Instrukcja realizacji procesu zarządzania ryzykiem w Państwowej Wyższej Szkole Zawodowej w Głogowie

Instrukcja zawiera dwa katalogi: (1) katalog przykładowych czynników ryzyka oraz (2) katalog przykładów mechanizmów kontrolnych, które mogą ułatwić identyfikację oraz zarządzanie ryzykiem na uczelni. Poszczególne elementy katalogów są typowe i wykorzystywane na innych uczelniach, a także specyficzne dla Państwowej Wyższej Szkoły Zawodowej w Głogowie. Instrukcja jest merytorycznym uzupełnieniem „*Zarządzenia o Kontroli Zarządczej na PWSZ w Głogowie*" oraz „*Zarządzenia o Identyfikacji i Zarządzaniu Ryzkiem na PWSZ w Głogowie*".

Katalog przykładowych czynników ryzyka

Czynnik ryzyka	Przykład
Czynniki ryzyka finansowego	✓ Niski jest budżet w stosunku do zidentyfikowanych, zaakceptowanych potrzeb i realizowanych zadań; ✓ Występuje utrata lub odczuwalne ograniczenie istotnego, dostępnego źródła finansowania działalności; ✓ Nastąpiła potrzeba zwrotu środków z tytułu nieprawidłowości w rozliczaniu wsparcia finansowego; ✓ Wystąpiła utrata zdolności do terminowego regulowania zobowiązań przez PWSZ w Głogowie; ✓ Jest obowiązek uregulowania kwot finansowych (pieniężnych) tytułem odszkodowań, kar finansowych, odsetek karnych, kosztów procesowych i innych; ✓ Wystąpiło naruszenie dyscypliny finansów publicznych; ✓ Wystąpiło zaciąganie zobowiązań bez upoważnienia lub przekroczenia zakresu posiadanego upoważnienia; ✓ Nastąpiła utrata środków na realizację zadań i przyjętych projektów; ✓ Wystąpił wzrost wydatków czy kosztów prowadzonej działalności; ✓ Niewystarczające jest zabezpieczenie środków finansowych na realizację umów; ✓ Brak jest odpowiedniej weryfikacji warunków finansowych w zawieranych umowach; ✓ Brak jest lub występuje nieskuteczna weryfikacja/autoryzacja prowadzonej dokumentacji księgowej; ✓ Wystąpiły błędy w rejestrowaniu transakcji w systemie finansowo-księgowym na uczelni; ✓ Dostrzeżono błędy w opisie transakcji na dokumentach księgowych;
Czynniki ryzyka organizacyjnego	✓ Brak jest lub niejasno została przypisana odpowiedzialność za realizację danych celów i zadań; ✓ Zupełny brak lub nieodpowiednie jest do rzeczywistości planowanie realizacji zadań; ✓ Zupełny brak lub nieskuteczne są zasady zarządzania ryzykiem operacyjnym; ✓ Niejasno określone zostały standardy pracy oraz realizowanych zadań; ✓ Niejasne jest lub wystąpił brak priorytetów realizowanych zadań;

