Załącznik nr 1.3 do Zarządzenia nr 260/2026 Rektora APS
z dnia 08 czerwca 2026 r. zmieniający treść
Załącznika nr 1.3 do Polityki Zarządzania Ryzykiem
do Zarządzenia nr 425/2022 Rektora APS
z dnia 29 grudnia 2022 r.

Lista przykładowych czynników ryzyka*

Czynniki ryzyka finansowego

1. Zbyt niski budżet w stosunku do potrzeb i realizowanych zadań (niedoszacowanie kosztów).
2. Utrata lub ograniczanie istotnego źródła finansowania działalności (np. subwencji, grantów, spadek liczby studentów, konieczność zwrotu niewykorzystanych środków).
3. Zwrot środków z tytułu nieprawidłowości w rozliczaniu wsparcia finansowego (np. błędy przy rozliczaniu projektów).
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 (np. inflacja, wyższe koszty energii).
10. Brak lub niewystarczające zabezpieczenie środków finansowych na realizację umowy (ryzyko braku płynności w trakcie trwania umowy).
11. Brak weryfikacji warunków finansowych w zawieranych umowach (np. podpisanie umowy nieopłacalnej lub z ukrytymi kosztami).
12. Brak lub nieskuteczna weryfikacja merytoryczna, formalno-rachunkowa lub autoryzacja dokumentacji księgowej.
13. Błędy w rejestrowaniu transakcji w systemie finansowo-księgowym (np. błędy wprowadzania danych).
14. Błędy w opisie transakcji na dokumentach księgowych(np. błędne przypisanie do klasyfikacji budżetowej).

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 pracy, w tym nierównomierne obciążenie pracowników.
7. Brak lub nieefektywne monitorowanie realizacji zadań, w tym niezapewnienie niezależnego audytu lub kontroli.
8. Brak zastępowalności pracownika w czasie jego nieobecności.
9. Brak formalnych zasad i procedur zapewnienia ciągłości działania operacyjnego.
10. Brak lub niejasna misja i wizja, w tym niejasna ich 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. Nieobsadzenie stanowiska pracy.
2. Trudności w pozyskiwaniu pracownika w procesie rekrutacji.
3. Odejście kluczowych pracowników.
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 lub zorganizowanego mechanizmu szkoleń wewnętrznych lub zewnętrznych.
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 wykonywanymi zadaniami niezależnie od powodu.
12. Molestowanie pracownika w związku z wykonywanymi zadaniami, polegające na naruszaniu godności, poniżaniu i upokorzeniu.
13. Molestowanie seksualne, polegające na nieakceptowalnym przez pracownika zachowaniu o charakterze seksualnym, mający charakter fizyczny, werbalny lub poza werbalny.
14. Naruszenie zasad współżycia społecznego w miejscu pracy oraz w związku z wykonywaną pracą.

Czynniki 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 informatycznego.
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 zabezpieczenia fizyczne obiektów lub mienia przed zdarzeniami losowymi lub awaryjnymi.
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 egzekwowania zasad korzystania przez pracowników z aktywów i mienia Akademii.
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 Akademii
15. Brak lub ograniczone możliwości prowadzenia działalności w obecnej lokalizacji

16. Brak planów ochrony krytycznej infrastruktury lub planów ciągłości działania lub odstąpienie od ich aktualizacji.
17. Brak zabezpieczenia lub niewystarczające środki finansowe na utrzymanie infrastruktury informatycznej.

Czynniki ryzyka cyberbezpieczeństwa, bezpieczeństwa informacji i naruszenia danych osobowych

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 dokumentów wewnątrz Uczelni.
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 zapewnienia / 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 działania 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.
26. Brak lub nieaktualna polityka / procedury przetwarzania danych osobowych.
27. Niepełny zakres regulacji zabezpieczających przetwarzanie danych osobowych.
28. Brak lub nieaktualne procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

29. Wadliwe powołanie Inspektora Ochrony Danych (IOD).
30. Brak lub niewystarczające kompetencje Inspektora Ochrony Danych.
31. Naruszenie niezależności Inspektora Ochrony Danych.
32. Brak lub niewystarczające zasoby do realizacji zadań Inspektora Ochrony Danych.
33. Przetwarzanie danych osobowych w sytuacji braku lub niejasno wyrażonej przesłanki legalizującej.
34. Brak lub niewystarczający nadzór nad umowami powierzenia przetwarzania danych osobowych.
35. Brak lub niewystarczająca uzasadniona podstawa przetwarzania danych osobowych.
36. Brak lub niejasne cele przetwarzania danych osobowych.
37. Brak lub niekompetentne rejestrowanie czynności przetwarzania danych osobowych.
38. Brak lub niewystarczające i nieadekwatne zarządzanie ryzykiem przetwarzania danych osobowych.
39. Brak lub niewystarczające i nieadekwatne zabezpieczenie danych osobowych, brak domyślnej ochrony danych lub brak ochrony danych na etapie projektowania.
40. Brak, niepełna lub nierzetelna ocena zakresu i skutków przetwarzania danych osobowych.
41. Brak lub nierzetelne prowadzenie rejestru naruszeń ochrony danych osobowych.
42. Zaniechanie zawiadomienia o naruszeniu ochrony danych osobowych uprawnionych organów zewnętrznych.
43. Brak lub niewystarczająca świadomość użytkowników (pracowników, studentów) w zakresie cyberbezpieczeństwa i ochrony danych (podatność na ataki socjotechniczne, np. phishing).
44. Brak lub nieregularne testy penetracyjne i skanowanie podatności systemów IT.
45. Brak lub niejasne zasady dotyczące wykorzystywania prywatnych urządzeń pracowników do celów służbowych.

