PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA W ELBLĄGU

Załącznik do zarządzenia Nr 24/2011
Rektora PWSZ w Elblągu
z dnia 22 czerwca 2011r.

INSTRUKCJA

przetwarzania informacji niejawnych o klauzuli „zastrzeżone”
w jednostkach organizacyjnych Państwowej Wyższej Szkoły Zawodowej
w Elblągu oraz zakres i warunki stosowania środków bezpieczeństwa
fizycznego w celu ich ochrony

Elbląg 2011

I. POSTANOWIENIA OGÓLNE

1. Niniejsza instrukcja dotyczy sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w jednostkach organizacyjnych Uczelni. Określa zasady ochrony informacji niejawnych, które wymagają ochrony przed nieuprawnionym ujawnieniem oraz zakres stosowania środków ochrony fizycznej informacji niejawnych. Ujednolica czynności oraz metody pracy administracyjnej związane z organizowaniem ochrony informacji niejawnych, ewidencją i obiegiem dokumentów niejawnych.

2. Zasady i organizację ochrony informacji niejawnych regulują[1]:

   1) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228);
   2) ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.);
   3) rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. z 2010 r. Nr 114, poz. 765);
   4) rozporządzenie Prezesa Rady Ministrów z 13 sierpnia 2010 r. w sprawie oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. z 2010 r. Nr 159, poz. 1069);
   5) rozporządzenie Prezesa Rady Ministrów z dn. 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2005 r. Nr 171, poz. 1433);
   6) rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2005 r. Nr 200, poz. 1650 z późn. zm.);
   7) rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie szczegółowego trybu przygotowania i prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych (Dz. U. z 2005 r. Nr 171, poz. 1430);
   8) rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. z 2010 r. Nr 258, poz. 1751);
   9) rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. z 2010 r. Nr 258, poz. 1752);
   10) rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U. z 2010 r. Nr 258, poz. 1750).

[1] Zgodnie z art. 189 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) dotychczasowe akty wykonawcze wydane na podstawie ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.) zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych, nie dłużej jednak niż przez okres 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

3. Użyte w instrukcji określenia oznaczają:

1) państwowa jednostka organizacyjna – PWSZ w Elblągu (zwaną dalej Uczelnią);
2) jednostka organizacyjna – wyodrębnioną jednostkę organizacyjną określoną w Statucie i Regulaminie organizacyjnym Uczelni (instytut, dział, sekretariat, biuro, kancelaria, samodzielne stanowisko pracy);
3) służba ochrony państwa – Agencję Bezpieczeństwa Wewnętrznego (ABW);
4) rękojmia zachowania tajemnicy – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem;
5) informacje niejawne – informacje, stanowiące tajemnice prawnie chronione odpowiednio do nadanej klauzuli tajności, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne;
6) dokument (dokumentacja) – każdą utrwaloną informację niejawną;
7) materiał – dokument lub przedmiot albo dowolną ich część, chronioną jako informację niejawną;
8) przetwarzanie informacji niejawnych – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich *wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie*;
9) klasyfikowanie informacji niejawnych – przyznanie danej informacji w sposób wyraźny, jednej z klauzul tajności;
10) klauzula tajności – oznaczenie dokumentów następującymi wyrazami ich niejawności: „*zastrzeżone*”, „*poufne*”, „*tajne*”, „*ściśle tajne*”;
11) klauzula „zastrzeżone” – informację niejawną, której nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organ władzy publicznej lub inne jednostki organizacyjne zadań w zakresie *obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych RP*;
12) system teleinformatyczny – system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający przetwarzanie informacji niejawnych;
13) akredytacja bezpieczeństwa teleinformatycznego – dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;
14) dokumentacja bezpieczeństwa teleinformatycznego – dokumenty: „Szczególne Wymagania Bezpieczeństwa (SWB)” i „Procedury Bezpiecznej Eksploatacji (PBE)”;
15) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych – skoordynowane działania w zakresie ochrony informacji niejawnych (szacowania ryzyka, ustalanie poziomu zagrożeń, stosowanie środków bezpieczeństwa osobowego, fizycznego, teleinformatycznego);
16) UOIN – ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
17) wykonawca – pracownika Uczelni, niezależnie od zajmowanego stanowiska służbowego, upoważnionego do dostępu do informacji niejawnych o klauzuli „zastrzeżone” i „poufne”;
18) poświadczenie bezpieczeństwa – dokument uprawniający do dostępu do informacji niejawnych o wskazanej w nim odpowiedniej klauzuli tajności, przez okres na jaki zostało wydane.