	✓ Nieefektywna i nieskuteczna jest organizacja realizacji zadań, a także wystąpiło nierównomierne obciążanie pracowników określonymi obowiązkami; ✓ Wystąpił brak lub nieefektywne jest monitorowanie realizacji zadań, w tym niezapewnienie zależnego audytu (kontroli); ✓ Wystąpił brak zastępowalności pracownika w czasie jego nieobecności; ✓ Wystąpił brak zasad i procedur zapewnienia ciągłości działania na poziomie operacyjnym; ✓ Wystąpił brak lub niejasna jest misja oraz wizja uczelni; ✓ Wystąpił brak zasad zarządzania zmianami i zarządzania w warunkach gwałtownych turbulencji; ✓ Wystąpił brak lub niedostosowanie do rzeczywistości planów długo- i krótkoterminowych; ✓ Wystąpił brak lub nieskuteczne są zasady zarządzania różnymi rodzajami ryzyka; ✓ Wystąpił brak lub niewystarczający jest nadzór nad realizacją umów;
Czynniki ryzyka zasobów ludzkich	✓ Nieobsadzone są stanowiska pracy (wakaty); ✓ Pojawiają się trudności w pozyskiwaniu pracownika w formie rekrutacji; ✓ Nastąpiło odejście kluczowych pracowników/pracownika z pracy; ✓ Brak jest pełnej zastępowalności personalnej na kluczowych stanowiskach; ✓ Brak jest planów sukcesji zawodowej i na kluczowych stanowiskach pracy; ✓ Wystąpiły niewystarczające umiejętności lub doświadczenie pracowników; ✓ Pojawiło się niezadowolenie pracowników z warunków zatrudnienia i realizowanej pracy; ✓ Wystąpił brak lub niewystarczająca jest liczba szkoleń dla pracowników; ✓ Pojawiają się konflikty w relacjach między pracownikami i/lub między pracownikami a przełożonymi; ✓ Nierówne jest traktowanie pracownika w związku z wykonywanymi zadaniami niezależnie od powodu tego traktowania; ✓ Pojawiło się zachęcanie do nierównego traktowania pracownika w związku z wykonywaniem zadań niezależnie od powodu tego traktowania; ✓ Pojawiło się molestowanie pracownika w związku z wykonywaniem zadania, polegające na naruszeniu godności, poniżaniu lub upokorzeniu; ✓ Pojawiło się molestowanie seksualne, polegające na nieakceptowalnym przez pracownika zachowaniu o charakterze seksualnym, mający charakter fizyczny, werbalny lub pozawerbalny; ✓ Wystąpiło naruszanie zasad współżycia społecznego w miejscu pracy oraz w związku z wykonywaną pracą;
Czynniki ryzyka infrastruktury i systemów informatycznych	✓ Pojawił się brak lub niewystarczające są informacje na temat ilości zasobów sieci i sprzętu teleinformatycznego na uczelni; ✓ Brak jest lub nieregularne są przeglądy stanu technicznego i sprzętu teleinformatycznego na uczelni; ✓ Brak jest lub nieregularne są przeglądy obiektów i mienia uczelnianego; ✓ Brak jest lub nieregularnie występuje fizyczne zabezpieczenie mienia przed niekorzystnymi zdarzeniami losowymi lub awariami;

	✓ Brak jest lub nieregularne są przeglądy stanu technicznego i sprzętu teleinformatycznego w kontekście zdarzeń losowych lub awarii; ✓ Wystąpił brak lub nieaktualna jest inwentaryzacja stanu i ilości obiektów infrastruktury i mienia; ✓ Wystąpił brak lub nieaktualna jest inwentaryzacja stanu sieci i sprzętu teleinformatycznego na uczelni; ✓ Pojawił się brak lub niewystarczające jest zabezpieczenie dostępu do obiektów lub mienia uczelnianego; ✓ Brak jest przypisania jednoznacznej własności mienia powierzonego pracownikom do wykorzystania dla celów służbowych; ✓ Brak jest określonej lub skutecznej formy nadzorowania zasad korzystania przez pracowników z aktywów i mienia uczelni; ✓ Wystąpił brak regularnych remontów i konserwacji majątku (sprzętu) uczelni; ✓ Brak jest zasad zwrotu i rozliczania mienia powierzonego pracownikom; ✓ Brak jest lub niejasne są zasady zapewnienia bezpieczeństwa pracownikom lub innym osobom, w związku z korzystaniem z aktywów i mienia uczelni; ✓ Wystąpił brak możliwości prowadzenia działalności w obecnej lokalizacji; ✓ Brak jest planów ochrony krytycznej infrastruktury i/lub planów ciągłości działania; ✓ Brak jest planów ciągłości funkcjonowania mienia (sprzętu) uczelni lub odstąpienia od ich aktualizacji;
Czynnik ryzyka bezpieczeństwa informacji	✓ Wystąpił brak lub niejasne są zasady/polityki zarządzania bezpieczeństwem informacji na uczelni; ✓ Pojawił się brak lub nieregularne są przeglądy zasad/polityki zarządzania bezpieczeństwem informacji na uczelni; ✓ Wystąpił brak lub niejasno są przypisane zakresy odpowiedzialności w zakresie bezpieczeństwa informacji na uczelni; ✓ Brak jest lub niejasno są określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników uczelni; ✓ Pojawił się brak lub niejasno zostały określone zasady zachowania poufności informacji przez podmioty zewnętrzne, na przykład w związku z realizowanymi umowami; ✓ Brak jest lub niejasno zostały określone zasady obiegu dokumentacji wewnątrz uczelni; ✓ Wystąpił brak lub niejasno są określone zasady kontaktowania się pracowników z podmiotami zewnętrznymi, w tym korzystania przez pracowników z mediów społecznościowych w ramach realizowanych zadań; ✓ Pojawił się brak zabezpieczenia/inwentaryzacji miejsca przechowania i nośników informacji na uczelni; ✓ Wystąpił brak lub niejasne są zasady udzielania informacji podmiotom zewnętrznym; ✓ Pojawił się brak lub nieregularne jest archiwizowanie informacji; ✓ Wystąpił brak lub niejasne są zasady dostępu użytkowników do sieci teleinformatycznej, w tym rejestracji, udzielania przywilejów, zarządzania hasłami oraz odbioru praw; ✓ Pojawił się brak lub niewłaściwa jest ochrona przed nieautoryzowanym dostępem do systemów operacyjnych; ✓ Wystąpił brak lub niewłaściwa jest ochrona przed nieuprawionym dostępem do informacji w aplikacji, w tym luki w użytkowanych systemach;