Czynniki ryzyka wizerunku

1. Brak lub niejasne zasady zarządzania wizerunkiem Akademii oraz procedury kontaktowania się z mediami i otoczeniem.
2. Brak lub nierzetelna weryfikacja zewnętrznych podmiotów współpracujących z Uczelnią.
3. Prowadzenie działalności lub badań o wysokiej wrażliwości społeczno-politycznej.
4. Niezadowolenie interesariuszy z działań Uczelni lub jej pracowników zgłaszane przez podmioty zewnętrzne.
5. Podejmowanie przez władze Uczelni decyzji nieakceptowalnych społecznie lub prawnie.
6. Działalność pracowników Uczelni naruszająca prawo, normy etyczne lub społecznego zaufania.

Czynniki ryzyka prawnego

1. Brak lub utrudniony dostęp do aktualnych informacji o zmianach w przepisach prawa.
2. Niejasność i niespójność przepisów prawa powszechnego, generująca błędy interpretacyjne.
3. Brak lub ograniczony dostęp do profesjonalnego wsparcia prawniczego.
4. Brak niekompletność lub niespójność procedur i regulacji wewnętrznych (wymagających dodatkowych interpretacji).
5. Nadmiar regulacji wewnętrznych skutkujący paraliżem operacyjnym.
6. Wzrost skali i częstotliwości naruszeń procedur wewnętrznych przez pracowników.
7. Podejmowanie działań bez wymaganej podstawy prawnej lub z jej przekroczeniem.
8. Wzrost liczby incydentów naruszenia przepisów prawa powszechnego.

9. Wzrost liczby sporów prawnych oraz wpływających pozwów sądowych.
10. Rosnąca liczba przegranych postępowań sądowych i administracyjnych.
11. Zawieranie umów nieuzasadnionych z punktu widzenia celów i strategii organizacji.
12. Brak lub niedostateczna weryfikacja wiarygodności kontrahenta.
13. Niedostateczne zabezpieczenie interesów prawnych i finansowych Uczelni w zapisach umowy.
14. Niezgodność zapisów umownych z bezwzględnie obowiązującymi przepisami prawa lub wytycznymi regulatora.

Czynniki ryzyka korupcji i nadużyć

1. Możliwość przedkładania przez osoby decyzyjne interesu prywatnego nad obowiązki służbowe.
2. Podatność pracowników na korzyść majątkową lub osobistą w zamian za faworyzowanie określonych podmiotów.
3. Przyzwolenie na nieformalne relacje i przyjmowanie drobnych upominków.
4. Niewystarczający poziom ochrony danych, brak audytowalności procedur dostępu do informacji poufnych oraz brak bezpiecznych kanałów sygnalizowania nieprawidłowości.
5. Wpływy / naciski zewnętrzne na pracowników Akademii (zwłaszcza o charakterze korupcyjnym).
6. Działanie lub zaniechanie działania, związane z wykorzystaniem stanowiska służbowego zajmowanego przez pracownika Akademii, mające 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. Przechwycenie lub defraudacja wpływów/należności pieniężnych wynikających z wystawionych faktur zanim zostaną ujęte w księgach i rejestrach Akademii.
12. Niezasadne wydatki wynikające z faktur za fikcyjne towary lub usługi zawyżone faktury lub faktury za wydatki osobiste.
13. Fałszowanie dokumentacji (np. faktur, list prac, 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.
18. Spadek motywacji i presja finansowa na pracowników wynikająca z niskiego poziomu wynagrodzeń.

Czynniki ryzyka zewnętrznego

1. Otoczenie polityczne (np. zmiana władzy, ustawy)
2. Otoczenie społeczno-gospodarcze (np. inflacja, kryzys finansowy).
3. Sytuacja demograficzna (np. niż demograficzny i mniejsza liczba absolwentów szkół średnich).
4. Zdarzenia losowe (np. pandemie, kataklizmy, kryzysy energetyczne, wojna).

5. Częste zmiany lub zmiana przepisów prawnych (np. nowelizacje Ustawy Prawo o szkolnictwie wyższym i nauce, zmiany standardów kształcenia, prawa pracy).
6. Działalność konkurencyjnych Uczelni krajowych.
7. Zmiana preferencji i oczekiwań klientów Akademii (kandydaci na studia, studenci, doktoranci, słuchacze, partnerzy biznesowi).
8. Dostawcy Uczelni.
9. Kradzież, dewastacja mienia.

_____

* Lista przykładowych czynników ryzyka może podlegać rozbudowywaniu bez potrzeby zmian w Polityce.