

System Zarządzania Bezpieczeństwem Zasobów na Politechnice Śląskiej

Rozdział I

CELE I ZAŁOŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM ZASOBÓW NA POLITECHNICE ŚLĄSKIEJ

§ 1

1. System Zarządzania Bezpieczeństwem Zasobów (SZBZ) określa ramy postępowania związanego z zarządzaniem bezpieczeństwem i ochroną zasobów na Politechnice Śląskiej. SZBZ jest zgodny ze standardami kontroli zarządczej dla sektora finansów publicznych, określonymi przez ministra finansów.
2. Celem SZBZ jest wspomaganie kadry zarządzającej Politechniki Śląskiej w wypełnianiu podstawowych zadań statutowych Politechniki Śląskiej oraz zapewnienie procedur zapobiegających wykorzystywaniu zasobów Uczelni w sposób, który może spowodować zagrożenie dla życia i zdrowia ludzi, bezpieczeństwa i porządku publicznego, cyberprzestrzeni, a także procedur postępowania w przypadku powstania zagrożenia na terenie Uczelni.
3. Opracowanie SZBZ ma na celu optymalne wykorzystanie zasobów przy jednoczesnym ograniczeniu strat i marnotrawstwa, które mogą wystąpić na skutek niewłaściwego alokowania zasobów bądź zaniechania działań chroniących zasoby.

§ 2

1. Ograniczenie niewłaściwego gospodarowania zasobami i ochrona zasobów prowadzona jest przez zaprojektowanie i wdrożenie odpowiednich mechanizmów kontrolnych na podstawie wyników monitoringu poziomu ryzyka odniesionego do zasobów oraz jego oceny, jak i podjęcie działań zmniejszających skutki zaistniałych negatywnych zdarzeń.
2. System Zarządzania Bezpieczeństwem Zasobów został opracowany przy uwzględnieniu specyficznych cech i uwarunkowań środowiskowych Uczelni.

Rozdział II
ZAKRES PODMIOTOWY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM
ZASOBÓW

§ 3

1. System Zarządzania Bezpieczeństwem Zasobów ma zastosowanie do wszystkich jednostek organizacyjnych Uczelni oraz wszystkich pracowników zatrudnionych w Uczelni.
2. System Zarządzania Bezpieczeństwem Zasobów obejmuje poziomy:
 - 1) strategiczny,
 - 2) operacyjny,
 - 3) projektów.
3. Zarządzanie i ochrona zasobów w Uczelni na poziomie strategicznym polega na identyfikacji i analizie zasobów w oparciu o analizę i ocenę ryzyka strategii. Na tym poziomie dokonuje się wyznaczenia osób lub zespołów odpowiedzialnych za identyfikację i analizę zasobów newralgicznych oraz definiowanie instrukcji zabezpieczających właściwe wykorzystanie zasobów.
4. Zarządzanie i ochrona zasobów w Uczelni na poziomie operacyjnym polega na działaniach związanych z przestrzeganiem procedur dotyczących ochrony i wykorzystania zasobów w jednostkach organizacyjnych Uczelni oraz na bieżącej identyfikacji i ocenie poziomu wykorzystania zasobów.
5. Zarządzanie i ochrona zasobów w Uczelni na poziomie projektów polega na działaniach związanych z przestrzeganiem procedur dotyczących ochrony i wykorzystania zasobów w ramach projektów.
6. Zarządzanie i ochrona zasobów na każdym z poziomów obejmuje następujące etapy:
 - 1) identyfikację zasobów, które wiążą się z realizacją celów Uczelni,
 - 2) ocenę istniejących zasobów i stopnia ich wykorzystywania,
 - 3) analizę i ocenę zasobów w celu wyodrębnienia zasobów newralgicznych,
 - 4) zdefiniowanie działań wymaganych do postępowania z zasobami newralgicznymi,
 - 5) wskazanie osób z kierownictwa Uczelni odpowiedzialnych za podjęcie działań zaradczych oraz ustalenie daty, do której należy podjąć działania.

