załącznik nr 9 do zarządzenia nr 108/2021

Lista przykładowych czynników ryzyka

Czynniki ryzyka finansowego	
1.	Zbyt niski budżet w stosunku do potrzeb i realizowanych zadań
2.	Utrata lub odczuwalne ograniczenie istotnego źródła finansowania działalności
3.	Zwrot środków z tytułu nieprawidłowości w rozliczaniu wsparcia finansowego
4.	Utrata zdolności do terminowego regulowania zobowiązań przez Uczelnię (brak płynności)
5.	Obowiązek zapłaty kwot pieniężnych tytułem odszkodowań, kar finansowych, odsetek karnych, kosztów procesowych
6.	Naruszenie dyscypliny finansów publicznych
7.	Zaciąganie zobowiązań bez upoważnienia lub z przekroczeniem zakresu upoważnienia
8.	Utrata środków na realizację zadań i projektów
9.	Wzrost wydatków lub kosztów prowadzonej działalności
10.	Brak lub niewystarczające zabezpieczenie środków finansowych na realizację umowy
11.	Brak weryfikacji warunków finansowych w zawieranych umowach
12.	Brak lub nieskuteczna weryfikacja lub autoryzacja dokumentacji księgowej
13.	Błędy w rejestrowaniu transakcji w systemie finansowo-księgowym
14.	Błędy w opisie transakcji na dokumentach księgowych

Czynniki ryzyka organizacyjnego	
1.	Brak lub niejasno przypisana odpowiedzialność za realizację celów i zadań
2.	Brak lub nieadekwatne do rzeczywistości planowanie realizacji zadań
3.	Brak lub nieskuteczne zasady zarządzania ryzykiem operacyjnym

4.	Niejasno określone standardy pracy oraz realizowanych zadań
5.	Niejasne priorytety realizowanych zadań
6.	Nieefektywna organizacja realizacji zadań, w tym nierównomierne obciążenie pracowników zadaniami
7.	Brak lub nieefektywne monitorowanie realizacji zadań, w tym niezapewnienie niezależnego audytu lub kontroli
8.	Brak zastępowalności pracownika w czasie jego nieobecności
9.	Brak zasad i procedur zapewnienia ciągłości działania operacyjnego
10.	Brak lub niejasna misja i wizja, w tym niejasna komunikacja ogółowi pracowników
11.	Brak zasad zarządzania zmianami
12.	Brak lub nieadekwatne do rzeczywistości plany długoterminowe
13.	Brak lub nieskuteczne zasady zarządzania ryzykiem strategicznym
14.	Brak lub niewystarczający nadzór nad realizacją umowy

Czynniki ryzyka zasobów ludzkich	
1.	Nieobsadzone stanowiska pracy
2.	Trudności w pozyskaniu pracownika w procesie rekrutacji
3.	Odejście kluczowych pracowników/pracownika z pracy
4.	Brak zastępowalności na kluczowych stanowiskach
5.	Brak planów sukcesji na kluczowych stanowiskach pracy
6.	Niewystarczające umiejętności lub doświadczenie pracowników
7.	Niezadowolenie pracowników z warunków zatrudnienia
8.	Brak lub niewystarczająca liczba szkoleń pracowników
9.	Konflikty w relacjach między pracownikami lub między pracownikami a przełożonym
10.	Nierówne traktowanie pracownika w związku z wykonywanymi zadaniami niezależnie od powodu

11.	Zachęcanie do nierównego traktowania pracownika w związku z wykonywaniu zadaniami niezależnie od powodu
12.	Molestowanie pracownika w związku z wykonywanymi zadania, polegające na naruszeniu godności, poniżeniu lub upokorzeniu
13.	Molestowanie seksualne, polegające na nieakceptowanym przez pracownika zachowaniu o charakterze seksualnym, mający charakter fizyczny, werbalny lub poza werbalny
14.	Naruszenie zasad współżycia społecznego w miejscy pracy oraz w związku z wykonywaną pracą

Czynnika ryzyka infrastruktury i systemów informatycznych	
1.	Brak lub niewystarczające informacje na temat stanu technicznego obiektów infrastruktury lub mienia
2.	Brak lub niewystarczające informacje na temat ilości zasobów sieci i sprzętu teleinformatycznego
3.	Brak lub nieregularne przeglądy stanu technicznego obiektów lub mienia
4.	Brak lub nieregularne przeglądy stanu technicznego sieci i sprzętu teleinformatycznego
5.	Brak lub niewystarczające zabezpieczenie fizyczne obiektów lub mienia przed zdarzeniami losowymi lub awariami
6.	Brak lub niewystarczające zabezpieczenie fizyczne sieci i sprzętu teleinformatycznego przed zdarzeniami losowymi lub awariami
7.	Brak lub nieaktualna inwentaryzacja stanu i ilości obiektów infrastruktury lub mienia
8.	Brak lub nieaktualna inwentaryzacja stanu sieci i sprzętu teleinformatycznego
9..	Brak lub niewystarczające zabezpieczenie dostępu do obiektów lub mienia
10.	Brak przypisania jednoznacznej własności mienia powierzonego pracownikom do wykorzystania dla celów służbowych
11.	Brak określenia lub skutecznego nadzorowania zasad korzystania przez pracowników z aktywów i mienia organizacji
12.	Brak regularnych remontów lub konserwacji
13.	Brak zasad zwrotu i rozliczania mienia powierzonego pracownikom
14.	Brak lub niejasne zasady zapewnienia bezpieczeństwa pracownikom lub innym osobom, w związku z korzystaniem z aktywów i mienia organizacji
15.	Brak możliwości prowadzenia działalności w obecnej lokalizacji
16.	Brak planów ochrony krytycznej infrastruktury lub planów ciągłości działania
17.	Brak planów ciągłości działania lub odstąpienie od ich aktualizacji

