Spółdzielnia Mieszkaniowa "Naftowiec"
ul. Stefana Wyszyńskiego 11A
65-536 Zielona Góra

ZARZĄDZANIE RYZYKIEM

Informacja o dokumencie:

Dokument:	Zarządzanie ryzykiem
Wersja:	0.1
Opis:	Załącznik do Polityki Bezpieczeństwa Informacji
Właściciel:	Spółdzielnia Mieszkaniowa "Naftowiec" (zwana dalej Organizacją)
Obszar zastosowania:	Dokument ma zastosowanie do wszystkich pracowników Organizacji
Status:	Do użytku służbowego
Źródło/plik::	SMN_Zarzadzanie_Ryzykiem_2018_v0.2sta.docx

Historia zmian:

Nr wersji	Data	Autorzy	Opis zmian
1.0	2018-MM-DD		pierwsza wersja „produkcyjna"

Spis treści:

Spis tabel:

I.
DEFINICJE / TERMINOLOGIA

§ 1

Dla celów niniejszego dokumentu stosuje się terminy i definicje podane w Polityce Bezpieczeństwa Informacji.

II. CEL, ZAKRES I UŻYTKOWNICY

§ 2

1. Celem niniejszego dokumentu (procedury) jest zdefiniowanie metodyki szacowania oraz postępowania z ryzykiem związanym z przetwarzaniem informacji w Organizacji oraz określenie akceptowalnych poziomów ryzyk zgodnie z normą PN-ISO/IEC 27001 oraz PN-ISO/IEC 27005.
2. Użytkownikami niniejszego dokumentu są wszyscy pracownicy Organizacji, którzy biorą udział w szacowaniu ryzyka oraz postępowaniu z ryzykiem.
3. Załącznikami dokumentu są:
   1) zestawienie aktywów Organizacji
   2) zestawienie zagrożeń
   3) zestawienie podatności
   4) wstępna analiza ryzyka dla wybranych aktywów w celu ustalenia metodyki postępowania z ryzykiem przed wykonaniem analizy dla większej grupy aktywów,
   5) propozycje działań doskonalących (zapobiegawcze i/lub korygujące) dla stwierdzonych ryzyk w kategorii Średnie i Wysokie

III.
KLASYFIKACJA INFORMACJI

§ 3

1. Dla każdej klasy aktywów informacyjnych określa się poziom istotności informacji dla Organizacji z punktu widzenia trzech kategorii (atrybutów bezpieczeństwa informacji): Poufności (P), Integralności (I), Dostępności (D),
2. Wprowadza się trzystopniową klasyfikację **poufności** (P) informacji ze względu na potencjalny rozmiar szkód, które mogłoby spowodować ujawnienie informacji nieuprawnionym osobom lub instytucjom:

1) 1 (poziom niski) – dotyczy informacji, które mogą być publicznie znane lub których ujawnienie nie powoduje lub powoduje niewielkie konsekwencje natury prawnej lub finansowej.
2) 2 (poziom średni) – dotyczy informacji, których ujawnienie może wiązać się z poważnymi konsekwencjami natury finansowej lub prawnej. Do tej grupy zaliczymy również dane osobowe.
3) 3 (poziom wysoki) – informacje krytyczne, których ujawnienie mogłoby zagrozić funkcjonowaniu Organizacji lub spowodować bardzo poważne szkody natury prawnej lub finansowej. Do tej grupy zaliczamy również tzw. wrażliwe dane osobowe.

3. Wprowadza się trzystopniową klasyfikację **integralności** (I) informacji ze względu na potencjalny rozmiar szkód, które mogłaby spowodować nieautoryzowana zmiana informacji:
   1) 1 (poziom niski) – informacje, których nieautoryzowana zmiana nie powoduje lub powoduje niewielkie konsekwencje natury prawnej lub finansowej.
   2) 2 (poziom średni) – informacje, których nieautoryzowana zmiana może wiązać się z poważnymi konsekwencjami natury finansowej lub prawnej. Do tej grupy zaliczamy dane osobowe.
   3) 3 (poziom wysoki) – informacje, których nieautoryzowana zmiana mogłaby zagrozić funkcjonowaniu Organizacji lub spowodować bardzo poważne szkody natury prawnej lub finansowej.
4. Wprowadza się trzystopniową klasyfikację **dostępności** (D) informacji ze względu na maksymalny akceptowalny okres niedostępności do informacji lub konsekwencje ich utraty:
   1) 1 (poziom niski) – długotrwały brak dostępu do tych informacji nie wpływa negatywnie w istotny sposób na funkcjonowaniu Organizacji oraz nie pociąga za sobą konsekwencji prawnych lub finansowych,
   2) 2 (poziom średni) – informacje, dla których brak dostępu krótszy niż jeden dzień nie wpływa negatywnie w istotny sposób na funkcjonowaniu Organizacji oraz nie pociąga za sobą konsekwencji prawnych lub finansowych,
   3) 3 (poziom wysoki) – informacje dla których brak dostępu dłuższy niż cztery godziny w istotny sposób odbije się na funkcjonowaniu Organizacji lub może pociągać za sobą poważne konsekwencje natury prawnej lub finansowej.

IV. SZACOWANIE RYZYKA

§ 4

1. Proces analizy ryzyka polega na identyfikacji ryzyk tzn. prawdopodobieństwa wystąpienia określonych zagrożeń wykorzystujących podatność systemu, określenia ich wielkości i wpływu na bezpieczeństwo systemu oraz opisaniu obszarów wymagających zabezpieczenia i zastosowania środków ochrony.
2. Szacowanie ryzyka wykonywane jest z użyciem tabeli szacowania ryzyka.

§ 5

Kompetencje i odpowiedzialność

1. Identyfikacja zagrożeń i podatności jest wykonywana przez właścicieli aktywów.
2. Szacowanie konsekwencji oraz prawdopodobieństwa jest wykonywane przez właścicieli aktywów.
3. Każdy pracownik Organizacji zobowiązany jest zgłaszać przełożonym zaobserwowane lub potencjalne zagrożenie oraz incydenty związane z bezpieczeństwem informacji.

§ 6

Tryb postępowania

1. Istotą procesu oceny ryzyka jest określenie znaczenia ryzyka na podstawie porównania wyznaczonych wartości ryzyk dla zidentyfikowanych aktywów z kryteriami akceptowania ryzyka w kontekście celów strategicznych i biznesowych Organizacji oraz spełnienia przepisów prawa.
2. Ocena ryzyka powinna być prowadzona na właściwym stopniu szczegółowości z uwzględnieniem strat finansowych, wizerunkowych i informacyjnych, które Organizacja doświadczyła bądź może doświadczyć w przyszłości - polega to na przypisywaniu wartości liczbowej prawdopodobieństwu wystąpienia, podatności oraz skutkom zdarzeń.

V. AKTYWA, SKUTKI, PODATNOŚCI I ZAGROŻENIA

§ 7Aktywa

1. Pierwszym krokiem w szacowaniu ryzyka jest zidentyfikowanie wszystkich aktywów, które mogą wpływać na poufność, integralność i dostępność informacji w Organizacji. Aktywami mogą być dokumenty w postaci papierowej lub elektronicznej, aplikacje i bazy danych, ludzie, sprzęt IT, infrastruktura oraz usługi

zewnętrzne i procesy zlecane na zewnątrz. Podczas identyfikacji aktywów, konieczne jest także określenie ich właścicieli – osób lub jednostek organizacyjnych odpowiedzialnych za poszczególne aktywa.

2. Kolejnym krokiem jest identyfikacja wszystkich zagrożeń i podatności związanych z poszczególnymi aktywami. Poszczególne aktywa mogą być związane z więcej niż jednym zagrożeniem, a każde zagrożenie może być związane z więcej niż jedną podatnością.