II. ZASADY I ORGANIZACJA OCHRONY INFORMACJI NIEJAWNYCH

1) Głównym aktem prawnym, który określa zasady i organizację systemu ochrony informacji niejawnych w Polsce jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwana dalej „ustawą", która zastąpiła regulację o tej nazwie z 1999 r.

2) W ustawie określono, miedzy innymi, procedury ochrony fizycznej i teleinformatycznej informacji niejawnych.

3) Warunkiem skutecznej ochrony informacji niejawnych jest stosowanie kilku podstawowych zasad, które są wiążące niezależnie od zmian wprowadzanych w rozwiązaniach szczegółowych. Są to:

   1) zasada udostępniania informacji niejawnych wyłącznie osobom gwarantującym ich ochronę, przed nieuprawnionym ujawnieniem. *Warunkiem wykonywania obowiązków związanych z dostępem do informacji niejawnych jest uzyskanie odpowiedniego poświadczenia bezpieczeństwa (upoważnienia) oraz odbycie przeszkolenia.*

   2) zasada ograniczonego dostępu. *Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku.*

   3) zasada podporządkowania środków ochrony klauzuli informacji. *Środki ochrony fizycznej i zasady bezpieczeństwa obiegu dokumentów muszą być adekwatne do klauzuli tajności informacji.*

   4) zasada kontroli wytwórcy nad sposobem ochrony informacji. *Klauzulę tajności przyznaje osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Bez zgody tej osoby lub jej przełożonego nie można zmienić lub znieść klauzuli.*

   5) zakaz zaniżania lub zawyżania klauzuli tajności.

4. Realizacja zadań nałożonych przez przepisy ustawy w zakresie ochrony informacji, które nie są powszechnie jawne, ma na celu skuteczne zapobieganie ewentualnym przypadkom ich ujawnienia podmiotom do tego nieuprawnionym i eliminowanie wykrytych nieprawidłowości w obszarze bezpieczeństwa informacji.

5. Uwzględniając potrzeby i możliwości realizacyjne przyjęto w Uczelni następujące ustalenia w zakresie bezpieczeństwa osobowego, fizycznego i teleinformatycznego ochrony informacji niejawnych o klauzuli „zastrzeżone":

   1) w rozumieniu przepisów ustawy PWSZ w Elblągu jest uczelnią sporadycznie przyjmującą i przetwarzającą informacje niejawne o niskich klauzulach tajności;

   2) od 2 stycznia 2011 r. w PWSZ przetwarza się informacje niejawne tylko do poziomu „**zastrzeżone**";

3) dostęp do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po pisemnym upoważnieniu przez Rektora, jeżeli nie posiada się poświadczenia bezpieczeństwa oraz po przeszkoleniu w zakresie ochrony informacji niejawnych. Wzory pisemnego upoważnienia Rektora i zaświadczenia o przeszkoleniu przedstawiono w **załącznikach 1** i **2**. Poświadczenia bezpieczeństwa wydane na podstawie ustawy z 22 stycznia 1999 r. o ochronie informacji niejawnych zachowują ważność przez okres, na jaki zostały wydane;

4) upoważnienie do klauzuli „zastrzeżone” wydaje się na okres:

– w konkretnym celu np. wykonanie określonego zadania,
– na czas określony konkretnymi datami np. „od dnia … do dnia …”,
– do odwołania np. „od dnia wydania do odwołania”,
– do czasu wystąpienia określonego wydarzenia np. „na czas zatrudnienia w jo.”;

5) ustalenie okoliczności utraty ważności upoważnienia pozostaje w zakresie uprawnień Rektora. Samo potwierdzenie utraty ważności upoważnienia dokonuje się w formie pisemnej;

6) kierownik przedsiębiorcy przyjmującego zlecenie wykonania prac lub zadań samodzielnie upoważnia podległych pracowników do dostępu do informacji niejawnych o klauzuli „zastrzeżone” w jednostce zlecającej wykonanie umowy, związanej z dostępem do informacji niejawnych o tej klauzuli tajności;

7) podczas spotkań (narad, konferencji, posiedzeń, szkoleń) pisemne upoważnienie wydane przez Rektora stanowi odpowiednią podstawę do zapoznawania się z informacjami niejawnymi o klauzuli „zastrzeżone” przetwarzanymi podczas tego spotkania;

8) kierownik jednostki organizacyjnej (Rektor) ma zapewniony dostęp do klauzuli „zastrzeżone” na mocy ustawy, bez konieczności wydawania odrębnego pisemnego upoważnienia;

9) zgodnie z art. 14 ust.3 pkt 3 ustawy osoba zajmująca stanowisko pełnomocnika ds. ochrony informacji niejawnych (niezależnie od stopnia tajności dokumentów przetwarzanych w jednostce, w której jest on zatrudniony) musi posiadać odpowiednie poświadczenie bezpieczeństwa wydane przez ABW.

6. Zgodnie z art. 48 ust. 1 systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego – odpowiednio do określonych klauzul tajności.

7. W świetle ustawowych uregulowań Rektor udziela akredytacji bezpieczeństwa, na czas do 5 lat, dla komputera przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przez zatwierdzenie dokumentacji bezpieczeństwa teleinformatycznego. Opracowana i zatwierdzona dokumentacja przekazywana jest do określonej jednostki organizacyjnej Agencji Bezpieczeństwa Wewnętrznego (ABW) w celu dokonania stosownych weryfikacji i uzgodnień.

8. W skład zestawu dokumentów bezpieczeństwa teleinformatycznego wchodzą:

1) dokument „Szczególne Wymagania Bezpieczeństwa (SWB)”,

2) dokument „Procedury Bezpiecznej Eksploatacji (PBE)”.

Dokument SWB definiuje zagadnienia bezpieczeństwa informacji dla konkretnego systemu (budowa systemu, zasady działania, eksploatacja). Opracowuje go Ośrodek Informatyki na etapie projektowania. Dokument PBE jest zbiorem procedur, które należy spełnić w celu realizacji bezpieczeństwa informatycznego danego systemu. Dokument ten opracowuje się na podstawie SWB, podczas wdrażania systemu teleinformatycznego.

9. Tworzony system teleinformatyczny powinien być autonomicznym systemem komputerowym (ASK) tzn., że nie może on być połączony z innymi systemami i nie może stanowić sieci informatycznej ani też funkcjonować w wprowadzanej w PWSZ platformie e-Learning. Ma to być Bezpieczne Stanowisko Komputerowe (BSK) przeznaczone do przetwarzania informacji niejawnych o klauzuli, „zastrzeżone” z całej Uczelni.

10. System teleinformatyczny (TI) powinien spełniać, co najmniej minimalne wymagania dotyczące ochrony przetwarzanych w tym systemie informacji przed nieuprawnionym ujawnieniem. Komputer przeznaczony do pracy ze zbiorami niejawnymi oznaczonymi klauzulą „zastrzeżone” powinien być galwanicznie odizolowany od sieci i posiadać odpowiedni, poświadczony „akredytacją”, poziom bezpieczeństwa.

III. ZASADY PRZYJMOWANIA I PRZEKAZYWANIA DOKUMENTÓW OZNACZONYCH KLAUZULĄ TAJNOŚCI „ZASTRZEŻONE”

1. W obiegu dokumentów uczestniczą upoważnieni pracownicy:

   – Kancelarii Ogólnej;
   – Sekretariatu Rektora;
   – Samodzielnego stanowiska pracy ds. ochrony informacji niejawnych.

   Oprócz ww. **jednostek organizacyjnych**, **w zależności od potrzeb**, **uczestniczyć mogą**:

   – Wykonawcy (sporządzający i wykonujący dokumenty niejawne);
   – Archiwum zakładowe.

2. Do obiegu dokumentów oznaczonych klauzulą „zastrzeżone” stosuje się przepisy „Instrukcji kancelaryjnej PWSZ w Elblągu” (wprowadzonej do użytku zarz. Rektora Nr 8/2008).

3. Dokumenty zawierające informacje niejawne oznaczone klauzulą „zastrzeżone” przyjmuje, rejestruje i przekazuje pracownikom za pokwitowaniem Kancelaria Ogólna.

4. Do ewidencjonowania przyjmowanych dokumentów służą:

   – Dziennik korespondencji kancelarii – przeznaczony do rejestracji każdego listu poleconego wpływającego lub wysyłanego;
   – Dziennik podawczy sekretariatu – przeznaczony do rejestracji każdego dokumentu (w tym „zastrzeżonego”) wchodzącego, przekazywanego bądź wysyłanego;
   – „Dziennik korespondencji” – przeznaczony wyłącznie do tego rodzaju dokumentów (prowadzony przez pracownika stanowiska ds. ochrony informacji niejawnych)[2].

[2] Zgodnie z § 11 ust. 3 rozp. Rady Ministrów z dn. 1 czerwca 2010 r. w sprawie org. i funkcjonow. kancelarii tajnych (Dz. U. Nr 114, poz. 765) w jedn. org. można prowadzić odrębne dzienniki dla dok. oznacz. różnymi klauzul. tajności.

5. Pracownik Kancelarii Ogólnej nie otwiera bez upoważnienia przesyłek adresowanych „Do rąk własnych”, wpisując do „Dziennika korespondencji” dane z opakowania. Na opakowaniu przesyłki wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę w „Dzienniku korespondencji”. Następnie przesyłkę przekazuje się bezpośrednio adresatowi lub w razie jego nieobecności – osobie przez niego wyznaczonej do odbioru – za pokwitowaniem w „Dzienniku korespondencji”.

6. Każdy rok kalendarzowy stanowi oddzielny cykl ewidencjonowania dokumentów, rozpoczynany z dniem 1 stycznia i zamykany z dniem 31 grudnia.

7. Do obowiązków upoważnionych pracowników należy, w szczególności:

   1) **w Kancelarii Ogólnej**:

   – wykonywanie obowiązków zgodnie z „Instrukcją kancelaryjną”;
   – ewidencjonowanie w dokumentacji kancelaryjnej, wchodzących i wychodzących, przesyłek poleconych – spisując potrzebne dane z kopert bez ich otwierania;
   – otwieranie wpływów oznaczonych klauzulą „zastrzeżone” tylko wtedy, gdy adresowane są do PWSZ w Elblągu bez określonego adresata;
   – terminowe przekazywanie adresatom otrzymanych, bądź dekretowanych pism (materiałów) dotyczących merytorycznych spraw;
   – ewidencjonowanie i niezwłoczne przekazywanie Sekretariatowi Rektora informacji wysyłanych z MNiSW do Uczelni, pocztą elektroniczną (e-mail). W sprawach dotyczących obronności, zarządzania kryzysowego i ochrony informacji niejawnych powiadamianie, przez techniczne środki łączności, Pełnomocnika do spraw ochrony informacji niejawnych o treści otrzymanej informacji.

   2) **w Sekretariacie Rektora**:

   – ewidencjonowanie dokumentów niejawnych otrzymanych z Kancelarii Ogólnej;
   – przekazywanie materiałów do decyzji Rektora, a następnie zgodnie z zamieszczoną dekretacją – przekazywanie dokumentów wykonawcom (adresatom);
   – przechowywanie wykorzystywanych lub opracowywanych dokumentów do czasu otrzymania decyzji o ich przekazaniu do Samodzielnego stanowiska pracy ds. ochrony informacji niejawnych, zniszczeniu lub przekazaniu do archiwum;
   – prowadzenie bieżącej kontroli stanu faktycznego posiadanych dokumentów i przesyłek niejawnych.

   3) **w Samodzielnym stanowisku pracy ds**. **ochrony informacji niejawnych**:

   – potwierdzanie (kwitowanie) w urządzeniach ewidencyjnych Sekretariatu Rektora lub Kancelarii Ogólnej faktu otrzymania dokumentu niejawnego, zgodnie z dekretacją Rektora (Prorektora, Kanclerza);
   – ewidencjonowanie (rejestrowanie) otrzymanego dokumentu w Dzienniku korespondencji dokumentów oznaczonych klauzulą „zastrzeżone”;
   – kwalifikowanie otrzymanych materiałów niejawnych do przetwarzania na stanowisku pracy poprzez grupowanie i segregowanie ich w teczkach spraw;
   – odmawianie wydania lub udostępniania materiału niejawnego osobie nieuprawnionej do informacji niejawnych.

   4) **u wykonawców**:

   – potwierdzanie (kwitowanie) w Dzienniku korespondencji kancelarii/sekretariatu dokumentów zgodnie z dekretacją Rektora, Prorektora, Kanclerza;

- ewidencjonowanie w spisie spraw i umieszczanie w teczkach aktowych przekazanych do przetwarzania, na stanowisku pracy, dokumentów niejawnych;
- zabezpieczenie posiadanych, na czasowym przechowaniu, dokumentów niejawnych przed wglądem osób nie mających stosownego poświadczenia bezpieczeństwa lub upoważnienia.

5) **w Archiwum zakładowym**:

- ewidencjonowanie dokumentów niejawnych przekazanych do przechowania.

IV. PRZETWARZANIE INFORMACJI NIEJAWNYCH I ZASADY OBIEGU DOKUMENTÓW WYCHODZĄCYCH O KLAUZULI „ZASTRZEŻONE”

1. Przetwarzaniem informacji niejawnych – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przekazywanie lub udostępnianie.

2. Informacje niejawne klasyfikuje się w oparciu o zawartą w nich treść i definicje klauzul tajności nadawanych przez osobę, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

3. Wytwarzanie dokumentów niejawnych polega na ich sporządzaniu i wykonywaniu.

4. Dokumenty niejawne mogą być wykonywane na sprzęcie komputerowym dopuszczonym przez właściwą jednostkę organizacyjną ABW, na maszynie do pisania odpowiedniego typu lub odręcznie w trybie i na zasadach określonych w przepisach dotyczących ochrony informacji niejawnych.

5. Podczas sporządzania (opracowywania), wykonywania i obiegu dokumentów wychodzących o klauzuli „zastrzeżone” należy przestrzegać następujących zasad i ustaleń:

   1) dokumenty zawierające niejawności treści informacji, których nieuprawnione ujawnienie *może mieć szkodliwy wpływ* na wykonywanie zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych RP, oznacza się klauzulą „**zastrzeżone**” oraz literą „**Z**” przed numerem rejestracyjnym;

   2) pracownik opracowujący projekt dokumentu kwalifikuje go i oznacza wstępną klauzulą tajności „zastrzeżone”. Ostateczna decyzja w tym zakresie należy do osoby podpisującej dokument lub oznaczenia innego niż dokument materiału;

   3) projekt dokumentu niejawnego może być opracowany w brulionie lub na pojedynczych zszytych (spiętych) i ponumerowanych kartkach. Brudnopisy projektów dokumentów należy po utrwaleniu w formie pisemnej lub elektronicznej zniszczyć w taki sposób, aby nie można było odtworzyć ich treści;

   4) dokumenty niejawne o klauzuli „zastrzeżone” mogą drukować (przepisywać, kopiować) wyłącznie osoby upoważnione, w warunkach gwarantujących ochronę zawartych w nich informacji;

5) oznaczenie materiału zawierającego informacje zastrzeżone polega na wyraźnym umieszczeniu na nim, w pełnym brzmieniu, przyznanej klauzuli tajności „**zastrzeżone**". Podstawą do nadania materiałom klauzuli tajności jest nie wykaz informacji niejawnych, a definicja danej klauzuli tajności;

6) materiały zawierające informacje niejawne z przyznaną klauzulą tajności „zastrzeżone", utrwalone w formie pisemnej, oznacza się według wzoru podanego w **załącznikach 3** i 4[3]. W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dyspozycje dla adresata dotyczące: udzielania informacji, kopiowania, odpisów, wypisów, wyciągów. Na załącznikach do pism, na pierwszej stronie w prawym górnym rogu umieszcza się napis: „Załącznik nr … do pisma nr … z dnia …";

7) opracowane, przez wykonawców, dokumenty o klauzuli „zastrzeżone" przeznaczone do przekazania (wysłania) powinny być zarejestrowane w Dzienniku korespondencji jednostki organizacyjnej sporządzającej i wykonującej określony dokument;

8) przeznaczony do wysłania dokument, przekazuje się do Kancelarii Ogólnej w dwóch opakowaniach (kopertach), z których zewnętrzne opatrzone jest tylko adresem odbiorcy i nadawcy. Natomiast wewnętrzne posiada ponadto oznakowanie klauzulą „zastrzeżone" oraz literą „Z" przed numerem rejestracyjnym. Kancelaria Ogólna rejestruje przesyłkę w Dzienniku korespondencji według danych z opakowania zewnętrznego i przekazuje do wysłania za pośrednictwem **poczty** na zasadach obowiązujących w odniesieniu do przesyłek **poleconych** lub **wartościowych**, stosownie do zalecenia nadawcy. W przypadku konieczności dostarczenia dokumentu adresatowi z pominięciem urzędu pocztowego, pokwitowanie odbioru powinno być dokonane w „**wykazie przesyłek nadanych**";

9) dokumenty opracowane na użytek wewnętrzny rejestruje się jako pisma własne tylko w Dzienniku korespondencji danej jednostki organizacyjnej Uczelni;

10) kopie wysyłanych (przekazywanych) dokumentów niejawnych przechowują wykonawcy, po pokwitowaniu ich w Dzienniku korespondencji.

V. POSTANOWIENIA KOŃCOWE

1. W PWSZ stosuje się środki bezpieczeństwa fizycznego w szczególności chroniące przed: *kradzieżą lub zniszczeniem materiału, próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne, nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień*. W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „zastrzeżone" uwzględnia się następujące wskazania:

   1) dobór środków bezpieczeństwa fizycznego uzależniono od faktycznego poziomu zagrożeń;

   2) określając poziom zagrożeń uwzględniono klauzulę tajności, liczbę dokumentów pozostających w dyspozycji Uczelni, lokalizację pomieszczeń (w których będą

[3] Sposób oznaczania materiałów (dokumentów, pism) zawierających informacje niejawne utrwalone w formie pisemnej i elektronicznej określono w rozp. Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. (Dz. U. Nr 159, poz. 1069).

przetwarzane informacje niejawne), liczbę osób mających dostęp do informacji niejawnych;

3) ustalono, że podstawową ewidencję (rejestrowanie) dokumentów i materiałów o klauzuli „zastrzeżone” prowadzą: Kancelaria Ogólna, Sekretariat Rektora, Samodzielne stanowisko ds. ochrony informacji niejawnych;

4) organizacja pracy ww. jednostek organizacyjnych zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „zastrzeżone” pozostający w dyspozycji Uczelni oraz kto z tym materiałem się zapoznał;

5) system ochrony informacji niejawnych w Uczelni realizuje się przez ochronę fizyczną przy wykorzystaniu technicznych środków ją wspomagających;

6) ochronę fizyczną (czynną) realizują inspektorzy ochrony mienia w portierniach i pracownicy agencji ochrony;

7) ochrona czynna informacji niejawnych jest wspomagana ochroną bierną (ogrodzenia, bramy, szlabany, bramki) i środkami technicznymi (wewnętrzne systemy wizyjne i alarmowo-pożarowe, łączność telefoniczna przewodowa i komórkowa, oświetlenie obiektów (zewnętrzne, wewnętrzne, awaryjne), zabezpieczenia mechaniczne pomieszczeń (wzmocnienia drzwi, szafy metalowe, zamki, rolety);

8) w budynkach Uczelni wydzielono ciągi administracyjne i drogi ewakuacyjne – będące pod stałym nadzorem wizyjnym pracowników portierni;

9) strefę ochronną przetwarzanych informacji niejawnych stanowi płn. zach. część budynku DS 2 z pomieszczeniem służbowym, wyposażeniem i wszystkimi technicznymi zabezpieczeniami, Pełnomocnika ds. ochrony informacji niejawnych;

10) wejście do strefy, wym. w pkt. 9, nie jest równoznaczne z bezpośrednim dostępem do dokumentów rejestrowanych i przechowywanych w tym pomieszczeniu. Dostęp do informacji niejawnych uzyskują wyłącznie osoby dające rękojmię zachowania tajemnicy i znające zasady postępowania oraz odpowiedzialności za naruszenie przepisów w zakresie ochrony informacji.

2. Ujawnienie informacji niejawnych o klauzuli „zastrzeżone” osobom nieupoważnionym grozi sankcjami prawnymi (administracyjnymi i służbowymi).

3. Dokumenty o klauzuli „zastrzeżone” mogą być przechowywane w szafach (biurkach) drewnianych, zamykanych w sposób uniemożliwiający zapoznanie się z ich treścią, przez osoby nieupoważnione. Po zakończeniu pracy szafy (biurka) powinny być zamknięte na klucz.

4. Dokumenty, o których mowa w pkt. 3 po ich załatwieniu kompletuje się w teczki spraw i przechowuje w jednostce organizacyjnej, która sprawy te prowadzi. W „Dzienniku korespondencji” odnotowuje się numer teczki, do której dokument włączono.

5. Brudnopisy projektów dokumentów niejawnych należy po wykonaniu w czystopisie (na sprzęcie komputerowym, na maszynie lub odręcznie) zniszczyć w taki sposób, aby nie można było odtworzyć ich treści.

6. Dokumenty wykorzystane, wytworzone na potrzeby wewnętrzne, niemające wartości archiwalnej oraz inne dokumenty pomocnicze mogą być na bieżąco niszczone. Fakt zniszczenia dokumentu odnotowuje się w „Dzienniku korespondencji” w rubryce „Uwagi” i potwierdza podpisem pracownika prowadzącego ewidencję.

7. Kontrolę i nadzór w zakresie przestrzegania przepisów o ochronie informacji niejawnych w Uczelni sprawuje pełnomocnik ds. ochrony informacji niejawnych zgodnie z kompetencją ogólną i zadaniami szczególnymi wynikającymi z przepisów ustawy;

8. Za ochronę informacji niejawnych o klauzuli „zastrzeżone” przetwarzanych w jednostce organizacyjnej odpowiada dyrektor/kierownik (równorzędny).

9. Informacje niejawne o klauzuli „zastrzeżone” podlegają ochronie w sposób określony instrukcją, bez sztywnego okresu ochrony, na zasadach określonych w ustawie.

10. Zasady brakowania i archiwizowania dokumentów regulują przepisy Instrukcji kancelaryjnej i Archiwum zakładowego PWSZ.

11. Pracownik odchodzący ze stanowiska związanego z dostępem do informacji niejawnych o klauzuli „zastrzeżone” podlega rozliczeniu potwierdzanym podpisami pracownika Kancelarii/Sekretariatu i kierownika danej jednostki organizacyjnej na karcie obiegowej – po zdaniu dokumentów niejawnych.

12. Wszystkie osoby mające dostęp do informacji niejawnych o klauzuli „zastrzeżone” podlegają szkoleniu w zakresie ochrony tych informacji nie rzadziej niż co 5 lat. Szkolenie organizuje i prowadzi pełnomocnik ochrony informacji niejawnych. Pełnomocnik ochrony może odstąpić od przeprowadzenia szkolenia, jeżeli osoba podejmująca pracę albo wykonywanie czynności zleconych przedstawi aktualne zaświadczenie o odbyciu takiego szkolenia. Uczestnik szkolenia po jego zakończeniu otrzymuje odpowiednie zaświadczenie (zał. 2).

13. W przepisach ustawy nie określono wymogów specjalnych dotyczących ewidencji oraz obiegu informacji niejawnych o klauzuli „zastrzeżone”. Zgodnie z art. 43 ust. 5 UOIN Kierownik jednostki organizacyjnej zatwierdzając, opracowaną przez pełnomocnika ochrony, instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony – określa szczegółowe wymogi w tej sprawie.

14. Ustalenia i rekomendacje niniejszej Instrukcji są wiążące dla jednostek organizacyjnych i wykonawców przetwarzających informacje niejawne w Uczelni.

15. Obowiązek ochrony informacji niejawnych spoczywa na każdym, kto w posiadanie takich informacji wszedł, niezależnie czy nastąpiło to w sposób uprawniony czy też przypadkowy.

16. Ochronie określonej przepisami ustawy podlegają tylko takie informacje, których ujawnienie przyniosłoby szkody interesom państwa, gdyż sposób postępowania z informacjami dotyczącymi pracowników i jednostek organizacyjnych, a objętych tajemnicami różnego rodzaju, jest przewidziany w innych ustawach normujących te tajemnice.

17. W Uczelni przetwarza się tylko i wyłącznie informacje niejawne oznaczane klauzulą „zastrzeżone”. W przypadku gdyby zaistniała potrzeba przetwarzania materiałów niejawnych oznaczonych maksymalnie klauzulą „poufne”, to funkcję kancelarii

niejawnej spełniać będzie „Samodzielne stanowisko pracy ds. ochrony informacji niejawnych” (art. 43 ust. 2 i art. 44 ustawy).

Załączniki do Instrukcji:

1. Wzór upoważnienia do informacji niejawnych o klauzuli „zastrzeżone”
2. Wzór zaświadczenia stwierdzającego odbycie szkolenia w zakresie ochrony informacji niejawnych
3. Wzór oznaczenia dokumentu o klauzuli „zastrzeżone”
4. Wzór oznaczenia załącznika do dokumentu o klauzuli „zastrzeżone”