

**Zarządzenie Nr 27/2020**

**Rektora Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie**

**z dnia 01 kwietnia 2020 roku**

**w sprawie: przyjęcia Polityki zarządzania ryzykiem w obszarze ochrony danych osobowych**

Działając na podstawie art. 23 ust. 2 pkt. 2 ustawy z dnia 20 lipca 2018 roku - Prawo szkolnictwie wyższym i nauce (t.j. Dz.U. z 2020 roku, poz. 85)

zarządza się co następuje:

**§1**

W Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie, wprowadzona zostaje **Polityka zarządzania ryzykiem w obszarze ochrony danych osobowych**, stanowiąca załącznik do zarządzenia.

**§ 2**

Do przestrzegania Polityki zobowiązani są wszyscy pracownicy i współpracownicy Uczelni mający dostęp do danych osobowych.

**§ 3**

Za nadzór merytoryczny nad realizacją Zarządzenia odpowiada Inspektor Ochrony Danych Osobowych, za nadzór techniczny i organizacyjny odpowiada Kanclerz.

**§ 4**

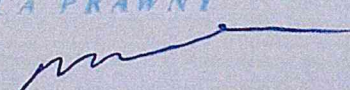
Zarządzenie wchodzi w życie z dniem podpisania.

Z upoważnienia Rektora

**PROREKTOR**

  
dr inż. Grzegorz Koc

**RADCA PRAWNY**

  
Dorota Nadratowska-Malinowska

Załącznik do Zarządzenia nr 27/2020  
Rektora PUZ im. Ignacego Mościckiego  
z dnia 01.04.2020r.

# **POLITYKA ZARZĄDZANIA RYZYKIEM W OBSZARZE OCHRONY DANYCH OSOBOWYCH**



**PAŃSTWOWA UCZELNIA ZAWODOWA**  
**im. Ignacego Mościckiego**  
**w Ciechanowie**

Ciechanów, kwiecień 2020r.

## Postanowienia ogólne

### § 1.

Polityka zarządzania ryzykiem w obszarze ochrony danych osobowych u **Administradora danych osobowych** opisuje model zarządzania ryzykiem oraz określa jego ogólne zasady.

## Ogólne zasady zarządzania ryzykiem

### § 2.

1. Zarządzanie ryzykiem w kontekście ochrony danych osobowych jest procesem ciągłym.
2. Celem zarządzania ryzykiem jest wdrożenie odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie danych odbywało się zgodnie z RODO (ROZPORZĄDZENIEM PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
3. Zarządzanie ryzykiem powinno prowadzić do eliminacji lub ograniczenia - do akceptowanego poziomu - prawdopodobieństwa i następstw wystąpienia zdarzeń negatywnych.
4. Ilekroć w niniejszej procedurze jest mowa o:
  - 1) **analizie ryzyka** - rozumie się przez to identyfikowanie i opisywanie ryzyka oraz oszacowanie wielkości jego następstw i prawdopodobieństwa przy uwzględnieniu skuteczności istniejących zabezpieczeń, zastosowanych organizacyjnych, logicznych i technicznych środków bezpieczeństwa,
  - 2) **następstwach, skutkach naruszenia praw lub wolności dla osób fizycznych** - zidentyfikowane reakcje dla określonych procesów przetwarzania danych (np.: kradzież tożsamości),
  - 3) **organizacyjnych i technicznych środkach bezpieczeństwa, mechanizmach kontrolnych** - rozumie się przez to polityki, zarządzenia, procedury, instrukcje, praktyki, fizyczne i techniczne środki zabezpieczeń, systemy, zaprojektowane i wdrożone w celu ograniczenia prawdopodobieństwa wystąpienia i/lub następstw ryzyka; podstawowy zestaw mechanizmów kontrolnych, nie stanowiący katalogu zamkniętego,
  - 4) **procesie** - rozumie się przez to ciąg czynności zaprojektowanych, a następnie wykonywanych w ten sposób, aby w ich wyniku powstał produkt lub usługa,
  - 5) **rejestrze ryzyka** - rozumie się przez to zestawienie zawierające informacje o wyniku przeprowadzonej identyfikacji i oceny ryzyka, a także proponowanej reakcji na ryzyko,
  - 6) **ryzyku** - rozumie się przez to zagrożenie związane ze zdarzeniem lub działaniem, które wpłynie na zdolność organizacji do realizacji skutecznej ochrony danych,
  - 7) **właścicielu ryzyka** - rozumie się przez to podmiot odpowiedzialny za zarządzanie danym ryzykiem; właścicielem ryzyka w organizacji jest Administrator danych lub właściciel procesu odpowiedzialny za realizację procesu, do którego odnosi się to

ryzyko,

- 8) **zarządzaniu ryzykiem** - rozumie się przez to działania podejmowane w celu identyfikacji, oceny, określenia reakcji na ryzyko, a także skoordynowanych działań dotyczących jego minimalizacji.

### **Identyfikacja ryzyka**

#### **§ 3.**

1. Identyfikacja ryzyka polega na rozpoznaniu, określeniu i opisanu ryzyk, które mogą wystąpić, jako przeszkody w realizacji zadań/procesów związanych z ochroną danych.
2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia związane z wystąpieniem jakiegokolwiek zdarzenia, działania lub braku działania, które może mieć negatywny wpływ dla osób fizycznych, których dane są przetwarzane w organizacji.
3. Podczas identyfikacji należy odnieść się w szczególności do:
  - 1) procesów dotyczących przetwarzania danych osobowych,
  - 2) celu przetwarzania danych osobowych,
  - 3) kategorii osób, których dane dotyczą,
  - 4) zakresu danych identyfikujących osobę fizyczną,
  - 5) możliwości przetwarzania danych szczególnie chronionych,
  - 6) odbiorców danych i sposobów wykorzystywania przez nich danych z uwzględnieniem ujawnianego ich zakresu,
  - 7) okresu retencji danych.
4. Identyfikacja ryzyka powinna prowadzić do możliwie dokładnego ustalenia charakteru ryzyka i jego zakresu, co umożliwi wybór i podjęcie we właściwym czasie odpowiednich czynności zapobiegawczych bądź też ograniczających wpływ ryzykownych działań.
5. Identyfikacja powinna uwzględniać ryzyko znane powszechnie oraz nowo identyfikowane - aktualizowane.
6. Identyfikacji podlega zarówno ryzyko wewnętrzne, mające swoje źródło w działaniach podejmowanych przez pracowników organizacji, jak i ryzyko zewnętrzne, wynikające z czynników zewnętrznych.
7. Identyfikacja ryzyka powinna uwzględniać wyniki z przeprowadzonych w organizacji audytów i kontroli: zarówno wewnętrznych, jak i zewnętrznych.