Czynniki ryzyka bezpieczeństwa informacji	
1.	Brak lub niejasne zasady/polityki zarządzania bezpieczeństwem informacji
2.	Brak lub nieregularne przeglądy zasad/polityki zarządzania bezpieczeństwem informacji
3.	Brak lub niejasno przypisany zakres odpowiedzialności w zakresie bezpieczeństwa informacji
4.	Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników
5.	Brak lub niejasno określone zasady zachowania poufności przetwarzanych informacji przez podmioty zewnętrzne, np. w związku z realizowanymi umowami
6.	Brak lub niejasno określone zasady obiegu dokumentacji wewnątrz organizacji
7.	Brak lub niejasno określone zasady kontaktowania się pracowników z podmiotami zewnętrznymi, w tym korzystania przez pracowników z mediów społecznościowych w ramach realizowanych zadań
8.	Brak zabezpieczenia/inwentaryzacji miejsca przechowywania i nośników informacji
9.	Brak lub niejasne zasady udzielania informacji podmiotom zewnętrznym
10.	Brak lub nieregularne archiwizowanie informacji
11.	Brak lub niejasne zasady dostępu użytkowników do sieci teleinformatycznej, w tym rejestracji, udzielania przywilejów, zarządzania hasłami, oraz odbioru praw
12.	Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych
13.	Brak lub niewłaściwa ochrona przed nieuprawnionym dostępem do informacji w aplikacjach, w tym luki w systemach
14.	Brak lub niejasne, w tym nieaktualne zasady pracy przy przetwarzaniu mobilnym i na odległość
15.	Brak lub niewłaściwa ochrona przed dokonywaniem nieuprawnionych zmian informacji w systemach i/lub aplikacjach
16.	Brak lub niewłaściwa ochrona bezpieczeństwa plików systemowych, w tym kodów źródłowych
17.	Brak lub niejasne zasady zarządzania incydentami bezpieczeństwa
18.	Brak działania lub działanie z opóźnieniem w sytuacji wystąpienia incydentów bezpieczeństwa teleinformatycznego
19.	Brak lub niewystarczające zapewnienie wsparcia teleinformatycznego w zawieranych umowach serwisowych
20.	Brak zapewnienia ciągłości działania systemów teleinformatycznych
21.	Brak lub niewystarczające zabezpieczenie dostępu do sieci i sprzętu teleinformatycznego
22.	Brak lub nieskuteczna ochrona antywirusowa lub brak ochrony przed złośliwym oprogramowaniem

23.	Brak lub nieregularne tworzenie kopii zapasowych informacji przetwarzanych w systemach teleinformatycznych
24.	Brak lub niejasne zasady używania przez pracowników nośników informatycznych
25.	Brak lub niejasne zasady ochrony dokumentacji systemów teleinformatycznych

Czynniki ryzyka naruszenia danych osobowych	
1.	Brak lub nieaktualna polityka/procedury przetwarzania danych osobowych
2.	Niepełny zakres regulacji zabezpieczających przetwarzanie danych osobowych
3.	Brak lub nieaktualne procedury postępowania w sytuacji naruszenia ochrony danych osobowych
4.	Wadliwe powołanie inspektora ochrony danych osobowych
5.	Brak lub niewystarczające kompetencje inspektora ochrony danych osobowych
6.	Naruszenie niezależności inspektora ochrony danych osobowych
7.	Brak lub niewystarczające zasoby do realizacji zadań inspektora ochrony danych osobowych
8.	Przetwarzanie danych w sytuacji braku lub niejasno wyrażonej zgody na przetwarzanie danych osobowych
9.	Brak lub niewystarczający nadzór nad umowami przetwarzania danymi osobowymi
10.	Brak lub niewystarczająca uzasadniona podstawa przetwarzania danych osobowych
11.	Brak lub niejasne cele przetwarzania danych osobowych
12.	Brak lub niska jakość procesu oceny przetwarzania danych osobowych
13.	Brak lub niekompletne rejestrowanie czynności przetwarzania danych osobowych
14.	Brak lub niewystarczające i nieadekwatne zarządzanie ryzykiem przetwarzania danych osobowych
15.	Brak lub niewystarczająca i nieadekwatne zabezpieczenie danych osobowych chronionych domyślnie lub na etapie projektowania
16.	Brak, niepełna lub nierzetelna ocena zakresu i skutków przetwarzania danych osobowych
17.	Brak lub nierzetelne prowadzenie rejestru naruszeń ochrony danych osobowych
18.	Zaniechanie zawiadamiania o naruszeniu danych osobowych uprawnionych organów zewnętrznych

