanie	Osoba odpowiedzialna	termin
L.p	Zagrożenie	Prawdopodobieństwo wystąp. zagrożenia /Z/	Skutek wystąpienia zagrożenia /S/	Podatność /P/	Obliczone ryzyko /R/	Dopuszcza-ilość ryzyka			
1	Pożar	1	3	2	6	Pomijalne			
2	Włamanie.	1	2	2	4	Pomijalne			
3	Awaria zasilania biura/poradni	2	1	3	6	Pomijalne			
4	Awaria infrastruktury teleinformatycznej	1	1	1	1	Pomijalne			
5	Kradzież sprzętu informatycznego	1	3	2	6	Pomijalne			
6	Nieuprawniony dostęp do informacji wrażliwej przez osoby nieupoważnione	1	2	2	4	Pomijalne			
7	Niedobór personelu	1	1	1	1	Pomijalne			
8	Nieuprawniona działalność klientów i podwykonawców	1	3	2	6	Pomijalne			
9	Nieprzestrzeganie procedur postępowania lub bezpieczeństwa	2	1	2	4	Pomijalne			