	✓ Brak jest lub niejasne, w tym nieaktualne są zasady pracy przy przetwarzaniu mobilnym i na odległość; ✓ Wystąpił brak lub niewłaściwa jest ochrona przed dokonywaniem nieuprawnionych zmian informacji w systemach i/lub aplikacjach; ✓ Pojawił się brak lub niewłaściwa jest ochrona bezpieczeństwa plików systemowych; ✓ Wystąpił brak lub niejasne są zasady zarządzania incydentami w zakresie bezpieczeństwa; ✓ Wystąpił brak działania lub działanie z opóźnieniem w sytuacji wystąpienia incydentów bezpieczeństwa teleinformatycznego; ✓ Wystąpił brak lub niewystarczające jest zapewnienie wsparcia teleinformatycznego w zawieranych umowach serwisowych; ✓ Wystąpił brak zapewnienia ciągłości działania systemów teleinformatycznych; ✓ Pojawił się brak lub niewystarczające są zabezpieczenie dostępu do sieci i sprzętu teleinformatycznego przez pracowników i uczelnię; ✓ Wystąpił brak lub nieskuteczna jest ochrona antywirusowa lub brak jest ochrony przed działaniami hackerskimi; ✓ Wystąpił brak lub nieregularne jest tworzenie kopii zapasowych informacji przetwarzanych w systemach teleinformatycznych; ✓ Wystąpił brak lub niejasne są zasady używania przez pracowników uczelnianych nośników informatycznych; ✓ Wystąpił brak lub niejasne są zasady ochrony dokumentacji systemów teleinformatycznych;
Czynnik ryzyka naruszania danych osobowych	✓ Wystąpił brak lub nieaktualna jest polityka/procedury przetwarzania danych osobowych; ✓ Występuje niepełny zakres regulacji zabezpieczających przetwarzania danych osobowych; ✓ Wystąpił brak lub nieaktualne są procedury postępowania w sytuacji naruszania ochrony danych osobowych; ✓ Wadliwe jest powołanie lub występuje brak inspektora ochrony danych osobowych; ✓ Wystąpił brak lub niewystarczające są zasoby do realizacji zadań z zakresu ochrony danych osobowych; ✓ Nastąpiło naruszenie niezależności inspektora ochrony danych; ✓ Wystąpił brak lub niewystarczające są zasoby do realizacji zadań inspektora ochrony danych osobowych; ✓ Pojawiło się przetwarzanie danych w sytuacji braku lub niejasno wyrażonej zgody na przetwarzanie danych osobowych; ✓ Wystąpił brak lub niewystarczający jest nadzór nad umowami przetwarzania danych osobowych; ✓ Wystąpił brak lub niewystarczająco uzasadniona jest podstawa przetwarzania danych osobowych; ✓ Wystąpił brak lub niejasne są cele przetwarzania danych osobowych; ✓ Wystąpił brak lub niska jest jakość procesu oceny przetwarzania danych osobowych; ✓ Wystąpił brak lub niekompletne jest rejestrowanie czynności przetwarzania danych osobowych; ✓ Wystąpił brak lub niewystarczające i nieadekwatne jest zarządzanie ryzykiem przetwarzania danych osobowych; ✓ Wystąpił brak lub niewystarczająca i nieadekwatne jest zarządzanie danych osobowych chronionych domyślnie lub na etapie projektowania; ✓ Pojawił się brak, niepełna lub nierzetelna jest ocena zakresu i skutków przetwarzania danych osobowych; ✓ Wystąpił brak lub nierzetelne jest prowadzenie rejestru naruszeń ochrony danych osobowych;

	✓ Nastąpiło zaniechanie zawiadomienia o naruszeniu danych osobowych uprawnionych;
Czynnik ryzyka wizerunku	✓ Wystąpił brak lub niejasne są zasady zarządzania wizerunkiem organizacji oraz kontaktowania się z mediami i opinią publiczną; ✓ Wystąpił brak lub nierzetelna jest weryfikacja zewnętrznych podmiotów współpracujących; ✓ Wysoka jest wrażliwość polityczna prowadzonej działalności; ✓ Pojawiły się skargi na pracowników od podmiotów zewnętrznych; ✓ Pojawiło się podejmowanie na uczelni działań nieakceptowalnych społecznie, etycznie lub prawnie; ✓ Nieakceptowana społecznie, etycznie lub prawnie jest działalności pracowników uczelni pod jej szyldem;
Czynnik ryzyka prawnego	✓ Wystąpił brak lub ograniczony jest dostęp do informacji o zmieniających się przepisach prawa; ✓ Pojawia się duża liczba niejasnych przepisów prawa, wymagających dodatkowej interpretacji; ✓ Wystąpił brak lub ograniczony jest dostęp do usług czy wsparcia prawnego; ✓ Wystąpił brak lub niejasne są regulacje wewnętrzne (wymagają dodatkowych interpretacji); ✓ Nadmierna jest liczba regulacji wewnętrznych powodująca nieefektywne działanie i szum informacyjny; ✓ Rosnąca jest liczba naruszeń regulacji wewnętrznych; ✓ Pojawiają się działanie bez lub z naruszeniem odpowiedniej podstawy prawnej; ✓ Rosnąca jest liczba naruszeń prawa zewnętrznego; ✓ Rosnąca jest liczba spraw lub pozwów sądowych; ✓ Rosnąca jest liczba przegranych spraw sądowych; ✓ Wystąpił brak uzasadnienia zawarcia umowy z punktu widzenia realizacji celów i zadań projektu lub uczelni; ✓ Wystąpił brak lub niewystarczająca jest weryfikacja kontrahenta (wykonawcy umowy); ✓ Wystąpił brak lub niewystarczające jest zabezpieczenie interesów prawnych organizacji w zawartej umowie; ✓ Brak jest spełnienia w umowie wymogów wynikających z przepisów obowiązującego prawa lub wymagań;
Czynnik ryzyka zewnętrznego	✓ Pojawił się konflikt interesów przy realizacji zadań, który wpływa na podejmowane decyzje; ✓ Pojawiło się przekupstwo (korupcja), polegające na oferowaniu lub przyjmowaniu łapówek; ✓ Pojawiło się przyjmowanie lub oferowanie dowodów wdzięczności (prezentów), celem uzyskania osobistych korzyści; ✓ Wystąpiło wymuszenie korzyści w celu ujawnienia poufnych informacji lub podjęcia decyzji skutkującej korzyścią dla podmiotu lub osoby spoza organizacji; ✓ Pojawiły się wpływy/naciski zewnętrzne na pracowników PWSZ w Głogowie; ✓ Pojawiło się działanie lub zaniechanie działania, związane z wykorzystaniem stanowiska służbowego zajmowanego przez pracownika PWSZ w Głogowie, wypełniające znamiona korupcji; ✓ Pojawiło się kumoterstwo i nepotyzm związane z faworyzowaniem, oparte na nieformalnych lub rodzinnych powiązaniach; ✓ Występuje nierzetelne przeprowadzenie i dokumentowanie odbiorów realizowanych zadań inwestycyjnych, robót, usług i dzieł;

	✓ Występuje przeprowadzenie i dokumentowanie postępowań o udzielenie zamówień publicznych w sposób nierzetelny oraz z naruszeniem obowiązujących przepisów prawa; ✓ Wystąpił brak lub słabość kontroli; ✓ Pojawiła się kradzież płatności wynikających z wystawionych faktur zanim zostaną ujęte w księgach i rejestrach organizacji; ✓ Pojawiły się niezasadne wydatki wynikające z faktur za fikcyjne towary lub usługi, zawyżone faktury lub faktury za wydatki osobiste; ✓ Występuje fałszowanie dokumentacji; ✓ Pojawiły się nieuzasadnione zwroty kosztów związane z fikcyjnymi lub zawyżonymi wydatkami służbowymi; ✓ Występuje przechowywanie lub fałszowanie płatności dokonywanych drogą elektroniczną; ✓ Niewłaściwe jest wykorzystanie, w celach prywatnych, zasobów niepieniężnych pozostawionych pracownikowi do jego dyspozycji; ✓ Nastąpiła kradzież zapasów lub innych aktywów niepieniężnych;

Katalog przykładów mechanizmów kontrolnych

Lp.	Standard	Zalecenia jakościowe	Przykłady zalecanych praktyk
1.	**Ewidencja dokumentacji systemu kontroli zarządczej**	- Dokumentacja systemu kontroli zarządczej obejmuje wszystkie procedury wewnętrzne, instrukcje, wytyczne, dokumenty określające zakres obowiązków, uprawnień i odpowiedzialności pracowników i inne dokumenty wewnętrzne oraz rejestr obowiązujących przepisów wewnętrznych; - Dokumentacja systemu kontroli zarządczej jest dostępna dla wszystkich osób, którym jest niezbędna; - Dokumentacja systemu kontroli zarządczej jest systematycznie aktualizowana.	- stworzenie wykazu regulacji prawnych, - archiwizacja akt spraw, - uporządkowane zapisy w systemach informatycznych są stosowane, - składanie pisemnych potwierdzeń wykonanych weryfikacji, zatwierdzeń i stosowania mechanizmów kontroli jest stosowane.
2.	**Monitoring wykonywanych zadań**	- Wprowadzenie nadzoru nad wykonywaniem zadań w celu ich oszczędnej, efektywnej i skutecznej realizacji, z uwzględnieniem właściwego sposobu podziału zadań i odpowiedzialności oraz zakresu decyzji możliwych do podjęcia przez poszczególne osoby.	- instruktaż stanowiskowy dla pracowników jest realizowany, - weryfikacja i zatwierdzanie poszczególnych działań ma miejsce, - informacja zwrotna od przełożonego do pracownika o sposobie wykonania zadania jest przekazywana, - wykorzystywane są praktyki określone w standardach obejmujących cele

			i zarządzanie ryzykiem oraz monitorowanie i ocena.
3.	**Zabezpieczenie ciągłości działania uczelni**	- Wdrożenie mechanizmów kontrolnych zapobiegających zdarzeniom, które mogą spowodować zatrzymanie działalności uczelni – w ramach przeprowadzonej analizy ryzyka należy również uwzględnić tego typu zdarzenia; - Zostały wskazane osoby zastępujące każdego z pracowników w przypadku jego nieobecności; - Zostały wskazane osoby zastępujące poszczególne osoby zarządzające podczas ich nieobecności; - Opracowany został plan bezpieczeństwa na wypadek przerw w działaniu systemów informatycznych.	- procedury ciągłości działania są określone, - procedury/plany zastępstw są przygotowane, - plany działalności systemów informatycznych są opracowane, - tworzenie kopii zapasowych jest obowiązkiem, - zapisy w umowach z dostawcami energii, mediów, usług informatycznych i teleinformatycznych są sprecyzowane.
4.	**Ochrona zasobów (niefinansowych) uczelni**	- Dostęp do zasobów mają jedynie upoważnione osoby; - Określono odpowiedzialność kierującym komórkami organizacyjnymi i pozostałym pracownikom za zapewnienie ochrony i właściwe wykorzystanie zasobów jednostki; - Weryfikowanie czy dostęp do poszczególnych zasobów, w tym m.in. do danych osobowych jest limitowany oraz przypisany do właściwych osób, z uwzględnieniem wyników analizy i oceny ryzyka w tym zakresie; - Zapewnione zostało bezpieczeństwo fizyczne obiektów, w tym przeciwpożarowe; - Istnieją i są stosowane zasady BHP.	- procedury zapewnienia jakości istnieją, - procedury cyberbezpieczeństwa są określone, - procedury zarządzania bezpieczeństwem informacji istnieją, - polityki i procedury bezpieczeństwa teleinformatycznego istnieją i są znane, - procedury ochrony danych osobowych są bezwzględnie stosowane, - instrukcja bezpieczeństwa przeciwpożarowego istnieje i obowiązuje, - procedury BHP są znane i aktualizowane, - procedury ochrony informacji prawnie chronionych są stosowane.
5.	**Procedury kontroli dotyczące operacji gospodarczych i finansowych**	- Zaciąganie zobowiązań w granicach określonych w planie finansowym; - Ustalenie limitów do podejmowania decyzji finansowych i gospodarczych przez upoważnione osoby;	- plany finansowe istnieją, - polityka rachunkowości jest stosowana, - instrukcja obiegu dokumentacji

		– Rzetelne i pełne dokumentowanie oraz rejestrowanie operacji finansowych i gospodarczych; – Wielokrotna weryfikacja operacji finansowych i gospodarczych; – Zatwierdzane (autoryzacja) operacji finansowych i gospodarczych przez Rektora/Kwestora lub przez osoby upoważnione; – Weryfikacja wykonawcy, dostawcy oraz kontrahenta pod kątem wykonalności umowy oraz zabezpieczenia przed ryzykiem korupcji jest stosowana; – Konsekwentne opiniowanie projektów umów przez radcę prawnego; – Stosuje się ograniczenie stosowania płatności gotówkowych w związku z wykonywanymi operacjami finansowymi.	finansowo-księgowej istnieje i obowiązuje, – procedury windykacji i egzekucji należności są wykorzystywane, – procedury rozliczania delegacji służbowych jest stosowana, – procedury udzielania zamówień publicznych, w tym weryfikacji kontrahentów są konsekwentnie wykorzystywane, – wykaz zawieranych umów istnieje, – na bieżąco aktualizowany jest system finansowo-księgowy.
6.	**Procedury kontroli dotyczące systemów informatycznych**	– Mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych, obejmują m.in. mechanizmy kontroli dostępu do zasobów informatycznych, mające na celu ich ochronę przed nieautoryzowanymi zmianami, utratą lub ujawnieniem; – Stosowane jest licencjonowanie i regularne aktualizowanie wykorzystywanego oprogramowania komputerowego; – Istnieją mechanizmy kontroli stosowanego oprogramowania systemowego; – Stan infrastruktury sieciowej jest adekwatny do potrzeb uczelni; – Dokonuje się regularnych audytów systemów informatycznych.	– standardy budowy i rozwoju infrastruktury sieciowej jest przestrzegany, – wykaz licencjonowanego oprogramowania i aplikacji istnieje, – praktyki z obszaru standardu ochrony zasobów są stosowane.