

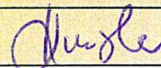
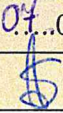
P7-01

Identyfikacja i szacowanie ryzyka

Procedura SZJ

Egzemplarz nr⁰

aktualizowany / nieaktualizowany

	Opracował	Sprawdził	Zatwierdził
Imię i nazwisko	Beata Szambora	Małgorzata Krzyśko	Agata Świdorska-Ostapiak
Data	07.02.2020r.	07.02.2020r.	07.02.2020r.
Podpis			

Nowa Sól, luty 2020

Historia akceptacji

PR.ZD-000016/20

Lp	St a n	Stan akceptacji (opis)	Do kogo	Data operacji	Operację wykonał	Adnotacje odb.	Rodzaj akc.	Adnotacje wys.	Od kogo	Data wysłania
1		Zaakceptowane	Krzyśko Małgorzata (Dział Rozwoju i Inwestycji)	2020.02.07 10:05	Krzyśko Małgorzata		Merytoryczna		Szambora Beata (Dział Rozwoju i Inwestycji)	2020.02.07 09:43
2		Zaakceptowane	Świderska- Ostapiak Agata (Prezes Zarządu)	2020.02.07 11:04	Świderska- Ostapiak Agata		Formalna		Szambora Beata (Dział Rozwoju i Inwestycji)	2020.02.07 10:05

	IDENTYFIKACJA I SZACOWANIE RYZYKA	P7-01
	Wersja 3_2020	Strona 2 / 5

1. CEL

Celem procedury jest zapewnienie, że wyniki uzyskane w ramach określania ryzyka będą wiarygodne, rzetelne, powtarzalne i porównywalne, a na ich podstawie określone zostaną strategia i regulacje operacyjne.

2. PRZEDMIOT I ZAKRES

Przedmiotem procedury jest tryb postępowania podczas identyfikacji i szacowania ryzyk przy realizacji poszczególnych procesów.

3. ODPOWIEDZIALNOŚĆ

Za nadzór nad identyfikacją i szacowaniem ryzyk odpowiedzialny jest kierownik/osoba odpowiedzialna za realizację danego procesu.

4. TRYB POSTĘPOWANIA

4.1 Szacowanie ryzyka musi przebiegać zgodnie z niniejszą procedurą oddzielnie dla obszaru objętego certyfikacją (Laboratorium zakładowe) i oddzielnie dla pozostałego obszaru działalności MZGK sp. z o.o. w Nowej Soli.

4.2 Rozpoczynając szacowanie ryzyka należy w pierwszej kolejności przeprowadzić inwentaryzację aktyw w firmie.

4.3 Pojęcie „aktywa” zaczerpnięte z normy ISO/IEC 27001 jest następujące:
aktywa – wszystko co ma wartość dla Organizacji w poszczególnych procesach.
Przykładem takich aktywów mogą być:

- infrastruktura wodociągowo-kanalizacyjna, COŚ, SUW będąca własnością Spółki,
- siedziba,
- pracownicy oraz ich wiedza i doświadczenie,
- bazy klientów,
- bazy dostawców usług laboratoryjnych i innych,
- sprzęt i oprogramowanie,

czyli informacje, których utrata może narazić Organizację na straty finansowe lub wizerunkowe.

4.4 Po zakończeniu etapu identyfikacji aktywów w procesach należy przejść do techniki tzw. „burzy mózgów”, podczas której należy próbować przewidzieć wszelkie możliwe zdarzenia, które mogą zagrozić danemu aktywowi. Po sporządzeniu listy potencjalnych zagrożeń należy oszacować ryzyko zgodnie z przyjętą metodyką w celu otrzymania wartości punktowej danego zagrożenia.

	IDENTYFIKACJA I SZACOWANIE RYZYKA	P7-01
	Wersja 3_2020	Strona 3 / 5

4.5 W ocenie ryzyka znajduje się przyjęta metodyka określania wartości punktowych zgodnie z matrycą, gdzie oceniany jest skutek potencjalnego zdarzenia i prawdopodobieństwo wystąpienia tego zdarzenia. Dopuszcza się stosowanie matrycy w następujących wariantach:

Wariant A:

PRAWDOPODOBIENSTWO	ZNACZENIE/ SKUTEK DLA JAKOŚCI PRODUKTU			
	<i>katastrofalne</i>	<i>istotne</i>	<i>umiarkowane</i>	<i>nieistotne</i>
Sporadyczne (1 lub 2 razy w roku)	3	3	2	1
Częste (kilka razy w roku)	3	2	1	1
Niezwykłe (bardzo małe ryzyko wystąpienia - raz na 5-30 lat)	3	2	1	1

lub **Wariant B:**

PRAWDOPODOBIENSTWO	ZNACZENIE/ SKUTEK DLA JAKOŚCI PRODUKTU				
	<i>nieistotne</i> 1	<i>niewielkie</i> 2	<i>umiarkowane</i> 3	<i>poważne</i> 4	<i>katastrofalne</i> 5
Niespotykane (1)	1	2	3	4	5
Mało prawdopodobne (2)	2	4	6	8	10
Umiarkowanie prawdopodobne (3)	3	6	9	12	15
Prawdopodobne (4)	4	8	12	16	20
Niemal pewne (5)	5	10	15	20	25

lub **Wariant C:** (stosowany w analizie ryzyka w obszarze ochrony danych osobowych).