Tabela nr 1- Zestawienie aktywów

Aktywa								
L.p.	Rodzaj (id)	ID	Opis grupy aktywów	Właściciel	Atrybuty bezpieczeństwa			Wartość (P + I + D)
					P	I	D	

§ 8

Identyfikowanie potencjalnych zagrożeń i podatności

Ocena ryzyka - przeprowadzana jest dla każdego zidentyfikowanego podczas inwentaryzacji aktywa - rozpatruje trzy obszary:

1) prawdopodobieństwo wystąpienia zagrożenia (**Pr**),
2) podatność aktywów na zagrożenia (**Po**),
3) skutków potencjalnych zagrożeń (**Sk**),

biorąc pod uwagę następstwa naruszenia lub utraty:

1) poufności (P),
2) integralności (I),
3) dostępności (D),

które mogą nastąpić w wyniku działań:

1) umyślnych (U)
2) przypadkowych (P)
3) naturalnych (N)

Przyjmuje się, że zagrożenia „U/P" są wynikiem działań ludzkich, natomiast źródła zagrożeń „N" są niezależne od człowieka.

Listę potencjalnych i realnych dla Organizacji zagrożeń umieszczono w Tabeli nr 2. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa, podatności oraz skutków zdarzeń.

Uwaga:

Należy uwzględnić, że podatność nie powoduje jeszcze szkody, ale należy zgodnie z Tabelą nr 3 oszacować stopień zabezpieczenia aktywa pod kątem zidentyfikowanych zagrożeń.

Tabela nr 2 - Zestawienie zagrożeń

ZAGROŻENIA

L.p.	Rodzaj / Grupa	ID	Zagrożenie	Możliwe naruszenie atrybutów bezpieczeństwa: (Poufność / Integralność / Dostępność)

Tabela nr 3 - Zestawienie podatności i przykłady odpowiadającym im zagrożeń

PODATNOŚCI

L.p.	Rodzaj	ID	Podatność	Przykłady zagrożeń

§ 9

Zagrożenia utraty atrybutów bezpieczeństwa

Ustalono reprezentatywny zestaw **potencjalnych zagrożeń** utraty poszczególnych atrybutów bezpieczeństwa tj. poufności, integralności i dostępności, dla których przeprowadzono szacowanie ryzyka:

Zagrożeniami dla **poufności (P)** informacji są np.:

1) ujawnienie informacji
2) wynoszenie materiałów poza obszar
3) pozostawianie dokumentów i/lub otwartych aplikacji
4) niezamykanie pomieszczeń i/lub sejfów
5) nieuprawnione przeglądanie zasobów
6) podgląd edytowanych tekstów
7) błędy użytkowników i administratora
8) zainfekowanie złośliwym oprogramowaniem
9) przełamanie haseł dostępu
10) podsłuch podczas dyktowania treści dokumentów
11) błędy oprogramowania

Zagrożeniami dla **integralności (I)** informacji są np.:

1) fizyczne zniszczenie aktywów
2) dywersja i terroryzm
3) klęski żywiołowe

4) usunięcie części danych
5) kradzież sprzętu i oprogramowania
6) awaria komputerów i serwerów
7) awarie instalacji elektrycznej
8) awarie instalacji CO
9) błędy użytkowników i administratora
10) zainfekowanie złośliwym oprogramowaniem
11) błędy oprogramowania

Zagrożeniami dla **dostępności** (D) informacji są np.:
1) fizyczne zniszczenie aktywów
2) klęski żywiołowe
3) utrata dostępu do Internetu
4) zmiana zawartości zgromadzonych danych
5) usunięcie części danych
6) kradzież sprzętu i oprogramowania
7) awarie komputerów i serwerów
8) awaria urządzeń sieci LAN
9) awarie instalacji elektrycznej
10) błędy użytkowników i administratora
11) zainfekowanie złośliwym oprogramowaniem
12) przełamanie haseł dostępu
13) błędy oprogramowania

