|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nazwa  i symbol jednostki | INSPEKTORAT SPRAW OBRONNYCH  I BEZPIECZEŃSTWA INFORMACJI | | | **ROI** |
| Jednostka  nadrzędna | Podległość formalna | | Podległość merytoryczna | |
| Rektor | R | Rektor | R |
| Jednostki  podległe | Podległość formalna | | Podległość merytoryczna | |
|  |  |  |  |
|  | | | | |
| Cel działalności | | | | |
| * Tworzenie i utrzymanie warunków do właściwego funkcjonowania Uniwersytetu w sytuacjach kryzysowych, zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny. * Zapewnienie bezpieczeństwa informacji niejawnych, danych osobowych oraz informacji istotnych  z punktu widzenia interesów Uczelni. | | | | |
| Kluczowe zadania | | | | |
| **W zakresie zarządzania kryzysowego:**   1. Organizacja i zapewnienie właściwego funkcjonowania Zespołu Zarządzania Kryzysowego Uniwersytetu. 2. Tworzenie dokumentów w zakresie zarządzania kryzysowego oraz ustalanie procedur zarządzania  i ich uruchamiania w sytuacjach kryzysowych. 3. Identyfikowanie ryzyk i wdrażanie działań zapobiegających sytuacjom kryzysowym. 4. Gromadzenie informacji o istotnych zagrożeniach oraz środkach zapobiegania i przeciwdziałania sytuacjom kryzysowym.   **W zakresie spraw obronnych i obrony cywilnej:**   1. Opracowywanie i aktualizowanie Planu Operacyjnego Uniwersytetu w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny. 2. Koordynacja działań w zakresie realizacji zadań operacyjnych oraz przedsięwzięć wynikających  z Planu Operacyjnego Uniwersytetu Medycznego. 3. Opracowanie i wdrażanie Planu Obrony Cywilnej Uniwersytetu Medycznego. 4. Organizacja i zapewnienie właściwego funkcjonowania systemu Stałego Dyżuru Uniwersytetu. 5. Przeprowadzanie okresowych i rocznych analiz oraz ocen stanu właściwego przygotowania Uniwersytetu do realizacji zadań w zakresie obrony cywilnej. 6. Podejmowanie działań w kierunku przygotowania techniczno-organizacyjnego Uniwersytetu  w celu udzielania pomocy poszkodowanym na wypadek nadzwyczajnych zagrożeń, do czasu przejęcia akcji ratowniczej przez wyspecjalizowane służby. 7. Planowanie, organizowanie i prowadzenie szkoleń w zakresie spraw obronnych i obrony cywilnej. 8. Prowadzenie dokumentacji i sprawozdawczości związanej ze sprawami obronnymi i zadaniami obrony cywilnej w Uczelni.   **W zakresie bezpieczeństwa informacji:**   1. Prowadzenie wykazu stanowisk oraz osób dopuszczonych do pracy z dostępem do informacji niejawnych. 2. Organizacja systemu ochrony informacji niejawnych, w tym opracowywanie, wdrażanie  i aktualizowanie planu ochrony informacji niejawnych. 3. Zarządzanie ryzykiem bezpieczeństwa informacji niejawnych. 4. Prowadzenie okresowych kontroli w zakresie przestrzegania przepisów i stosowania zabezpieczeń dotyczących informacji niejawnych, w tym sprawowanie nadzoru nad ochroną i zabezpieczeniem systemów teleinformatycznych do przetwarzania informacji niejawnych. 5. Planowanie, organizowanie i prowadzenie szkoleń z zakresu ochrony informacji niejawnych. 6. Opracowywanie procedur wewnętrznych i instrukcji w zakresie ochrony informacji niejawnych, w tym procedury przetwarzania informacji o klauzuli „poufne” i „zastrzeżone” oraz nadzorowanie ich realizacji. 7. Wskazywanie kierunków działań naprawczych oraz minimalizujących przesłanki do powstawania zdarzeń negatywnych w obszarze bezpieczeństwa informacji.   **W zakresie ochrony danych osobowych:**   1. Tworzenie warunków i nadzór nad bezpieczeństwem danych osobowych w Uniwersytecie zgodnie  z aktualnie obowiązującymi przepisami o ochronie danych osobowych, w tym informowanie władz Uniwersytetu, podmiotów przetwarzających oraz pracowników o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, a także doradzanie we wszelkich kwestiach związanych z przetwarzaniem danych osobowych. 2. Ocena i monitorowanie skuteczności działania wdrożonych środków organizacyjnych i technicznych w zakresie ochrony danych osobowych, w tym prowadzenie audytów w tym zakresie. 3. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych  w Uniwersytecie, w tym prowadzenie działań zwiększających świadomość w obszarze przetwarzania danych osobowych. 4. Pełnienie funkcji punktu kontaktowego w sprawach związanych z przetwarzaniem danych osobowych oraz wykonywaniem praw przysługujących osobom, których dane dotyczą. 5. Współpraca, prowadzenie konsultacji oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego.   **W zakresie funkcjonowania kancelarii niejawnej**   1. Zapewnienie bezpieczeństwa fizycznego materiałom i dokumentom zawierającym informacje niejawne i inne tajemnice ustawowo chronione, związane z przetwarzaniem informacji niejawnych. 2. Dokumentowanie, kontrola obiegu i archiwizacja dokumentów niejawnych. 3. Ewidencjonowanie i przechowywanie materiałów i dokumentów zawierających informacje niejawne, uwierzytelnianie dokumentów niejawnych. | | | | |