Załącznik Nr 2

do Procedury zarządzania ryzykiem w Starostwie Żyrardowskim

Kategorie ryzyka wraz z przykładami dotyczącymi jego możliwych źródeł (przyczyn) oraz skutków

Tabela nie określa zamkniętego katalogu ryzyka.

Ryzyko finansowe	
Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów
Oszustwa i kradzieży	Związane ze stratą środków rzeczowych i finansowych będącą wynikiem przestępstwa lub wykroczenia, np. kradzież mienia przez interesantów lub pracowników.
Podlegające ubezpieczeniu	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia np. ryzyko pożaru, zalania, wypadku
Zamówień publicznych i zlecania zadań publicznych	Związane z podejmowaniem decyzji oraz udzielaniem zamówień publicznych lub zlecaniem zadań publicznych innym podmiotom, np. ryzyko naruszenia zasad, form lub trybu ustawy o zamówieniach publicznych.
Odpowiedzialności	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek karnych, kosztów procesowych
Realizacji programów współfinansowanych z różnych źródeł	Związane z wystąpieniem nieprawidłowości przy realizacji projektu i jego rozliczeniu, mogących skutkować zwrotem środków.
Ryzyko dot. zasobów ludzkich	
Pracowników	Związane z liczebnością i kompetencjami pracowników, np. wprowadzanie nowych zadań bez zabezpieczenia etatowego, absencja chorobowa pracowników.
Bhp	Związane z bezpieczeństwem warunków pracy i wypadkami przy pracy, np. śliska podłoga, wypadek komunikacyjny.
Ryzyko działalności	
Regulacji wewnętrznych	Związane z istnieniem i aktualnością regulacji wewnętrznych, np. brak aktualnych procedur, brak aktualnych aktów prawnych.
Organizacji i podejmowania decyzji	Związane ze strukturą organizacyjną, organizacją pracy oraz przekazywaniem obowiązków i uprawnień np. ryzyko nieprecyzyjnie określonych obowiązków, ryzyko braku formalnie powierzonych obowiązków, ryzyko nieodpowiedniej struktury organizacyjnej.
Kontroli zarządczej	Związane z funkcjonowaniem systemu kontroli wewnętrznej, np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontrolnych, ryzyko nieprawidłowo wydanej decyzji.
Informacji	Związane, z jakością informacji na podstawie, których podejmowane są decyzje, np. ryzyko braku komunikacji w pionie i poziomie struktury organizacyjnej.
Wizerunku	Związane z wizerunkiem Gminy oraz jednostki organizacyjnej, np. ryzyko negatywnych opinii i artykułów w prasie.

Systemów informatycznych	Związane z używanymi w Urzędzie i Jednostkach Organizacyjnych systemami i programami informatycznymi oraz ochroną zawartych w nich danych np. ryzyko awarii systemu, ryzyko dostępu do danych w systemach przez nieuprawnione osoby, ryzyko niekontrolowanej modyfikacji danych.
Ochrony zasobów	Ryzyko nieuprawnionego dostępu do pomieszczeń Urzędu, do danych osobowych przetwarzanych przez pracowników, ryzyko nieznajomości procedur opracowanych na wypadek wystąpienia sytuacji nadzwyczajnej, np. pożaru, powodzi, poważnej awarii lub nieumiejętnego ich stosowania itp.

Zasady oceny stopnia prawdopodobieństwa ziszczenia się ryzyka

Prawdopodobieństwo	Opis szczegółowy
Bardzo wysokie 4	Zdarzenie wystąpi w najbliższym terminie – lub co najmniej raz w tygodniu
Wysokie 3	Zdarzenie występuje wielokrotnie w ciągu roku -co najmniej raz w miesiącu
Średnie 2	Zdarzenie występuje więcej niż raz w roku -co najmniej raz na kwartał
Niskie 1	Do tej pory takie zdarzenie nie wystąpiło w Urzędzie lub w Jednostkach Organizacyjnych lub może zaistnieć jedynie w wyjątkowych okolicznościach raz w roku

1. W oparciu o dokonaną ocenę wpływu i prawdopodobieństwa ziszczenia się ryzyka ustalany jest poziom istotności ryzyka:
2. Określenie prawdopodobieństwa (P) i wpływu ryzyka (W) w czterostopniowej skali, umożliwia ustalenie współczynnika istotności ryzyka (IR), – jako iloczynu (wyrażonych punktowo) prawdopodobieństwa wystąpienia ryzyka (P) oraz potencjalnego wpływu jego wystąpienia (W):

IR = P x W
gdzie:
IR – współczynnik istotności ryzyka
P – prawdopodobieństwo wystąpienia ryzyka
W – potencjalny wpływ ryzyka

