

Zasady Ochrony Informacji Niejawnych w Politechnice Warszawskiej

§ 1

1. Przez informacje niejawne rozumie się informacje stanowiące tajemnicę państwową lub służbową, niezależnie od formy i sposobu ich wyrażania, które wymagają ochrony przed nieuprawnionym ujawnieniem, także w trakcie ich opracowania.
2. Ilekroć w przepisach poniższych jest mowa o tajemnicy państwowej, tajemnicy służbowej, rękojmi zachowania tajemnicy, dokumencie niejawnym, materiale niejawnym, systemie teleinformatycznym i sieci teleinformatycznej oraz o służbach ochrony państwa, należy przez to rozumieć pojęcia zdefiniowane w art. 2 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. nr 11, poz. 95 z późn. zm.), zwanej dalej Ustawą.

§ 2

1. Za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w Politechnice Warszawskiej odpowiada Pełnomocnik Rektora ds. Ochrony Informacji Niejawnych, zwany dalej Pełnomocnikiem.
2. Pełnomocnik inicjuje i opracowuje projekty przedsięwzięć, w tym programy, plany i przepisy wewnętrzne, mające na celu poprawę stanu ochrony informacji niejawnych w Uczelni oraz dokonuje oceny tego stanu i przedkłada Rektorowi wynikające z tej oceny okresowe raporty oraz propozycje i wnioski w sprawach organizacyjnych, technicznych, formalno prawnych i finansowych.
3. W razie wprowadzenia stanu nadzwyczajnego, Pełnomocnik ma prawo żądać od jednostek i komórek organizacyjnych oraz pracowników Uczelni udzielenia natychmiastowej pomocy.
4. Pełnomocnik opracowuje plan postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową w razie wprowadzenia stanu nadzwyczajnego.
5. W przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne” lub wyższą, Pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności naruszenia oraz informuje właściwy organ służby ochrony państwa.

§ 3

1. Informacje niejawne mogą być udostępniane wyłącznie pracownikowi dającemu rękojmię zachowania tajemnicy, potwierdzoną wydaniem - po odbyciu przeszkolenia w zakresie ochrony informacji - odpowiedniego poświadczenia bezpieczeństwa, tylko w zakresie niezbędnym do wykonywania pracy na zajmowanym stanowisku lub wykonywania innej zleconej pracy.
2. Obowiązkiem każdego pracownika, posiadającego dostęp do informacji niejawnych, jest:

- 1) ściśle przestrzeganie przepisów „Instrukcji Kancelaryjnej Ochrony Informacji Niejawnych w Politechnice Warszawskiej”, zwanej dalej Instrukcją;
 - 2) we wszystkich wątpliwych sprawach kontaktowanie się z Pełnomocnikiem;
 - 3) w trakcie oraz po ustaniu stosunku pracy nie rozpowszechnianie wiadomości stanowiących tajemnicę służbową, poznanych w czasie wykonywania zadań.
3. Osoba, która stwierdziła fakt ujawnienia lub innego naruszenia tajemnicy państwowej i służbowej w Politechnice Warszawskiej, zobowiązana jest poinformować o tym swojego przełożonego, a ten - Pełnomocnika.
 4. Osoba winna naruszenia lub ujawnienia tajemnicy państwowej bądź służbowej, a także naruszenia przepisów Instrukcji, ponosi odpowiedzialność karną lub dyscyplinarną.
 5. Naruszeniem Instrukcji jest zaniechanie właściwego działania lub działanie niezgodne z przepisami Instrukcji oraz zarządzeniami i poleceniami wydanymi w celu ochrony informacji niejawnych, powodujące lub mogące spowodować ujawnienie tych informacji osobie nieuprawnionej.

§ 4

1. Informacje niejawne (materiały niejawne lub dokumenty niejawne) występujące w Politechnice Warszawskiej podlegają klasyfikacji. Klasyfikacja polega na przyznaniu informacji niejawnej, w sposób wyraźny, właściwej klauzuli tajności:
 - 1) „tajne” – dla tajemnicy państwowej,
 - 2) „poufne” albo „zastrzeżone” – dla tajemnicy służbowej.
2. Osoba upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału, przyznaje mu odpowiednią klauzulę tajności i ponosi odpowiedzialność za jej przyznanie.
3. Uprawnienie do przyznawania, obniżania i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych.
4. Informacje niejawne są chronione odpowiednio do przyznanej klauzuli tajności, tzn.:
 - 1) mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji o danej klauzuli tajności;
 - 2) muszą być wytwarzane, przetwarzane, przekazywane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnianie, odpowiednich dla przyznanej im klauzuli tajności, zgodnie z przepisami określającymi wymagania dla kancelarii tajnych, dotyczące obiegu i środków fizycznej ochrony informacji niejawnych;
 - 3) muszą być chronione, odpowiednio do przyznanej klauzuli tajności, i przy zastosowaniu właściwych środków.

§ 5

Rektor określa, odrębnie dla każdej klauzuli tajności, stanowiska lub rodzaje prac wykonywanych w Uczelni, z którymi może łączyć się dostęp do informacji niejawnych.

§ 6

1. Dopuszczenie do pracy na stanowiskach lub zlecenie prac, o których mowa w § 5, może nastąpić po pozytywnym zakończeniu postępowania sprawdzającego i przeszkoleniu w zakresie ochrony informacji niejawnych, potwierdzonych wydaniem pisemnego poświadczenia bezpieczeństwa i zaświadczenia o odbyciu szkolenia.
2. Przeprowadzenie postępowania sprawdzającego wymaga pisemnej zgody osoby, której ma dotyczyć. Wyrażana jest ona przez złożenie Pełnomocnikowi własnoręcznie wypełnionej i podpisanej ankiety bezpieczeństwa osobowego, której wzór jest załącznikiem do Ustawy.
3. W odniesieniu do stanowisk i prac związanych z dostępem do informacji stanowiących tajemnicę państwową przeprowadzane jest przez odpowiednią służbę ochrony państwa, na wniosek Rektora PW, postępowanie sprawdzające poszerzone.
4. W odniesieniu do stanowisk i prac związanych z dostępem do informacji stanowiących tajemnicę służbową przeprowadzane jest przez Pełnomocnika, na pisemne polecenie Rektora PW, postępowanie sprawdzające zwykłe.

§ 7

Szkolenie poprzedzające dopuszczenie do pracy łączącej się z dostępem do informacji niejawnych w PW przeprowadza Pełnomocnik. W szczególnych przypadkach szkolenie może być przeprowadzone przez uprawnione jednostki zewnętrzne.

§ 8

1. Przetwarzanie informacji niejawnych, stanowiących tajemnicę państwową lub tajemnicę służbową oznaczonych klauzulą „poufne” w urządzeniach systemu teleinformatycznego lub sieci teleinformatycznej (także w pojedynczych komputerach) może odbywać się wyłącznie za pośrednictwem certyfikowanych urządzeń dopuszczonych do eksploatacji na podstawie szczególnych wymagań bezpieczeństwa i powinno odbywać się w strefach bezpieczeństwa.
2. Za funkcjonowanie systemu teleinformatycznego lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci odpowiedzialny jest pracownik pełniący funkcję inspektora bezpieczeństwa teleinformatycznego, wyznaczony przez Rektora.

§ 9

Jednostki organizacyjne Politechniki Warszawskiej starające się o zawarcie umowy lub wykonujące umowę, z której realizacją łączy się dostęp do informacji niejawnych, mają obowiązek ochrony tych informacji; szczegółowe wymagania dotyczące ochrony powinny być określone w umowie przez zamawiającego.