VI.
METODYKA OCENY RYZYKA

§ 10

1. Sposób oceny ryzyka został ustanowiony w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w Organizacji oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka.
2. Za dane wejściowe do procesu oceny ryzyka uważa się wszelkie informacje przedstawione w analizie ryzyka (dane z inwentaryzacji aktywów) a w szczególności miejsce, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywu. Każde szacowanie prawdopodobieństwa, podatności oraz skutków zdarzenia powinno się odbywać w relacji z Tabelą nr 2 i 3 według zadanych kryteriów:

Tabela nr 4 - Szacowanie prawdopodobieństwa

Kryterium	Ryzyko	Wartość
(Pr) Prawdopodobieństwo (możliwość wystąpienia)	niskie, odległe, mało realne szanse na zdarzenie	1
	może się zdarzyć lub zdarza się sporadycznie	2
	bardzo realne szanse wystąpienia	3

Tabela nr 5 - Szacowanie podatności

Kryterium	Ryzyko	Wartość
(Po) Podatność *(słabość aktywu)*	aktywa bardzo dobrze zabezpieczone	1
	aktywa dostatecznie zabezpieczone	2
	aktywa słabo lub nie zabezpieczone	3

Tabela nr 6 - Szacowanie skutków

Kryterium	Ryzyko	Wartość
(Sk) Skutek *(wpływ na Organizację i/lub proces)*	utrata danych nie spowoduje utrudnień w pracy Organizacji lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu	1
	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku Organizacji, odtworzenie danych jest możliwe ale pracochłonne	2
	utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne, odtworzenie danych i reputacji będzie trudne i kosztowne	3

§ 11

Kategoria Ryzyka

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:

R = Pr * Po * Sk

gdzie:

R - ryzyko

Pr – prawdopodobieństwo

Po – podatność

Sk – skutek

Wynik otrzymany wg powyższego wzoru należy przypisać ustanowionym kategoriom ryzyka (zgodnie z poniższą tabelą), a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego.

Uwaga: W uzasadnionych przypadkach Organizacja może zaakceptować ryzyko kategorii drugiej lub trzeciej szczególnie, gdy działania profilaktyczne odnoszą się do długoterminowych i kosztownych inwestycji na rzecz bezpieczeństwa danego aktywu.

Tabela nr 7- Wytyczne do postępowania z ryzykiem

Klasa Kategori i Ryzyka	Kategoria Ryzyka	Wartość Ryzyka	Akceptacja Ryzyka Tak / Nie	Działania zapobiegawcze
1	Małe	1÷ 7	TAK	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące
2	Średnie	8 ÷ 17	**NIE**	Należy zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne
3	Wysokie	18 ÷ 27	**NIE**	Należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne

§ 12

Identyfikacja ryzyka

1. Proces oszacowania ryzyka został opracowany w oparciu o macierz występujących zagrożeń dla poufności, dostępności i integralności dla zidentyfikowanych aktywów. W podejściu tym ryzyko szacowane jest jakościowo w oparciu o wybrany poziom wymagań bezpieczeństwa.
2. W wierszach macierzy wyszczególniane są aktywa podlegające ochronie. Kolumny przedstawiają ryzyka, jakie zagrażają integralności, poufności i dostępności tych aktywów.
3. W poszczególne komórki macierzy wpisywane są rezultaty oszacowania:
   1) prawdopodobieństwa (Pr) wystąpienia zdarzenia
   2) skutków (Sk) utraty atrybutów bezpieczeństwa informacji,
   3) podatności/słabości) (Po) aktywu na zidentyfikowane zagrożenie,

4) wyniki obliczonego ryzyka (R) dla każdego aktywu.

Tabela nr 8 - Tabela szacowania ryzyka (Macierz ryzyka)

ANALIZA RYZYKA / MACIERZ RYZYKA (wybrane aktywa)

Kategoria ryzyka – Średnia – Wysoka

Zagrożenie (l.p. / ID / Opis / Naruszone atrybuty)

L.p.	Aktywa	Szacowanie*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			ZF1	ZF2	ZF3	ZF8	ZN1	ZU1	ZU2	ZU3	ZU4	ZI1	ZI2	ZI3	ZI4	ZI5	ZI6	ZI7	ZI8
			Zniszczenie urządzeń lub nośników	Zalanie	Pożar	Atak hakerski/socjotechniczny	Klęska żywiołowa (burza, orkan, powódź)	Utrata dostaw prądu	Utrata dostępu do Internetu	Utrata połączenia telefonicznego	Utrata usług wsparcia (np. technicznego)	Ujawnienie informacji	Wynoszenie materiałów poza obszar	Zmiana zawartości danych	Usunięcie części danych	Kradzież sprzętu, oprogramowania i danych	Podsłuch bądź przechwyt danych	Kopiowanie, podmiana bądź niszczenie plików	Pokonanie zabezpieczeń fizycznych pomieszczeń
			I, D	I, D	I, D	I, D	I, D	I, D	D	D	D	P	P, D	I, D	I, D	I, D	P	P, I, D	P, I, D

L.p.	Aktywa	Szacowanie*	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
			ZI11	ZI12	ZI13	ZT1	ZT2	ZT3	ZT4	ZT5	ZD3	ZD5	ZD6	ZB1	ZB2	ZB3	ZB5	ZB6
			Nadużycie prawa	Pozostawianie dokumentów i/lub otwartych aplikacji	Niezamykanie pomieszczeń i/lub sejfów	Awaria serwerów	Awaria komputerów PC	Awaria urządzeń sieci LAN	Awaria instalacji elektrycznej	Awaria instalacji co	Nieuprawniony dostęp do systemów IT	Nieautoryzowany dostęp do sieci	Nieautoryzowany dostęp fizyczny	Błędy użytkowników / administratorów	Zainfekowanie złośliwym oprogramowaniem	Przełamanie haseł dostępu	Przeciążenie systemu IT np. ataki typu ddos/dos	Błędy oprogramowania
			P	P	P	I, D	D	D	I, D	I	P	P	P	P, I, D	P, I, D	P, D	D	P, I, D

§ 13

Identyfikacja ryzyka

1. Tabela szacowania ryzyka ilustruje obszary poziomów zagrożenia dla bezpieczeństwa informacji w Organizacji.
2. Najistotniejsze obszary zakwalifikowane zostały jako ryzyko „Wysokie" i określone kolorem czerwonym.
3. W związku z kwalifikacją określonych ryzyk jako „Wysokich" odpowiednie aktywa objęte są szczególnym nadzorem gdyż wystąpienie wskazanych zagrożeń może zagrozić poważnie poufności, integralności lub dostępności informacji.
4. Obszary oznaczone kolorem żółtym określone zostały jako ryzyko „Średnie" i ich kwalifikacja wiąże się ze średnim prawdopodobieństwem wystąpienia bądź wpływu na bezpieczeństwo informacji.
5. Wartości prawdopodobieństwa wystąpienia zdarzeń/zagrożeń oraz ich wpływu na działalność Organizacji powzięto na podstawie aktualnych uwarunkowań sprzętowych oraz kadrowych podczas przeprowadzenia audytu.
6. W Organizacji podejmowane są działania zgodnie z procedurą zarządzania ryzykiem. Istotnym ich elementem jest zabezpieczanie środków finansowych oraz organizacyjnych niezbędnych do redukowania zagrożeń polegających na zmniejszeniu prawdopodobieństwa wystąpienia zdarzenia oraz w przypadku jego wystąpienia ograniczeniu wpływu na Organizację. Dotyczy to wszystkich obszarów i zidentyfikowanych ryzyk.

VII.
PLAN POSTĘPOWANIA Z RYZYKIEM

§ 14

1. Przyjmuje się warianty postępowania z ryzykiem:
   1) modyfikowanie

2) zachowanie
3) unikanie
4) dzielenie

§ 15

Działania doskonalące bezpieczeństwo informacji

1. Procesy doskonalące bezpieczeństwo informacji prowadzone są w oparciu o podjęte działania zapobiegawcze i/lub korygujące adekwatnie do wagi potencjalnych problemów. W wyniku tych działań należy według powyższych zasad powtórnie dokonać analizy w celu sprawdzenia skuteczności i odporności aktywu na przypadek zaistnienia zadanych w pierwszej fazie oceny zagrożeń naruszających poufność, integralność i dostępność.
2. Wynik z powtórnej analizy stanowi o ryzyku szczątkowym, które jest pozostałością po podjęciu wszystkich możliwych kroków zmierzających do unikania ryzyka, jego kontrolowania lub przeniesienia (transferu).
3. Wprowadza się działania doskonalące wskazane w poniższej tabeli:

Tabela nr 9 - Działania doskonalące

PROPONOWANE DZIAŁANIA DOSKONALĄCE

Lp.	Aktywa	Zagrożenie / Proponowane działanie korygujące	Zagrożenie (I.p. / ID / Opis / Naruszone atrybuty)																														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	30	31	32	33	34
			ZF1 Zniszczenie urządzeń lub nośników	ZF2 Zalanie	ZF3 Pożar	ZF6 Atak hakerski/cyberterroryzm	ZH1 Klęska żywiołowa (burza, orkan, powódź)	ZU1 Utrata dostaw prądu	ZU2 Utrata dostępu do Internetu	ZU3 Utrata połączenia telefonicznego	ZU4 Utrata usług wsparcia (np. technicznego)	ZI1 Ujawnienie informacji	ZI2 Wynoszenie materiałów poza obszar	ZI3 Zmiana zawartości danych	ZI4 Usunięcie części danych	ZI5 Kradzież sprzętu, oprogramowania i danych	ZI6 Podsłuch bądź przetwyt danych	ZI7 Kopiowanie, podmiana bądź niszczenie plików	ZI8 Pokonanie zabezpieczeń fizycznych pomieszczeń	ZI11 Nadużycie prawa	ZI12 Przestawianie dokumentów i/lub otwartych szafek	ZI13 Niezamykanie pomieszczeń i/lub szaf/biurek	ZT1 Awaria serwerów	ZT2 Awaria komputerów PC	ZT3 Awaria urządzeń sieci LAN	ZT4 Awaria instalacji elektrycznej	ZT5 Awaria instalacji co	ZD3 Nieuprawniony dostęp do systemów IT	ZD5 Niekontrolowany dostęp do sieci	ZD6 Nieautoryzowany dostęp fizyczny	ZB1 Błędy użytkowników / administratorów	ZB2 Zainfekowanie złośliwym oprogramowaniem	ZB3 Przestawianie nastaw dostępu	ZB5 Przeciążenie systemu IT np. atak typu ddos	ZB6 Błędy oprogramowania
			I, D	I, D	I, D	I, D	I, D	I, D	D	D	D	P	P, D	I, D	I, D	I, D	P	P, I, D	P, I, D	P	P	P	I, D	D	D	I, D	I	P	P	P	P, I, D	P, I, D	P, D	D	P, I, D

§ 16

Wprowadzanie zmian

1. Dokonywanie zmian w ocenie ryzyka odbywa się w wyniku każdorazowego podjęcia działań korygujących i/lub zapobiegawczych, zidentyfikowania nowego - realnego zagrożenia oraz dokonanego incydentu naruszającego bezpieczeństwo informacji.
2. Zapisy sporządzone w ocenie ryzyka nie ulegają przedawnieniu i są trwałe, w związku z czym każde działanie mające na celu ponowną ocenę ryzyka bezwzględnie dokonuje się w kolejnym cyklu analizy.

PREZES ZARZĄDU
Jan Kretowicz