### **Analiza ryzyka**

#### **§ 4.**

1. Wszystkie zidentyfikowane rodzaje ryzyka poddawane są całościowej analizie.
2. Proces analizy ryzyka ma charakter subiektywnej oceny dokonywanej przez osoby uprawnione do analizy ryzyka.
3. Ocena poszczególnych rodzajów ryzyka odbywa się w oparciu o przyjęty w Procedurze model oceny ryzyka, zapewniający porównywalność wyników we wszystkich obszarach funkcjonowania organizacji oraz ułatwiający przetwarzanie i łączenie indywidualnych ocen w celu stworzenia ogólnego profilu ryzyka.

4. Celem analizy ryzyka jest jego pomiar, polegający na określeniu prawdopodobieństwa wystąpienia danego rodzaju ryzyka oraz jego następstw / wpływu.
5. Ocena zarówno prawdopodobieństwa, jak i następstw polega na nadaniu im wartości szacunkowych w przyjętych skalach jakościowo-ilościowych.
6. W analizie ryzyka uwzględnia się częstotliwość wystąpienia ryzyka (liczbę możliwych powtórzeń), jako jeden ze wskaźników prawdopodobieństwa wystąpienia ryzyka.
7. Na podstawie oszacowanego prawdopodobieństwa oraz następstw określa się współczynnik istotności każdego zidentyfikowanego rodzaju ryzyka - poziom istotności, który pokazuje się jako iloczyn prawdopodobieństwa i następstw ryzyka.
8. Określenie współczynnika istotności ryzyka umożliwia dokonanie oceny istotności ryzyka i pozwala na uporządkowanie listy zidentyfikowanych i oszacowanych rodzajów ryzyka według kryterium ich znaczenia dla ewentualnych naruszeń praw lub wolności osób fizycznych.
9. Dla poszczególnych rodzajów zidentyfikowanego i oszacowanego ryzyka wskazuje się rozwiązania (w tym obowiązujące przepisy prawa oraz przyjęte w organizacji procedury, instrukcje i faktycznie podejmowane działania), które mają na celu ograniczenie prawdopodobieństwa lub następstw wystąpienia ryzyka.
10. W razie potrzeby wskazuje się propozycje modyfikacji stosowanych w organizacji rozwiązań lub zgłasza się propozycje nowych rozwiązań (mechanizmów i uregulowań wewnętrznych), których zaplanowanie i wdrożenie w organizacji jest konieczne dla ograniczenia ryzyka.

### **Przykłady zagrożeń ryzyk, następstw**

#### **§ 5.**

Biorąc pod uwagę specyfikę prac wykonywanych przy pomocy systemu informatycznego, przeznaczonego do przygotowywania dokumentów zawierających dane osobowe, podstawowe zagrożenia to: **utrata poufności, integralności i rozliczalności**.

1. **Poufność** to zapewnienie, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.

Zagrożenia w zakresie poufności obejmują:

- 1) nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe (pozostawianie drzwi niezamkniętych na klucz),
- 2) ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe,
- 3) nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- 4) utrata nośnika zawierającego dane osobowe,
- 5) klęska żywiołowa, w wyniku której utracono poufność danych osobowych,
- 6) nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

2. **Integralność** to zapewnienie, aby wszelkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były skutkiem zaplanowanych działań użytkowników systemu; właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Zagrożenia w zakresie rozliczalności obejmują:

- 1) brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
- 2) wprowadzenie zmian w treści dokumentu zawierającego dane osobowe,
- 3) błędy oprogramowania lub sprzętu.

3. **Rozliczalność** to właściwość zapewniająca, że działania podmiotu przetwarzającego dane osobowe mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Zagrożenia w zakresie integralności obejmują:

- 1) nielegalny dostęp danych osobowych, w tym do stanowiska komputerowego,
- 2) błędy, pomyłki,
- 3) brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika,
- 4) wadliwe działanie systemu operacyjnego,
- 5) wirus,
- 6) brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.

#### 4. Źródła zagrożeń

Źródłami zagrożeń dla stanowisk komputerowych, na których przetwarza się dane osobowe mogą być:

- 1) siły natury – zdarzenia, które nie wynikają z działalności człowieka, tzn. uderzenie pioruna, pożar będący konsekwencją uderzenia pioruna, starzenie się sprzętu, starzenie się nośników pamięci, kurz, katastrofy budowlane, ulewny deszcz, huragan, ekstremalne temperatury, wilgotność,
- 2) ludzie – mogą to być pracownicy lub osoby z zewnątrz, którzy działają w sposób celowy lub przypadkowy; zagrożenia te, to przede wszystkim: błędy i pomyłki użytkowników, błędy i pomyłki administratorów, błędy utrzymania systemu w poufności, integralności i rozliczalności, zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu, zagubienie nośnika zawierającego dane osobowe, niewłaściwe zniszczenie nośnika, nielegalne użycie oprogramowania, choroba ważnych osób i nieuprawnione zastępstwo, epidemia kadry i brak osób upoważnionych do dostępu, podpalenie obiektu, zalanie wodą, katastrofa budowlana będąca konsekwencją działania człowieka, zakłócenia elektromagnetyczne, radiotechniczne, podłożenie i wybuch ładunku wybuchowego, użycie broni, zmiany napięcia w sieci, utrata prądu, zbieranie się ładunków elektrostatycznych, utrata

kluczowych pracowników, niedobór pracowników, defekty oprogramowania, szpiegostwo, terroryzm, wandalizm, destrukcja zbiorów i programów impulsem elektromagnetycznym, kradzież, włamanie do systemu, wyłudzenie, fałszowanie dokumentów, podszycie się pod uprawnionego użytkownika, podsłuch, użycie złośliwego oprogramowania, wykorzystanie promieniowania ujawniającego.

Każde z ww. zagrożeń wynikających z działalności człowieka może być ograniczone poprzez:

- 1) rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi,
- 2) fizyczne zabezpieczenie obiektu (pomieszczeń), w którym działa system,
- 3) wdrożenie systemu kontroli użytkowników,
- 4) brak połączenia stanowisk komputerowych systemu z siecią internetową.

Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajdują się stanowisko komputerowe, na których przetwarza się dane osobowe.