Rozdział III

ZASADY ODPOWIEDZIALNOŚCI ZA REALIZACJĘ SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM ZASOBÓW

§ 4

1. Za realizację zadań Systemu Zarządzania Bezpieczeństwem Zasobów na poziomie strategicznym odpowiada Rektor Uczelni, poprzez:
 - 1) kształtowanie i wdrażanie polityki ochrony zasobów oraz nadzór nad nią,
 - 2) identyfikację zasobów newralgicznych na poziomie strategicznym,
 - 3) wyznaczanie właścicieli zasobów na poziomie strategicznym,
 - 4) określenie osób lub zespołów odpowiedzialnych za opracowanie szczegółowych instrukcji zaradczych w zakresie ochrony zasobów,
 - 5) wdrażanie instrukcji ochrony zasobów oraz monitorowanie skuteczności mechanizmów kontroli zarządzania zasobami.
2. W proces zarządzania i ochrony zasobów na poziomie strategicznym włączeni są Prorektorzy oraz Kanclerz i Kwestor.
3. Rektor może przypisać odpowiedzialność za ochronę newralgicznych zasobów właściwemu merytorycznie Prorektorowi, Kanclerzowi lub Kwestorowi Uczelni.

§ 5

Na poziomie operacyjnym za realizację celów Systemu Zarządzania Bezpieczeństwem Zasobów odpowiadają kierownicy jednostek organizacyjnych, poprzez:

- 1) identyfikację i udokumentowanie zasobów, które są istotne dla osiągnięcia celów operacyjnych, w odniesieniu do zdefiniowanych obszarów działania,
- 2) ocenę istotności zasobu w odniesieniu do realizowanych celów, z uwzględnieniem negatywnych skutków wywołanych jego brakiem lub niewłaściwym gospodarowaniem,
- 3) monitoring poziomu zasobów, w tym funkcjonowania mechanizmów kontrolnych pod kątem ich adekwatności i skuteczności, a także wszelkich odstępstw od istniejących procedur,
- 4) projektowanie działań zaradczych dotyczących zasobów poprzez zlecenie wyznaczonym osobom lub zespołom obowiązku w zakresie opracowania rozwiązań, które przyczynią się do poprawy ochrony zasobów.

§ 6

Na poziomie projektu za System Zarządzania Bezpieczeństwem Zasobów odpowiada kierownik projektu poprzez:

- 1) identyfikację zasobów, w tym zwłaszcza zasobów newralgicznych, które są właściwe dla projektu,
- 2) ocenę zasobów i ich wpływu na realizację projektu, przy uwzględnieniu istniejących mechanizmów kontrolnych,
- 3) zaprojektowanie mechanizmów kontrolnych ograniczających ryzyko zarządzania zasobami newralgicznymi w projekcie,
- 4) zgłaszanie bezpośrednio przełożonemu istotnych utrudnień w realizacji celu projektu.

Rozdział IV PRZEPISY KOŃCOWE

§ 7

Zobowiązuje się Rektora do opracowania nowych lub aktualizacji istniejących wewnętrznych regulacji dotyczących Systemu Zarządzania Bezpieczeństwem Zasobów w zakresie:

- wykonywania zadań obronnych, obrony cywilnej, ochrony informacji niejawnych i ochrony przeciwpożarowej,
- postępowania na wypadek groźby podłożenia lub zdetonowania ładunku wybuchowego,
- działalności Straży Akademickiej,
- ochrony danych osobowych przetwarzanych na Politechnice Śląskiej,
- ochrony informacji niejawnych na Politechnice Śląskiej,
- zasad zarządzania obiektami budowlanymi,
- ochrony systemów informatycznych,
- substancji chemicznych i ich mieszanin stosowanych i przechowywanych,
- zasad korzystania z usług telekomunikacyjnych i prawidłowego użytkowania infrastruktury łączności telefonicznej,
- wystąpienia zagrożenia terroryzmem i przypominania o systemie zgłaszania o zaistniałym zagrożeniu,
- współdziałania z policją w zakresie ochrony zasobów Uczelni.