3. Po przeprowadzonej analizie, wartości przyporządkowane, zarówno wpływów i jak i prawdopodobieństwu ryzyka, należy przenieść na mapę ryzyka. Mapę punktowej oceny istotności ryzyka „4 x4", przedstawiono poniżej:

Mapa ryzyka 4x4

Oddziaływanie					
Bardzo wysokie	4 niskie	8 średnie	12 wysokie	16 bardzo wysokie	
Wysokie	3 niskie	6 średnie	9 wysokie	12 wysokie	
Średnie	2 niskie	4 niskie	6 średnie	8 średnie	
Niskie	1 niskie	2 niskie	3 niskie	4 niskie	
	Niskie	**Średnie**	**Wysokie**	**Bardzo wysokie**	**Prawdopodobieństwo**

4. **Istotność ryzyka** obliczona według wzoru umożliwia dokonanie oceny i hierarchizacji ryzyka.
5. Dla oceny istotności ryzyka stosuje się trzystopniową skalę obejmującą następujące poziomy:

– **WYSOKI** – jest to ryzyko o wartości 9-16, które istotnie wpływa na kluczową działalność jednostki, uniemożliwia realizację jej zadań i celów, rodzi straty finansowe,

- **ŚREDNI** – jest to ryzyko o wartości 6-8, które potencjalnie wpływa na kluczową działalność jednostki, jest zagrożeniem dla realizacji zadań i celów, zagraża powstaniem strat finansowych,
- **NISKI** – jest to ryzyko o wartości 1–4, które nie ma wpływu na kluczową działalność jednostki, nie uniemożliwia realizacji zadań i osiągania celów.

Poziomy istotności	Wartość punktowa	Przesłanki
Niski	1-4	**Ryzyko akceptowalne** Akceptacja - ryzyko podlega minimalnemu monitorowaniu. Wartość ryzyka powinna zostać zweryfikowana dopiero przy następnej analizie lub gdy zmienią się warunki mające wpływ na podniesienie wartość ryzyka.
Średni	6-8	**Ryzyko możliwe do zaakceptowania** Działanie ograniczające ryzyko do poziomu akceptowalnego. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot. Ryzyko wymaga monitorowania oraz zaplanowania i podjęcia działań prewencyjnych w określonym dłuższym okresie czasu (w zależności od możliwości np. w ciągu kwartału, półrocza czy roku), przy czym dopuszcza się akceptację ryzyka z tego przedziału, gdyby szacowane koszty niezbędnych działań przewyższały korzyści z ograniczenia ryzyka lub właściciel ryzyka podwyższył jego akceptowalny poziom. W sytuacji akceptacji takiego ryzyka właściciel ryzyka powinien monitorować ryzyko i okresowo rozważać potrzebę podjęcia działań ograniczających ryzyko.
Wysoki	9-16	**Ryzyko nieakceptowane** Działanie niezwłoczne – ryzyko wymaga niezwłocznego podjęcia działań ograniczających ryzyko. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot lub jeśli jest to możliwe wycofania się z realizacji zadania powodującego ryzyko.

6. Metodami przeciwdziałania ryzyku są;

1) **kontrolowanie ryzyka** - podejmowanie działań zaradczych pozwalających na ograniczenie ryzyka do akceptowanego poziomu m. in. poprzez wzmocnienie mechanizmów kontroli wewnętrznej, w tym zwłaszcza procedury, instrukcje, upoważnienia, podział obowiązków, nadzór, szkolenia;
2) **akceptacja** - zaniechanie podejmowania działań zaradczych z uwagi na brak możliwości wskazania takich działań, które byłyby skuteczne lub w przypadku, gdy koszt podjętych działań zaradczych jest wyższy niż koszt poniesienia ryzyka;
3) **przeniesienie ryzyka** - przekazanie ryzyka podmiotowi zewnętrznemu np. w drodze ubezpieczenia, zlecenie wykonania usługi;
4) **unikanie** – zaprzestanie/zawieszenie działań rodzących zbyt duże ryzyko.

Załącznik nr 3 do Instrukcji zarządzania ryzykiem

Przykładowy katalog zagrożeń

Obszar przetwarzania danych osobowych

1) niewłaściwie zaadresowana poczta elektroniczna;
2) ujawnienie poszczególnych odbiorców wiadomości e-mail;
3) utrata (kradzież, zagubienie) elektronicznych nośników danych (tablet, laptop, smartphone, pendrive, dysk twardy);

4) utrata (kradzież, zagubienie) dokumentów zawierających zasoby informacyjne prawnie chronione, w tym dane osobowe;
5) udostępnienie istotnych zasobów informacyjnych osobie nieuprawnionej;
6) przetwarzanie istotnych zasobów informacyjnych przez osobę nieupoważnioną;
7) brak skutecznego usunięcia danych osobowych z dysków komputerowych przed przekazaniem poza jednostkę;
8) pozostawienie wydruków zawierających dane osobowe lub istotne zasoby informacyjne na ogólnodostępnej drukarce;
9) ujawnienie haseł innym, nieupoważnionym osobom;
10) wykonanie kserokopii lub skanu dokumentów tożsamości;
11) pozyskiwanie nadmiarowych danych osobowych;
12) przetwarzanie danych osobowych bez podstawy prawnej;
13) pozostawienie niezablokowanego konta.