Czynniki ryzyka wizerunku	
1.	Brak lub niejasne zasad zarządzania wizerunkiem organizacji oraz kontaktowania się z mediami i opinią publiczną
2.	Brak lub nierzetelna weryfikacja zewnętrznych pomiotów współpracujących
3.	Wysoka wrażliwość polityczna prowadzonej działalności
4.	Skargi na pracowników od podmiotów zewnętrznych
5.	Podejmowanie w Uczelni działań nieakceptowanych społecznie lub prawnie
6.	Nieakceptowana społecznie lub prawnie działalność pracowników Uczelni

Czynniki ryzyka prawnego	
1.	Brak lub ograniczony dostęp do informacji o zmieniających się przepisach prawa
2.	Duża liczba niejasnych przepisów prawa, wymagających dodatkowej interpretacji
3.	Brak lub ograniczony dostęp do usług lub wsparcia prawniczego
4.	Brak lub niejasne regulacje wewnętrzne (wymagające dodatkowych interpretacji)
5.	Nadmierna liczba regulacji wewnętrznych powodująca nieefektywne działanie
6.	Rosnąca liczba naruszeń regulacji wewnętrznych
7.	Działanie bez lub z naruszeniem podstawy prawnej
8.	Rosnąca liczba naruszeń przepisów prawa
9.	Rosnąca liczba spraw lub pozwów sądowych
10.	Rosnąca liczba przegranych spraw sądowych
11.	Brak uzasadnienia zawarcia umowy z punktu widzenia realizacji celów i zadań
12.	Brak lub niewystarczająca weryfikacja kontrahenta (wykonawcy umowy)
13.	Brak lub niewystarczające zabezpieczenie interesów prawnych organizacji w zawartej umowie
14.	Brak spełnienia w umowie wymogów wynikających z przepisów obowiązującego prawa lub wymagań regulatora

Czynniki ryzyka zewnętrznego	
1.	Związane z otoczeniem politycznym i społeczno-gospodarczym
2.	Związane ze zmianą przepisów prawnych
3.	Związane z działalnością konkurencyjnych uczelni
4.	Związane ze zmianą preferencji i oczekiwań klientów UEW (kandydaci na studia, studenci, doktoranci, partnerzy biznesowi)
5.	Związane z działalnością dostawców UEW
6.	Zagrożenie kradzieżą, dewastacją mienia itp.

Czynniki ryzyka korupcji i nadużyć	
1.	Korupcja: Konflikt interesów przy realizacji zadań, który wpływa na podejmowane decyzje
2.	Korupcja: Przekupstwo, polegające na oferowaniu lub przyjmowaniu łapówek
3.	Korupcja: Przyjmowanie lub oferowanie dowodów wdzięczności, celem uzyskania osobistych korzyści
4.	Korupcja: Wymuszenie korzyści w celu ujawniania poufnych informacji lub podjęcia decyzji skutkującej korzyścią dla podmiotu lub osoby spoza organizacji
5.	Wpływy/ naciski zewnętrzne na pracowników UEW (zwłaszcza o charakterze korupcyjnym)
6.	Działanie lub zaniechanie działania, związane z wykorzystaniem stanowiska służbowego zajmowanego przez pracownika UEW, wypełniające znamiona korupcji
7.	Kumoterstwo związane z faworyzowaniem, oparte na nieformalnych powiązaniach
8.	Nierzetelne przeprowadzanie i dokumentowanie odbiorów realizowanych zadań inwestycyjnych, robót, usług i dzieł
9.	Przeprowadzanie i dokumentowanie postępowań o udzielenie zamówień publicznych w sposób nierzetelny oraz z naruszeniem obowiązujących przepisów
10.	Brak lub słabość kontroli
11.	Kradzież płatności wynikających z wystawionych faktur zanim zostaną ujęte w księgach i rejestrach organizacji
12.	Niezasadne wydatki wynikające z faktur za fikcyjne towary lub usługi, zawyżone faktury lub faktury za wydatki osobiste
13.	Fałszowanie dokumentacji (np. faktur, list płac, wniosków kredytowych, wniosków o dofinansowanie, dokumentacji rozliczeniowej)
14.	Nieuzasadnione zwroty kosztów związane z fikcyjnymi lub zawyżonymi wydatkami służbowymi

15.	Przechwytywanie lub fałszowanie płatności dokonywanych drogą elektroniczną
16.	Niewłaściwe wykorzystanie, w celach prywatnych, zasobów niepieniężnych pozostawionych pracownikowi do jego dyspozycji
17.	Kradzież zapasów lub innych aktywów niepieniężnych