Prawdopodobieństwo i skutki w Wariacie C ustala się oddzielnie dla każdego atrybutu informacji: poufności, integralności i dostępności. Dokonując szacowania ryzyka w tym wariacie otrzymujemy oddzielne wartości ryzyka w odniesieniu do poufności, integralności i dostępności.

Analiza ryzyka w obszarze danych osobowych wykonywana jest w programie ARDO, którego właścicielem jest firma F-tec.pl., od której Spółka zakupiła licencję.

	IDENTYFIKACJA I SZACOWANIE RYZYKA	P7-01
	Wersja 3_2020	Strona 4 / 5

PRAWDOPODOBIENSTWO	ZNACZENIE/ SKUTEK DLA JAKOŚCI PRODUKTU				
	<i>brak</i> 0	<i>niskie</i> 1 - 2	<i>średnie</i> 3 - 5	<i>wysokie</i> 6 - 8	<i>maksymalne</i> 9 - 10
Brak (0)	0	0	0	0	0
Bardzo niskie (0,1-0,2)	0	0,1 - 0,4	0,3 - 1,0	0,6 - 1,6	0,9 - 2,0
Niskie (0,3-0,4)	0	0,3 - 0,8	0,9 - 2,0	1,8 - 3,2	2,7 - 4,0
Średnie (0,5-0,6)	0	0,5 - 1,2	1,5 - 3,0	3,0 - 4,8	4,5 - 6,0
Wysokie (0,6-0,8)	0	0,6 - 1,6	1,8 - 4,0	3,6 - 6,4	5,4 - 8,0
Bardzo wysokie (0,9-1)	0	0,9 - 2,0	2,7 - 5,0	5,4 - 8,0	8,1 - 10,0

4.6 Po otrzymaniu wartości punktowych dla danego ryzyka ustala się plan postępowania z nim w zależności od liczby punktów osiągniętych przez to ryzyko. Po przyjęciu odpowiednich kryteriów należy sprawdzić, czy oszacowane ryzyko jest do zaakceptowania, czy może należy podjąć działania zmierzające do sprowadzenia ryzyka do wartości akceptowalnej. Pamiętać należy tutaj o zasadzie racjonalnego zarządzania ryzykiem i ponoszonych z tego tytułu kosztach.

Wariant A:

Ocena 1 i 2 - ryzyko akceptowalne

Ocena 3 - ryzyko nieakceptowalne

Wariant B:

Ocena od 1 do 15 - ryzyko akceptowalne

Ocena od 16 do 25 - ryzyko nieakceptowalne

Wariant C

Ocena 0 – brak ryzyka

Ocena od 1 do 5 - ryzyko akceptowalne

Ocena od 6 do 10 - ryzyko nieakceptowalne

W każdym przypadku ryzyka nieakceptowalnego należy rozważyć możliwości jego obniżenia do poziomu akceptowalnego poprzez opracowanie, wdrożenie oraz utrzymywanie odpowiednich polityk, procedur, instrukcji lub innych wytycznych zwracających szczególną uwagę na dany problem, lub (jeśli nie jest to możliwe) należy prowadzić szczególny nadzór i przeprowadzać ocenę ryzyka z częstotliwością nie mniejszą niż co 6 miesięcy.

4.7 W zależności od stosowanego rodzaju matrycy oceny ryzyka Rejestr ryzyk należy sporządzić odpowiednio na formularzu F103A (w przypadku wyboru Wariantu A) lub 103B (w przypadku wyboru Wariantu B). W przypadku stosowania Wariantu C raport generowany jest z programu ARDO.

	IDENTYFIKACJA I SZACOWANIE RYZYKA	P7-01
	Wersja 3_2020	Strona 5 / 5

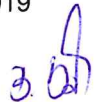
4.8 Szacowanie ryzyka należy przeprowadzić minimum raz w roku kalendarzowym w odstępach 12 miesięcznych, oraz w przypadku zmian organizacyjnych mających wpływ na bezpieczeństwo procesów.

5 Załączniki

F103A Rejestr ryzyk (Wariant A)

F103B Rejestr ryzyk (Wariant B)

6. TABELA ZMIAN I POPRAWEK

Lp.	Treść zmiany / poprawki	Zmianę wprowadził	Podpis / data
1	Wprowadzenie procedury	Pełnomocnik ds. SZJ	29.06.2018 
2	W pkt. 4.5 wprowadzono drugi wariant matrycy oceny ryzyka (Wariant B – skala pięciostopniowa). W pkt. 4.6 określono poziom ryzyka akceptowalnego i nieakceptowalnego dla Wariantu B. W pkt. 4.7 określono sposób sporządzania Rejestru ryzyk. Dotychczasowy pkt 4.7 jest obecnie pkt. 4.8. Wycofano formularz F103 Rejestr ryzyk. Wprowadzono nowy formularz F103A Rejestr ryzyk (Wariant A). Wprowadzono nowy formularz F103B Rejestr ryzyk (Wariant B).	Pełnomocnik ds. SZJ	11.03.2019 
3	W pkt. 4.5 wprowadzono trzeci wariant matrycy oceny ryzyka (Wariant C – stosowany w analizie ryzyka w obszarze ochrony danych osobowych) W pkt. 4.6 określono poziom ryzyka akceptowalnego i nieakceptowalnego dla Wariantu C. W pkt. 4.7 określono sposób dokumentowania oceny ryzyka przy zastosowaniu Wariantu C.	Pełnomocnik ds. SZJ	07.02.2020 