Bezpieczeństwo fizyczne i środowiskowe

1) pożar;
2) zalanie;
3) katastrofa budowlana;
4) kradzież jakiegokolwiek z aktywów informacyjnych (sprzętu, dokumentów itp.);
5) awaria zasilania urządzeń przetwarzających informacje (stacje robocze oraz systemy lub serwery);
6) nieuprawniony dostęp do strefy administracyjnej;
7) nieuprawniony dostęp do strefy bezpieczeństwa;
8) pozostawienie otwartych okien lub drzwi po zakończeniu pracy;
9) pozostawienie środków przetwarzania informacji bez nadzoru;
10) nieprzestrzeganie zasady czystego biurka oraz czystego ekranu;
11) nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych;
12) awaria innych systemów związanych z zabezpieczeniem fizycznym i środowiskowym;

Bezpieczeństwo osobowe

1) w wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień w systemach informacyjnych;
2) pracownik nie rozliczył się z powierzonych środków przetwarzania informacji;
3) pracownik nie przekazał wszelkich prowadzonych spraw, postępowań, informacji oraz danych, które prowadził lub wytworzył w trakcie wykonywania swoich obowiązków;
4) publikowanie obraźliwych treści np. na temat pracowników;
5) pomawianie (zniesławianie).

Bezpieczeństwo teleinformatyczne

1) złośliwe oprogramowanie, np. wirus, spyware (stacje robocze oraz systemy lub serwery), które nie zostało automatycznie usunięte przez oprogramowanie antywirusowe;
2) niestabilna praca systemów zaklasyfikowanych, jako ważne i krytyczne oraz stacji roboczych;
3) awaria kluczowego systemu informatycznego;
4) niedostępność kluczowego systemu informatycznego;
5) brak dostępności do sieci Internet;
6) utrudniona praca w systemie np. zbyt duże obciążenie procesora, przekroczenie dostępnych zasobów systemowych;

7) nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy;
8) nieuprawniona zmiana danych lub ich uszkodzenie;
9) utrata danych;
10) próby omijania lub łamania zdefiniowanych zabezpieczeń;
11) fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzającego informacje (celowe działania);
12) błędy w obsłudze i konserwacji sprzętu komputerowego służącego do przetwarzania informacji;
13) błędy w przechowywaniu, eksploatacji oraz konserwacji oprogramowania;
14) włamanie do sieci i systemów teleinformatycznych (np. atak hackera);
15) niewykonanie kopii bezpieczeństwa;
16) niezweryfikowanie możliwości odtworzenia danych z kopii zapasowych;
17) wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych;
18) próba instalacji niezatwierdzonego oprogramowania;
19) wykorzystano niezinwentaryzowany środek przetwarzania informacji (nienależący do organizacji);
20) zidentyfikowano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośnik);
21) wykorzystanie ogólnodostępnych serwisów pocztowych (np. gmail.com) w celach służbowych;
22) wykorzystanie służbowej poczty elektronicznej do celów prywatnych;
23) przesyłanie przy użyciu służbowej poczty elektronicznej informacji niezwiązanych z wykonywaną pracą;
24) zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby;
25) podjęcie pracy w stanie zagrożenia bezpieczeństwa informacji;
26) niestosowanie się do wymagań dotyczących złożoności haseł;
27) niezablokowana stacja robocza;
28) wykorzystanie służbowych środków przetwarzania informacji do celów prywatnych;
29) brak zabezpieczeń przenośnego sprzętu komputerowego (szyfrowanie dysku);
30) łączenie się z niezabezpieczoną siecią Wi-Fi;
31) brak zabezpieczeń w postaci uniemożliwienia zapisu na przenośne nośniki informacji;
32) korzystanie z prywatnego sprzętu komputerowego do celów służbowych;
33) używanie do połączeń nieszyfrowanych kanałów;
34) atak hackerski na stronę internetową.

Bezpieczeństwo w umowach zawartych z podmiotami zewnętrznymi

1) niewywiązywanie się z zapisów umowy;
2) brak możliwości świadczenia usługi z powodu wystąpienia incydentu po stronie wykonawcy;
3) celowe działanie na szkodę Zamawiającego;
4) podsłuch;
5) kradzież danych;
6) naruszenie obowiązujących przepisów prawa;
7) naruszenie obowiązujących regulacji wewnętrznych w zakresie bezpieczeństwa;
8) naruszenie praw autorskich: