PRZYKŁADY MECHANIZMÓW KONTROLNYCH

LP	STANDARD	ZALECENIA JAKOŚCIOWE	PRZYKŁADY ZALECANYCH PRAKTYK
1.	**Dokumentowanie systemu kontroli zarządczej**	a. Dokumentacja systemu kontroli zarządczej obejmuje procedury wewnętrzne, instrukcje, wytyczne, dokumenty określające zakres obowiązków, uprawnień i odpowiedzialności pracowników i inne dokumenty wewnętrzne oraz rejestr obowiązujących przepisów wewnętrznych; b. Dokumentacja systemu kontroli zarządczej jest dostępna dla wszystkich osób, dla których jest niezbędna; c. Dokumentacja systemu kontroli zarządczej jest na bieżąco aktualizowana	▪ Wykaz regulacji wewnętrznych ▪ Akta spraw ▪ Zapisy w systemach IT ▪ Pisemne potwierdzanie wykonywanych weryfikacji, zatwierdzeń i stosowania mechanizmów kontroli
2.	**Nadzór nad wykonywaniem zadań**	a. Wprowadzono nadzór nad wykonaniem 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 pracownika ▪ Weryfikacja i zatwierdzanie działań ▪ Informacja zwrotna przełożonego do pracownika o sposobie wykonania zadania ▪ Praktyki określone w standardach obejmujących cele i zarządzanie ryzykiem oraz monitorowanie i ocena
3.	**Zapewnienie ciągłości działania**	a. Wdrożenie mechanizmów kontrolnych zapobiegających zdarzeniom, które mogą spowodować zatrzymanie działalności - w ramach przeprowadzanej analizy ryzyka należy również uwzględnić tego typu zdarzenia. b. Zostały wskazane osoby zastępujące każdego z pracowników w przypadku jego nieobecności. c. Zostały wskazane osoby zastępujące poszczególne osoby zarządzające podczas ich nieobecności. d. Opracowany został plan bezpieczeństwa na wypadek przerw w działaniu systemów informatycznych.	▪ Procedury ciągłości działania ▪ Procedury/plany zastępstw ▪ Plany działalności systemów informatycznych ▪ Tworzenie kopii zapasowych ▪ Zapisy w umowach z dostawcami energii, mediów, usług informatycznych i telekomunikacyjnych
4.	**Ochrona zasobów (niefinansowych)**	a. Dostęp do zasobów mają jedynie upoważnione osoby. b. Określono odpowiedzialność kierującym komórkami organizacyjnymi i pozostałym pracownikom za zapewnienie ochrony i właściwe wykorzystanie	▪ Procedury zapewnienia zgodności. ▪ Procedury cyberbezpieczeństwa ▪ Procedury zarządzania bezpieczeństwem

		zasobów jednostki. c. 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. d. Zapewnione zostało bezpieczeństwo fizyczne obiektów, w tym przeciwpożarowe. e. Istnieją i są stosowane zasady BHiP.	informacji ▪ Polityki i procedury bezpieczeństwa teleinformatycznego ▪ Procedury ochrony danych osobowych ▪ Instrukcja bezpieczeństwa przeciwpożarowego ▪ Procedury BHiP ▪ Procedury ochrony informacji prawnie chronionych
5.	**Mechanizmy kontroli dotyczące operacji gospodarczych i finansowych**	a. Zaciąganie zobowiązań w granicach określonych w planie finansowym. b. Ustalenie limitów do podejmowania decyzji finansowych i gospodarczych przez upoważnione osoby. c. Rzetelne i pełne dokumentowanie i rejestrowanie operacji finansowych i gospodarczych. d. Weryfikacja operacji finansowych i gospodarczych z zastosowaniem zasady wielu par oczu. e. Zatwierdzanie (autoryzacja) operacji finansowych i gospodarczych przez Rektora/Kanclerza lub osoby przez niego upoważnione. f. Weryfikacja wykonawcy, dostawcy oraz kontrahenta pod kątem wykonalności umowy oraz zabezpieczenia przed ryzykiem korupcji. g. Zabezpieczenie interesów jednostki w zawieranych umowach. h. Opiniowanie projektów umów przez radcę prawnego. i. Ograniczenie stosowania płatności gotówkowych w związku z wykonywanymi operacjami finansowymi.	▪ Plany finansowe ▪ Polityka rachunkowości ▪ Instrukcja obiegu dokumentacji finansowo-księgowej ▪ Procedury windykacji i egzekucji należności ▪ Procedury rozliczania delegacji służbowych ▪ Procedury udzielania zamówień publicznych, w tym weryfikacji kontrahentów ▪ Wykaz zawieranych umów ▪ Na bieżąco aktualizowany system finansowo-księgowy.
6.	**Mechanizmy kontroli dotyczące systemów informatycznych**	a. 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. b. Stosowane jest licencjonowane i regularnie aktualizowane oprogramowanie. c. Istnieją mechanizmy kontroli oprogramowania systemowego. d. Stan infrastruktury sieciowej jest adekwatny do potrzeb jednostki. e. Dokonuje się regularnych audytów systemów informatycznych	▪ Standardy budowy i rozwoju infrastruktury sieciowej ▪ Wykaz aktywów w systemach teleinformatycznych ▪ Wykaz licencjonowanego oprogramowania i aplikacji ▪ Praktyki z obszaru standardu ochrony zasobów