### **Prawdopodobieństwo wystąpienia ryzyka**

#### **§ 6.**

1. Oceniając prawdopodobieństwo wystąpienia ryzyka, uwzględnia się możliwą częstotliwość wystąpienia zdarzenia (jak często dane zdarzenie może mieć miejsce). W odniesieniu do czynności powtarzalnych (spraw występujących cyklicznie lub wielokrotnie) uwzględnia się liczbę możliwych powtórzeń (ile razy względem ogólnej liczby spraw zdarzenie może mieć miejsce).
2. Jakościową ocenę prawdopodobieństwa wystąpienia ryzyka wyraża się zarówno procentowo, jak również ilościowo (punktowo), poprzez nadanie prawdopodobieństwu - oszacowanemu w sposób jakościowy - wartości w skali od 1 do 5, gdzie:
  - 1 - oznacza prawdopodobieństwo znikome (0-20%)
  - 2 - oznacza prawdopodobieństwo niskie (21-40%)
  - 3 - oznacza prawdopodobieństwo średnie (41-60%)
  - 4 - oznacza prawdopodobieństwo wysokie (61-80%)
  - 5 - oznacza prawdopodobieństwo bardzo wysokie (81-100%)

## WYTYCZNE DO OCENY PRAWDOPODOBIEŃSTWA WYSTĄPIENIA I NASTĘPSTW RYZYKA

| Skala prawdopodobieństwa wystąpienia ryzyka                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  | Skala następstw ryzyka |                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------------|-----------------------------------------|
| Prawdopodobieństwo wystąpienia                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  | Oszacowane ryzyko      | Następstwa (wpływ)<br>Oszacowane ryzyko |
| Tego typu ryzyko do tej pory jeszcze nigdy nie wystąpiło, <b>lub/i</b> ,<br>Przy realizacji danego procesu / zadania nie współpracuje się z innymi komórkami/jednostkami, <b>lub/i</b> ,<br>W ostatnich 3 latach obszar/proces nie podlegał zmianom technologicznym, organizacyjnym i kadrowym, <b>lub/i</b> ,<br>Oceniany obszar/proces uregulowany jest wyłącznie regulacjami wewnętrznymi.                                                                                                                                                                                                                                                                                                                               |  | 1<br>znikome           | 1<br>nieznaczące                        |
| Tego typu ryzyko wystąpiło 1 raz w okresie ostatnich 3 lat. Ryzyko prawdopodobnie nie wystąpi/może wystąpić w zupełnie wyjątkowych sytuacjach, <b>lub/i</b> ,<br>Przy realizacji danego zadania/procesu współpracuje się z małą (1 lub 2) liczbą komórek/jednostek, <b>lub/i</b> ,<br>W okresie ostatnich 3 lat obszar/proces podlegał zmianom technologicznym, organizacyjnym i kadrowym w minimalnym stopniu i uznaje się je za wdrożone, <b>lub/i</b> ,<br>Zadania/proces w małym zakresie objęty regulacjami o charakterze zewnętrznym. Nie podlegały one zmianom.                                                                                                                                                      |  | 2<br>niskie            | 2<br>małe                               |
| Tego typu ryzyko wystąpiło 2 razy w okresie ostatnich 3 lat, <b>lub/i</b> ,<br>Przy realizacji danego celu współpracuje się z dużą (co najmniej 3) liczbą komórek/jednostek, <b>lub/i</b> ,<br>Zadanie/proces podlegał zmianom organizacyjnym, technologicznym i kadrowym, które zakończyły się ponad rok temu, <b>lub/i</b> ,<br>Zadanie/proces objęty w małym stopniu regulacjami zewnętrznymi, które mogły podlegać w ostatnim okresie pewnym zmianom.                                                                                                                                                                                                                                                                   |  | 3<br>średnie           | 3<br>średnie                            |
| Tego typu ryzyko wystąpiło 3 razy w okresie ostatnich 3 lat. Istnieje wysokie prawdopodobieństwo na wystąpienie tego ryzyka, <b>lub/i</b> ,<br>Zadanie/proces wymaga współpracy z dużą (więcej niż 3) liczbą komórek i jednostek lub/i podmiotami zewnętrznymi, <b>lub/i</b> ,<br>W ciągu ostatniego roku obszar/proces podlegał zmianom technologicznym, organizacyjnym i kadrowym, z których część może wymagać poprawek i działań dostosowawczych, <b>lub/i</b> ,<br>Obszar/proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych), które w ostatnim roku podlegały istotnym zmianom.                                                                                                                |  | 4<br>wysokie           | 4<br>poważne                            |
| Tego typu ryzyko wystąpiło więcej niż 3 razy w okresie ostatnich 3 lat. Istnieje bardzo wysokie prawdopodobieństwo na wystąpienie tego ryzyka, <b>lub/i</b> ,<br>Zadanie/proces wymaga współpracy z bardzo dużą (więcej niż 10) liczbą komórek i jednostek lub/i podmiotami zewnętrznymi, <b>lub/i</b> ,<br>W ostatnim roku zadanie/proces podlegał istotnym zmianom technologicznym, organizacyjnym i kadrowym albo obszar podlega częstym zmianom tego typu bądź też obszar jest w trakcie zmian, <b>lub/i</b> ,<br>Obszar/proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych), które w ostatnim roku podlegały istotnym zmianom lub/i, które zmieniają się z pewnością w ciągu najbliższego roku. |  | 5<br>bardzo wysokie    | 5<br>katastrofalne                      |

## Następstwo (wpływ)

### § 6.

1. Jakościowa ocena następstw ryzyka opiera się na oszacowaniu potencjalnych skutków, jakie zaistnienie danego rodzaju ryzyka (zdarzenia) może mieć na organizacji. Uwzględnia się przy tym w szczególności konsekwencje prawne, finansowe i organizacyjne zaistnienia danego zdarzenia oraz jego wpływ na prawa bądź wolności dla osób fizycznych.
2. Jakościową ocenę możliwych następstw wystąpienia ryzyka można wyrazić ilościowo (punktowo), poprzez nadanie rozmiarom następstw - oszacowanym w sposób jakościowy - wartości w skali od 1 do 5, gdzie:
  - 1 - oznacza skutek nieznaczny
  - 2 - oznacza skutek mały
  - 3 - oznacza skutek średni
  - 4 - oznacza skutek poważny
  - 5 - oznacza skutek katastrofalny

## Istotność

### § 7.

1. Określenie prawdopodobieństwa (PR) i następstw (N) ryzyka w skalach pięciostopniowych umożliwia ustalenie współczynnika poziomu istotności ryzyka (IR) jako iloczynu (wyrażonych punktowo) prawdopodobieństwa wystąpienia ryzyka oraz następstw:

$$IR = PR \times N$$

gdzie:

IR - współczynnik istotności ryzyka

PR - prawdopodobieństwo wystąpienia ryzyka

N - potencjalne następstwa wystąpienia ryzyka.

2. Przyjęty wzór dla obliczenia współczynnika istotności ryzyka zakłada, że poziom zagrożenia w każdym wypadku zależy zarówno od prawdopodobieństwa wystąpienia ryzyka, jak i od następstw, a więc że ryzyko bardzo prawdopodobne, ale wywołujące niewielkie skutki, może mieć podobny stopień istotności, jak ryzyko mało prawdopodobne, ale o poważnych przewidywanych skutkach.
3. Z uwagi na pięciostopniową skalę zarówno prawdopodobieństwa, jak i następstw ryzyka współczynnik istotności danego rodzaju ryzyka może przyjąć wartość od 1 do 25.
4. Mapę ryzyka - matrycę punktowej oceny (współczynnika) istotności ryzyka, zawierającą prezentację ryzyka w macierzy "5x5", przedstawia załącznik nr 2 do niniejszej Procedury.

## Podatność na zagrożenia

### § 8.

Zagrożenia dla systemu teleinformatycznego i przetwarzanych w nim informacji zostały sklasyfikowane następująco:

1. Siły wyższe (klęski żywiołowe, katastrofy finansowe, zmiany prawa, etc.) – możliwe skutki: zniszczenie informacji i zasobów fizycznych, utrata dostępności, obniżenie poziomu ochrony.
2. Działania przestępcze, w tym:
  - 1) zagrożenia związane z kradzieżą fizyczną i zagubieniem sprzętu, oprogramowania i dokumentów – możliwe skutki: głównie utrata dostępności i poufności informacji,
  - 2) zagrożenia związane z podsłuchami różnego typu (wykorzystanie „klasycznych” technik szpiegowskich) sprzętu i oprogramowania – możliwe skutki: utrata poufności informacji,
  - 3) nieuprawnione działania personelu – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony,
  - 4) uprawnione działania osób postronnych – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony.
3. Błędy personelu obsługującego system komputerowy – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony.
4. Skutki złej organizacji pracy, w tym zagrożenia związane z błędami w ochronie fizycznej i technicznej – możliwość utraty dostępności, integralności i poufności.
5. Zagrożenia związane z awariami i uszkodzeniami sprzętu i wadami oprogramowania – możliwe skutki: głównie utrata dostępności informacji oraz obniżenie poziomu ochrony.

W związku z procesem szacowania ryzyka wymienione są możliwe zagrożenia dla poszczególnych zasobów, tak, aby usprawnić ten proces i zwizualizować potencjalne straty.

## 1. Sprzęt

- 1) nieuprawnione kopiowanie danych z dysku lub innych nośników informacji,
- 2) korzystanie z nielicencjonowanego oprogramowania,
- 3) użycie oprogramowania w nieuprawniony sposób,
- 4) uszkodzenie sprzętu komputerowego (drukarka, karta sieciowa, jednostka centralna, klawiatura, mysz, itp.) oraz łączy transmisyjnych,
- 5) uszkodzenie fizyczne nośników danych,
- 6) uszkodzenia sprzętu podczas wykonywania napraw i konserwacji przez niewyszkolonych pracowników,
- 7) starzenie się nośników danych,
- 8) wejście do systemu operacyjnego z wykorzystaniem obcego identyfikatora,
- 9) drukowanie danych osobowych na jednej, ogólnie dostępnej drukarce,
- 10) nieuprawniony dostęp do procesu przetwarzania danych:
  - włamanie do strefy bezpieczeństwa po godzinach pracy,
  - wykorzystanie pozostawionych fragmentów tworzonych dokumentów w pamięci RAM komputera .

## 2. Ludzie

- 1) kradzież dokumentów papierowych lub elektronicznych,
- 2) kradzież dysku twardego komputera,
- 3) zagubienie dokumentów lub utrata przetwarzanych informacji,
- 4) stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników,

- 5) infiltracja środowiska przez wyszukiwanie osób uważających się za pokrzywdzone przez pracodawcę, zwalnianych lub poszukujących zatrudnienia w innej komórce organizacyjnej,
- 6) podglądanie zawartości ekranu monitora przez użytkowników z innych komputerów
- 7) włamanie do systemu – podszycie się pod uprawnionego użytkownika,
- 8) wyłudzenie, fałszowanie dokumentów, kart dostępu, haseł dostępu itp. ,
- 9) nieuprawniona, świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
- 10) skorzystanie z cudzego identyfikatora i hasła,
- 11) dostęp nieuprawnionych użytkowników do informacji prezentowanej na ekranie stanowiska komputerowego,
- 12) błędy popełniane przez użytkowników,
- 13) wejście osoby nieupoważnionej do strefy administracyjnej,
- 14) zaniedbania ze strony personelu obsługującego proces przetwarzania danych,
- 15) utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwacyjnych,
- 16) odczytanie informacji z nośników przewidzianych do naprawy,
- 17) podgląd dokumentów przetwarzanych przez poprzedniego użytkownika,
- 18) zapisywanie informacji niejawnych na prywatne nośniki informacji użytkownika,
- 19) nieuprawnione kopiowanie danych z dysku twardego,
- 20) przeglądanie (przeszukiwanie) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji,
- 21) nieuprawniony dostęp do procesu przetwarzania danych,
- 22) włamanie do strefy bezpieczeństwa po godzinach pracy,
- 23) utrata kluczowych pracowników,
- 24) brak możliwości rozliczania działań użytkowników – brak kontroli nad dostępem do przetwarzanych dokumentów,
- 25) dostęp do informacji przez osoby nieuprawnione podczas ponownego wykorzystania używanych nośników danych,
- 26) podgląd przez nieuprawnionych użytkowników dokumentów zapisanych na dysku twardym,
- 27) przeglądania zawartości dokumentów przez osoby nieuprawnione w czasie przetwarzania informacji podczas grupowego dostępu.

### 3. Aplikacje

- 1) obserwacja bezpośrednia (filmowanie, fotografowanie, nagrywanie, użycie czytników laserowych lub na podczerwień etc.),
- 2) nieuprawniona próba modyfikacji dziennika zdarzeń,
- 3) nieuprawnione instalowanie urządzeń służących do naruszenia poufności przetwarzanych informacji,
- 4) nieuprawniona, świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
- 5) korzystanie z nielicencjonowanego oprogramowania,
- 6) przypadkowa zmiana ustawień konfiguracyjnych,
- 7) stosowanie niewłaściwego systemu plików,
- 8) wykorzystanie przechowywanych dokumentów na dysku twardym,

- 9) wykorzystanie pozostawionych na dysku twardym komputera plików roboczych wytworzonych przez oprogramowanie.

#### 4. Pomieszczenia

- 1) katastrofy budowlane,
- 2) ekstremalne czynniki środowiskowe (temperatura, wilgotność, zapylenie),
- 3) awaria klimatyzacji,
- 4) pożar w strefie administracyjnej,
- 5) zalanie pomieszczeń w strefie bezpieczeństwa,
- 6) zamach terrorystyczny (eksplozja ładunków wybuchowych, użycie broni),
- 7) nieuprawniony dostęp do określonych pomieszczeń (np. narad.).

### **Reakcja na ryzyko i działania zaradcze**

#### **§ 9.**

1. Dla każdego zidentyfikowanego i poddanego analizie ryzyka, jego właściciel wskazuje jedną z poniższych reakcji:
  - 1) ograniczanie - podjęcie działań zaradczych, które doprowadzić mają do likwidacji lub ograniczenia ryzyka do akceptowalnego poziomu.
  - 2) dzielenie się - częściowe lub całkowite przeniesienie ryzyka na inny podmiot,
  - 3) akceptacja (tolerowanie) - oznacza, że nie podejmuje się żadnych działań zaradczych, ale rozumie ewentualne skutki zdarzenia i świadomie godzi się na nie (np.: możliwość przeciwdziałania jest ograniczona lub koszt przeciwdziałania przewyższa potencjalne korzyści),
  - 4) unikanie (likwidacja ryzyka) - niepodejmowanie lub zaprzestanie działania narażającego na ryzyko,
2. Decyzja odnośnie reakcji na ryzyko powinna być podejmowana z uwzględnieniem, z jednej strony potencjalnych kosztów, które wiążą się z jego ograniczaniem, z drugiej zaś potencjalnych korzyści, które wynikają z podjęcia ryzyka.
3. Przy wskazaniu reakcji na ryzyko należy uwzględnić określony w niniejszym dokumencie akceptowany poziom ryzyka. W tym celu należy wykorzystać mapę ryzyka. Mapa ryzyka jest graficzną prezentacją wyników oceny ryzyka. Dla każdego z poziomów ryzyka przypisano odpowiednią kolorystykę:
  - 1) poziom niski - kolor zielony - akceptowalny poziom ryzyka, zaplanowanie i wdrożenie działań zaradczych zależy od decyzji właściciela ryzyka,
  - 2) poziom średni - kolor żółty - akceptowalny poziom ryzyka, konieczność stałego monitorowania poziomu ryzyka,
  - 3) poziom wysoki - kolor pomarańczowy - akceptowalny poziom ryzyka, wymóg stałego monitorowania poziomu ryzyka oraz konieczność zaplanowania działań zaradczych do ewentualnego wdrożenia,
  - 4) poziom bardzo wysoki - kolor czerwony - nieakceptowalny poziom ryzyka, konieczność wycofania się lub opracowania i wdrożenia Planu działań sprowadzających ryzyko do akceptowanego poziomu w terminie uzgodnionym z Administratorem danych. Właściciel ryzyka zobowiązany jest do monitorowania poziomu ryzyka i skuteczności przyjętych działań. Realizacja celów/procesów obciążonych ryzykiem bardzo wysokim wymaga akceptacji Administratora danych oraz przeprowadzeniem oceny skutków dla ochrony danych.

4. Zastosowane techniczne i organizacyjne środki bezpieczeństwa, mechanizmy kontrolne to działania zaradcze, które mają na celu ograniczenie ryzyka do akceptowanego dla organizacji poziomu - zarówno prawdopodobieństwa, jak i następstw jego wystąpienia.
5. Mechanizmy kontrolne powinny prowadzić do zmniejszenia niepewności wyników poprzez wykrycie i skorygowanie niepożądanych rezultatów, unikanie niepożądanych efektów lub ograniczenie ich występowania, a także osiągnięcie spodziewanych rezultatów.
6. Zastosowane techniczne i organizacyjne środki bezpieczeństwa, mechanizmy kontrolne obejmują przyjęte w organizacji procedury, instrukcje, jak i faktycznie realizowane działania.
7. W razie potrzeby wskazuje się planowane w organizacji działania, mające na celu modyfikację istniejących lub wdrożenie nowych techniczne i organizacyjne środków bezpieczeństwa czy mechanizmów kontrolnych koniecznych dla ograniczenia ryzyka.
8. W odniesieniu do każdego rodzaju ryzyka ustalana jest osoba odpowiedzialna za zarządzanie danym ryzykiem - właściciel ryzyka.

Do zadań właścicieli ryzyka należy, w szczególności:

- 1) identyfikacja i ocena ryzyk związanych z realizacją przypisanych procesów,
- 2) określenie istniejących zabezpieczeń, zastosowanych środków technicznych i organizacyjnych,
- 3) określenie następstw naruszeń praw lub wolności dla osób fizycznych,
- 4) określenie prawdopodobieństwa, następstw wystąpienia i istotności ryzyka w kontekście następstw dla osób fizycznych,
- 5) określenie reakcji w odniesieniu do poszczególnych ryzyk,
- 6) określenie następstw dla organizacji,
- 7) realizacja organizacyjnych i technicznych środków bezpieczeństwa w stosunku do zidentyfikowanych ryzyk.

### Rejestry ryzyk

#### § 10.

1. Przynajmniej raz na sześć miesięcy dokonuje się w organizacji przeglądu rejestru ryzyk związanych z obszarem ochrony danych. Jest to monitoring ryzyka.
2. Monitoring ryzyka obejmuje:
  - 1) awykonanie przeglądu, w celu określenia, czy ryzyko uległo zmianie,
  - 2) sprawdzenie, czy punktowa ocena ryzyka jest wciąż odpowiednia,
  - 3) zapewnienie skuteczności dotychczasowych zastosowanych mechanizmów kontrolnych, technicznych i organizacyjnych środków bezpieczeństwa,
  - 4) monitorowanie uzgodnionych działań w zakresie zarządzania ryzykiem.
3. Wzór rejestru ryzyka stanowi załącznik nr 1 do niniejszej procedury.

**PROREKTOR**  
*Z. KP*  
dr inż. Grzegorz Koc

**Załącznik nr 1 do Polityki Zarządzania Ryzykiem - szacowanie ryzyka**

| Lp. | Opis ryzyka/<br>zagrożenia                                                                   | Istniejące<br>zabezpieczenia /<br>Zastosowane<br>techniczne środki<br>bezpieczeństwa /<br>mechanizmy<br>kontrolne | Następstwa/skutki<br>naruszenia praw lub<br>wolności dla osób<br>fizycznych | Prawdopodo<br>bieństwo<br>wystąpienia<br>w skali<br>od 1 do 5 | Następstwa<br>(wpływ)<br>w skali<br>od 1 do 5 | Istotność<br>(5 x 6) | Reakcja na ryzyko<br>O - ograniczenie<br>D - dzielenie się<br>A - akceptacja<br>U - unikanie | Następstwa/ skutki dla<br>organizacji                               | Organizacyjne i<br>techniczne środki<br>bezpieczeństwa do<br>zastosowania                                  | Właściciel ryzyka -<br>osoba / dział / komórka<br>odpowiedzialna<br>za minimalizację ryzyka |
|-----|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------|----------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1   | 2                                                                                            | 3                                                                                                                 | 4                                                                           | 5                                                             | 6                                             | 7                    | 8                                                                                            | 9                                                                   | 10                                                                                                         | 11                                                                                          |
| 1   | Nieuprawnione<br>kopiowanie danych z<br>dysku lub innych<br>nośników informacji              | Proces<br>uwierzytelniania<br>Kopie<br>bezpieczeństwa.<br>Szkolenie, polityki<br>bezpieczeństwa<br>informacji,    | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 1                                                             | 4                                             | 4                    | O - ograniczenie                                                                             | Skutki prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa | Audyt bezpieczeństwa<br>informatycznego.<br>Bezpieczna<br>eksploatacja.                                    | Kierownicy działów                                                                          |
| 2   | Kradzież lub utrata<br>dokumentów<br>papierowych lub<br>elektronicznych,<br>nośników danych, | Gospodarka<br>kluczami. Fizyczne<br>zabezpieczenie<br>pomieszczeń                                                 | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 1                                                             | 4                                             | 4                    | U - unikanie                                                                                 | Utrata reputacji,<br>odpowiedzialność<br>prawna, finansowa          | Bezpieczeństwo<br>fizyczne - zamykanie na<br>klucz szafy, drzwi.<br>Ochrona budynku                        | Administrator danych<br>osobowych                                                           |
| 3   | Korzystanie z<br>nielicencjonowanego<br>oprogramowania                                       | Zabezpieczenie<br>przed możliwością<br>zainstalowania<br>oprogramowania.                                          | Szkody społeczne                                                            | 1                                                             | 2                                             | 2                    | U - unikanie                                                                                 | Odpowiedzialność<br>administracyjna i<br>finansowa                  | Zakaz i<br>uniemożliwienie<br>instalowania (firewall).<br>Zabezpieczenie systemu<br>(system antywirusowe). | Kierownicy działów                                                                          |
| 4   | Uszkodzenie sprzętu<br>komputerowego,<br>uszkodzenie fizyczne<br>nośników danych,            | Kopie<br>bezpieczeństwa.<br>Szkolenie, polityki<br>bezpieczeństwa<br>informacji,                                  | Utrata danych<br>osobowych                                                  | 2                                                             | 2                                             | 4                    | U - unikanie                                                                                 | Skutki prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa | Tworzenie okresowo<br>kopii danych w<br>systemie, bieżąca<br>konservacja,<br>Bezpieczna<br>eksploatacja.   | Kierownicy działów                                                                          |
| 5   | Użycie<br>oprogramowania w<br>nieuprawniony<br>sposób,                                       | Proces<br>uwierzytelniania<br>Szkolenie, polityki<br>bezpieczeństwa<br>informacji,                                | Utrata danych<br>osobowych                                                  | 1                                                             | 2                                             | 2                    | O - ograniczenie                                                                             | Skutki prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,<br>blokowanie<br>oprogramowania<br>(firewall).        | Kierownicy działów                                                                          |
| 6   | Drukowanie danych<br>osobowych na jednej,<br>ogólnie dostępnej<br>drukarkę,                  | Uwierzytelnianie,<br>Ograniczenia<br>dostępu.<br>Szkolenie, polityki<br>bezpieczeństwa<br>informacji,             | Naruszenie<br>prywatności<br>Nadużycia finansowe                            | 2                                                             | 3                                             | 6                    | U - unikanie                                                                                 | Skutki prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa | Uwierzytelniony /<br>ograniczony dostęp do<br>drukarki. Bezpieczna<br>eksploatacja.                        | Kierownicy działów                                                                          |

| Lp. | Opis ryzyka/<br>zagrożenia                                                                                  | Istniejące<br>zabezpieczenia /<br>Zastosowane<br>organizacyjne i<br>techniczne środki<br>bezpieczestwa /<br>mechanizmy<br>kontrolne | Następstwa/skutki<br>naruszenia praw lub<br>wolności dla osób<br>fizycznych | Prawdopodo<br>bieństwo<br>wystąpienia<br>w skali<br>od 1 do 5 | Następstwa<br>(wpływ)<br>w skali<br>od 1 do 5 | Istotność<br>(5 x 6) | Reakcja na ryzyko<br>O - ograniczanie<br>D - dzielenie się<br>A - akceptacja<br>U - unikanie | Następstwa/ skutki dla<br>organizacji                         | Organizacyjne i<br>techniczne środki<br>bezpieczestwa do<br>zastosowania                                            | Właściciel ryzyka -<br>osoba / dział / komórka<br>odpowiedzialna<br>za minimalizację ryzyka |
|-----|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------|----------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1   | 2                                                                                                           | 3                                                                                                                                   | 4                                                                           | 5                                                             | 6                                             | 7                    | 8                                                                                            | 9                                                             | 10                                                                                                                  | 11                                                                                          |
| 7   | Wejście do systemu operacyjnego z wykorzystaniem obcego identyfikatora,                                     | Uwierzytelnianie, Szkolenie, polityki bezpieczestwa informacji, Ograniczenia dostępu.                                               | Naruszenie prywatności<br>Nadużycia finansowe                               | 1                                                             | 4                                             | 4                    | U - unikanie                                                                                 | Skutki prawne<br>Odpowiedzialność administracyjna i finansowa | Szkolenie, nieprzekazywanie identyfikatorów i hasel.<br>Bezpieczestwo komunikacji.                                  | Kierownicy działów                                                                          |
| 8   | Nieuprawniony dostęp do procesu przetwarzania danych: włamanie po godzinach pracy                           | Uwierzytelnianie, Ograniczenia dostępu.<br>Szkolenie, polityki bezpieczestwa informacji,                                            | Naruszenie prywatności<br>Kradzież tożsamości                               | 1                                                             | 4                                             | 4                    | A - akceptacja                                                                               | Skutki prawne<br>Odpowiedzialność administracyjna i finansowa | Zamykanie szaf z danymi osobowymi, drzwi do pomieszczeń.<br>Ochrona budynku, system alarmowy.                       | Administrator danych osobowych.                                                             |
| 9   | Wyludzenie, fałszowanie dokumentów, hasel dostępu itp                                                       | Szkolenie, polityki bezpieczestwa informacji, blokowanie oprogramowania (firewall).<br>Uwierzytelnianie,                            | Naruszenie prywatności<br>Nadużycia finansowe                               | 2                                                             | 3                                             | 6                    | U - unikanie                                                                                 | Skutki prawne<br>Odpowiedzialność administracyjna i finansowa | Szkolenie, polityki bezpieczestwa informacji, blokowanie oprogramowania (firewall).                                 | Kierownicy działów                                                                          |
| 10  | Nieuprawniona, świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników. | Szkolenie, polityki bezpieczestwa informacji, blokowanie oprogramowania (firewall).                                                 | Szkody społeczne.<br>Naruszenie prywatności.                                | 1                                                             | 3                                             | 3                    | O - ograniczenie                                                                             | Utrata reputacji,                                             | Szkolenie, polityki bezpieczestwa informacji, blokowanie oprogramowania (firewall).                                 | Administrator danych osobowych.                                                             |
| 11  | Podglądanie zawartości ekranu monitora przez użytkowników z innych komputerów                               | Szkolenie, polityki bezpieczestwa informacji,                                                                                       | Szkody społeczne.<br>Nadużycia finansowe                                    | 2                                                             | 3                                             | 6                    | O - ograniczenie                                                                             | Skutki prawne<br>Odpowiedzialność administracyjna i finansowa | Szkolenie, polityki bezpieczestwa informacji, zabezpieczenia fizyczne stanowiska pracy<br>Bezpieczestwo komunikacji | Kierownicy działów                                                                          |
| 12  | Błędy popełniane przez użytkowników                                                                         | Szkolenie, polityki bezpieczestwa informacji,                                                                                       | Szkody społeczne.<br>Nadużycia finansowe                                    | 2                                                             | 3                                             | 6                    | O - ograniczenie                                                                             | Skutki prawne<br>Odpowiedzialność administracyjna i finansowa | Audyt bezpieczestwa informatycznego<br>Szkolenie, Bezpieczestwo komunikacji                                         | Kierownicy działów                                                                          |

| Lp. | Opis ryzyka/<br>zagrożenia                                                                                                                                               | Istniejące<br>zabezpieczenia /<br>Zastosowane<br>organizacyjne i<br>techniczne środki<br>bezpieczeństwa /<br>mechanizmy<br>kontrolne             | Następstwa/skutki<br>naruszenia praw lub<br>wolności dla osób<br>fizycznych | Prawdopodobieństwo<br>wystąpienia<br>w skali<br>od 1 do 5 | Następstwa<br>(wpływ)<br>w skali<br>od 1 do 5 | Istotność<br>(5 x 6) | Reakcja na ryzyko<br>O - ograniczanie<br>D - dzielenie się<br>A - akceptacja<br>U - unikanie | Następstwa/ skutki dla<br>organizacji                                                           | Organizacyjne i<br>techniczne środki<br>bezpieczeństwa do<br>zastosowania                                                                                                                | Właściciel ryzyka -<br>osoba / dział / komórka<br>odpowiedzialna<br>za minimalizację ryzyka |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------|-----------------------------------------------|----------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1   | 2                                                                                                                                                                        | 3                                                                                                                                                | 4                                                                           | 5                                                         | 6                                             | 7                    | 8                                                                                            | 9                                                                                               | 10                                                                                                                                                                                       | 11                                                                                          |
| 13  | Wejście osoby<br>nieupoważnionej do<br>strefy<br>administracyjnej                                                                                                        | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,                                                                                             | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 2                                                         | 3                                             | 6                    | U - unikania                                                                                 | Utrata reputacji, Skutki<br>prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa prawne | Szkolenie, polityki<br>bezpieczeństwa<br>informacji, Zamykanie<br>szaf z danymi<br>osobowymi,<br>zabezpieczenia fizyczne                                                                 | Kierownicy działów                                                                          |
| 14  | Zaniedbania ze strony<br>personelu<br>obsługującego proces<br>przetwarzania<br>danych,                                                                                   | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,                                                                                             | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 2                                                         | 3                                             | 6                    | O - ograniczenie                                                                             | Utrata reputacji, Skutki<br>prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa prawne | Audyt bezpieczeństwa<br>informatycznego<br>Szkolenie.<br>Bezpieczeństwo<br>komunikacji                                                                                                   | Kierownicy działów                                                                          |
| 15  | Utrata lub odczytanie<br>informacji przez<br>osoby nieuprawnione<br>podezas napraw<br>gwarancyjnych i<br>pogwarancyjnych<br>sprzętu oraz<br>czynności<br>konserwacyjnych | Powierzenie<br>przetwarzania<br>danych osobowych.<br>Uwierzytelnianie.<br>Ograniczony<br>dostęp do sprzętu i<br>systemu. Relacje z<br>dostawcami | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 2                                                         | 3                                             | 6                    | U - unikania                                                                                 | Utrata reputacji, Skutki<br>prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa prawne | Szkolenie, polityki<br>bezpieczeństwa<br>informacji, bezpieczna<br>eksploatacja. Relacje z<br>dostawcami.<br>Zarządzanie<br>incydentami<br>związanymi z<br>bezpieczeństwem<br>informacji | Kierownicy działów                                                                          |
| 16  | Odczytanie<br>informacji z<br>nośników<br>przewidywanych do<br>naprawy,                                                                                                  | Powierzenie<br>przetwarzania<br>danych osobowych.<br>Uwierzytelnianie.<br>Kontrola dostępu                                                       | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 2                                                         | 3                                             | 6                    | U - unikania                                                                                 | Utrata reputacji, Skutki<br>prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa prawne | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,                                                                                                                                     | Kierownicy działów                                                                          |
| 17  | Zapisywanie<br>informacji<br>niejawnych na<br>prywatne nośniki<br>informacji<br>użytkownika                                                                              | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,<br>kontrola dostępu                                                                         | Naruszenie dobrego<br>imienia<br>Nadużycia finansowe                        | 2                                                         | 3                                             | 6                    | O - ograniczenie                                                                             | Utrata reputacji, Skutki<br>prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa prawne | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,<br>Zabezpieczenie danych<br>przez możliwość<br>kopiowania.                                                                          | Kierownicy działów                                                                          |
| 18  | Nieuprawnione<br>kopiowanie danych z<br>dysku twardego                                                                                                                   | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,<br>kontrola dostępu                                                                         | Szkody społeczne.<br>Naruszenie dobrego<br>imienia<br>Nadużycia finansowe   | 1                                                         | 3                                             | 3                    | U - unikania                                                                                 | Utrata reputacji, Skutki<br>prawne<br>Odpowiedzialność<br>administracyjna i<br>finansowa prawne | Szkolenie, polityki<br>bezpieczeństwa<br>informacji,<br>Zabezpieczenie danych<br>przez możliwość<br>kopiowania.                                                                          | Kierownicy działów                                                                          |

| Lp. | Opis ryzyka/<br>zagrożenia                                                                                                   | Istniejące<br>zabezpieczenia /<br>Zastosowane<br>organizacyjne i<br>techniczne środki<br>bezpieczeństwa /<br>mechanizmy<br>kontrolne | Następstwa/skutki<br>naruszenia praw lub<br>wolności dla osób<br>fizycznych | Prawdopodo<br>bieństwo<br>wystąpienia<br>w skali<br>od 1 do 5 | Następstwa<br>(wpływ)<br>w skali<br>od 1 do 5 | Istotność<br>(5 x 6) | Reakcja na ryzyko<br>O - ograniczanie<br>D - dzielenie się<br>A - akceptacja<br>U - unikanie | Następstwa/ skutki dla<br>organizacji               | Organizacyjne i<br>techniczne środki<br>bezpieczeństwa do<br>zastosowania                                                         | Właściciel ryzyka -<br>osoba / dział / komórka<br>odpowiedzialna<br>za minimalizację ryzyka |
|-----|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------|----------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1   | 2                                                                                                                            | 3                                                                                                                                    | 4                                                                           | 5                                                             | 6                                             | 7                    | 8                                                                                            | 9                                                   | 10                                                                                                                                | 11                                                                                          |
| 19  | Brak możliwości<br>rozliczania działań<br>użytkowników – brak<br>kontroli nad<br>dostępem do<br>przetwarzanych<br>dokumentów | Szkolenie. Polityki<br>bezpieczeństwa<br>informacji,<br>kontrola dostępu                                                             | Szkody społeczne.<br>Naruszenie dobrego<br>imienia.                         | 1                                                             | 4                                             | 4                    | A - akceptacja                                                                               | Organizacja<br>bezpieczeństwa<br>informacji         | Organizacja<br>bezpieczeństwa<br>informacji. Szkolenie.<br>Polityki bezpieczeństwa<br>informacji, kontrola<br>dostępu.            | Administrator systemów<br>informatycznych                                                   |
| 20  | Przypadkowa zmiana<br>ustawień<br>konfiguracyjnych                                                                           | Kopie systemu,<br>kontrola dostępu.<br>Aspekty<br>bezpieczeństwa<br>informacji w<br>zarządzaniu<br>ciągłością działania              | Szkody społeczne.<br>Naruszenie dobrego<br>imienia.                         | 1                                                             | 3                                             | 3                    | U - unikanie                                                                                 | Szkody społeczne.<br>Naruszenie dobrego<br>imienia. | Kopie systemu,<br>kontrola dostępu.<br>Aspekty<br>bezpieczeństwa<br>informacji w<br>zarządzaniu ciągłością<br>działania           | Administrator systemów<br>informatycznych                                                   |
| 21  | Katastrofy budowlane                                                                                                         | Bezpieczna<br>eksploatacja.<br>Bezpieczeństwo<br>fizyczne i<br>środowiskowe                                                          | Naruszenie dobrego<br>imienia. Utrata<br>danych.                            | 1                                                             | 4                                             | 4                    | A - akceptacja                                                                               | Naruszenie dobrego<br>imienia. Utrata danych.       | Bezpieczeństwo<br>fizyczne i<br>środowiskowe.<br>Bezpieczna<br>eksploatacja.<br>Reagowanie na wpływ<br>czynników<br>zewnętrznych. | Administrator danych<br>osobowych                                                           |
| 22  | Pożar w strefie<br>administracyjnej                                                                                          | Bezpieczna<br>eksploatacja.<br>Przestrzeganie<br>zasad ochrony<br>ppoż.                                                              | Naruszenie dobrego<br>imienia. Utrata<br>danych.                            | 1                                                             | 4                                             | 4                    | A - akceptacja                                                                               | Naruszenie dobrego<br>imienia. Utrata danych.       | Bezpieczeństwo<br>fizyczne i<br>środowiskowe.<br>Bezpieczna<br>eksploatacja.<br>Reagowanie na wpływ<br>czynników<br>zewnętrznych. | Administrator danych<br>osobowych                                                           |

## Załącznik nr 2 do Polityki Zarządzania ryzykiem "Mapa ryzyka"

| NASTĘPSTWA "y" (wpływ)        |  | PRAWDOPODOBIEŃSTWO WYSTĄPIENIA "X" |             |              |              |                     |
|-------------------------------|--|------------------------------------|-------------|--------------|--------------|---------------------|
|                               |  | 1<br>znikome                       | 2<br>niskie | 3<br>średnie | 4<br>wysokie | 5<br>bardzo wysokie |
| 5<br>katastrofalne<br>81-100% |  |                                    |             |              |              |                     |
| 4<br>poważne<br>61-80%        |  |                                    |             |              |              |                     |
| 3<br>średnie<br>41-60%        |  |                                    |             |              |              |                     |
| 2<br>małe<br>21-40%           |  |                                    |             |              |              |                     |
| 1<br>nieznaczne<br>0-20%      |  |                                    |             |              |              |                     |