

Załącznik do zarządzenia
Wojewody Pomorskiego
z dnia 14 października 2026 r.

Instrukcja w sprawie sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą "zastrzeżone" oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Pomorskim Urzędzie Wojewódzkim w Gdańsku

Podstawy prawne

§ 1. 1. Niniejsza Instrukcja, zwana dalej "Instrukcją", określa sposób i tryb przetwarzania informacji niejawnych o klauzuli "zastrzeżone" oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Pomorskim Urzędzie Wojewódzkim w Gdańsku, zwanym dalej "Urzędem".

2. Instrukcja uwzględnia przepisy art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209), zwanej dalej "ustawą" oraz przepisy niżej wymienionych aktów wykonawczych wydanych na jej podstawie:

- 1) rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. nr 271 poz. 1603);
- 2) rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. z 2017 r. poz. 1558);
- 3) rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r. nr 288 poz. 1692);
- 4) rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r. poz. 683 oraz z 2017 r. poz. 522).
- 5) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r. nr 159, poz. 948).

Cel i zakres Instrukcji

§ 2. 1. Instrukcja określa tryb i sposób postępowania z informacjami niejawnymi o klauzuli „zastrzeżone” oraz zasady ochrony i obiegu tych informacji w Pomorskim Urzędzie Wojewódzkim w Gdańsku, a w szczególności:

- 1) warunki dostępu do tych informacji i nadzór nad ich bezpieczeństwem przed nieuprawnionym ujawnieniem;
- 2) zasady ich klasyfikacji, wytwarzania, oznaczania, przyjmowania, przewożenia, ewidencjonowania, przetwarzania, przechowywania, wysyłania, doręczania, przeglądu, niszczenia, znoszenia klauzul tajności i archiwizacji;
- 3) zasady ochrony informacji niejawnych podczas narad, spotkań i szkoleń;
- 4) odpowiedzialność za naruszenie przepisów dotyczących ich ochrony.

2. Instrukcja dotyczy pracowników Urzędu realizujących zadania służbowe, których wykonanie wymaga dostępu do informacji niejawnych o klauzuli „zastrzeżone”.

3. Dyrektorzy Wydziałów, w których przetwarzane są dokumenty niejawne, zapewniają stosowanie niniejszej instrukcji w zakresie ochrony informacji niejawnych o klauzuli „zastrzeżone” przez pracowników kierowanego wydziału.

§ 3. Użyte w Instrukcji określenia oznaczają:

- 1) urząd – Pomorski Urząd Wojewódzki w Gdańsku;
- 2) wojewoda – Wojewodę Pomorskiego;
- 3) kierownik jednostki organizacyjnej – wojewoda;
- 4) wydział – wydział, biuro oraz zespół wchodzący w skład urzędu;
- 5) dyrektor wydziału – kierujący wydziałem, biurem oraz kierujący zespołem wchodzącym w skład urzędu;
- 6) oddział zamiejskowy wydziału – należy przez to rozumieć komórki organizacyjne delegatury realizujące wszystkie lub część zadań wydziałów;
- 7) pełnomocnik ochrony – pełnomocnik wojewody ds. ochrony informacji niejawnych;
- 8) Pion Ochrony – wyodrębniona komórka organizacyjna Urzędu, którą stanowi Zespół ds. Ochrony Informacji Niejawnych zwana dalej „ZOIN”;
- 9) Kancelaria Tajna – wyodrębniona komórka organizacyjna w ZOIN,
- 10) Strefa ochronna III – pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób,
- 11) Strefa ochronna II – pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji,
- 12) informacja niejawna – oznacza informację, której nieuprawnione ujawnienie (także w trakcie jej opracowywania oraz niezależnie od formy i sposobu jej wyrażania) spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne;
- 13) dokument niejawny – każda utrwalona w formie papierowej lub elektronicznej informacja niejawna;
- 14) materiał niejawny – fizyczny nośnik informacji, dokument lub przedmiot albo dowolna ich część, chroniony jako informacja niejawna;

- 15) dekreteacja – pisemna dyspozycja kierownika jednostki lub innej upoważnionej osoby, wyrażona na dokumencie niejawnym, wskazująca jego odbiorcę oraz dalszy sposób postępowania z dokumentem;
- 16) przetwarzanie informacji niejawnych – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, przechowywanie, przekazywanie, udostępnianie itp.;
- 17) pracownik – osoba zatrudniona w urzędzie na podstawie umowy o pracę, zlecenia, mianowania, powołania;
- 18) wykonawca dokumentu niejawnego – pracownik posiadający poświadczenie bezpieczeństwa do dostępu do informacji niejawnych, a w razie jego braku pisemne upoważnienie kierownika jednostki organizacyjnej do dostępu do informacji niejawnych o klauzuli „zastrzeżone”;
- 19) dokumentacja ewidencyjna – dzienniki służące do rejestracji materiałów niejawnych o klauzuli „zastrzeżone”;
- 20) przesyłka niejawna – materiały w postaci odpowiednio zabezpieczonych, opisanych, zaadresowanych i oznaczonych paczek i listów;
- 21) Karta zapoznania – karta zapoznania z dokumentem niejawnym to dokument ewidencyjny służący do rejestrowania każdej osoby, która czyta lub przegląda materiały niejawne. Jej wzór określa odpowiednie rozporządzenie Rady Ministrów. Wzór karty zapoznania stanowi załącznik Nr 5 do Instrukcji;
- 22) CATEL – system bezpiecznej łączności rządowej opracowany przez Agencję Bezpieczeństwa Wewnętrznego, przeznaczony do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, „Restreint UE/EU Restricted”, „NATO Restricted”;
- 23) SKR-Z – system bezpiecznej łączności rządowej opracowany przez NASK-PIB, przeznaczony do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, „Restreint UE/EU Restricted”, „NATO Restricted”;
- 24) STI-PUW – akredytowany system teleinformatyczny Pomorskiego Urzędu Wojewódzkiego w Gdańsku umożliwiający przetwarzanie informacji niejawnych o klauzuli „zastrzeżone”, „NATO Restricted”, „poufne”;
- 25) SWB – Szczególne Wymagania Bezpieczeństwa, dokument opisujący system teleinformatyczny przetwarzający informacje niejawne oraz zastosowane w nim środki ochrony.
- 26) PBE – Procedury Bezpiecznej Eksploatacji, to dokument zawierający szczegółowy wykaz czynności wraz z dokładnym opisem sposobu ich wykonania, które powinny być realizowane przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie teleinformatycznym;
- 27) informatycznym nośniku danych – materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
- 28) SKD – System Kontroli Dostępu, to elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania

dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia.

Tryb i sposób postępowania z materiałami niejawnymi oznaczonymi klauzulą „zastrzeżone”

§ 4. 1. Materiały niejawne oznaczone klauzulą „zastrzeżone” przechowuje się w pomieszczeniach Zespołu ds. Ochrony Informacji Niejawnych oraz wyznaczonych pomieszczeniach Wydziału Bezpieczeństwa i Zarządzania Kryzysowego, Wydziału Spraw Cudzoziemców, Oddziału Zamiejskowego Wydziału Infrastruktury, Wydziału Spraw Cudzoziemców, Biura Obsługi Delegatury, Wydziału Spraw Obywatelskich.

2. Informacje niejawne o klauzuli „zastrzeżone” przetwarza się jedynie w pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu i przechowuje się w szafie metalowej lub zamkniętym na klucz meblu biurowym.

3. System kontroli dostępu (SKD) obejmuje elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia.

4. Dyrektorzy komórek organizacyjnych, w których przetwarzane są dokumenty niejawne, wyznaczają pomieszczenia, o których mowa w § 4. ust. 2 i 3, gwarantując zastosowanie rozwiązań organizacyjnych zapewniających identyfikację osób przebywających w tym pomieszczeniu i że dostęp do tego pomieszczenia uzyskać mogą wyłącznie osoby uprawnione.

5. Dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne określa się poziom zagrożeń, w celu doboru adekwatnych środków bezpieczeństwa fizycznego związanych z utratą poufności, integralności lub dostępności informacji niejawnych.

6. Dokumentów i materiałów „zastrzeżonych” nie przechowuje się razem z dokumentami jawnymi, chyba że stanowią integralną część dotyczącą danej sprawy.

7. Szczegółowe zasady przechowywania dokumentów i materiałów „zastrzeżonych” w postaci cyfrowej w systemach teleinformatycznych reguluje zatwierdzona przez Agencję Bezpieczeństwa Wewnętrznego dokumentacja Szczególnych Wymagań Bezpieczeństwa Teleinformatycznego, zwana dalej „SWB”.

§ 5. 1. Po zakończeniu dnia pracy pracownicy wydziałów wskazanych w § 4 ust. 1 wychodzący z pomieszczenia, w którym przechowywane są informacje niejawne o klauzuli „zastrzeżone”, zobowiązani są do zabezpieczenia dokumentów w odpowiednich szafach zamykanych na klucz oraz zamknięcia drzwi pomieszczenia

na klucz, oraz zdania klucza do depozytora kluczy lub portierni Urzędu, zgodnie z przyjętą gospodarką kluczami w Urzędzie.

2. Zabrania się wnoszenia kluczy od pomieszczeń i urządzeń w których przechowywane są materiały niejawne poza teren Pomorskiego Urzędu Wojewódzkiego w Gdańsku.

§ 6. 1. Materiały i dokumenty niejawne oznaczone klauzulą „zastrzeżone” mogą być przetwarzane wyłącznie przez pracownika posiadającego dostęp do tych informacji. Wzór Wniosku o Upoważnienie do przetwarzania dokumentów niejawnych o klauzuli „zastrzeżone” stanowi załącznik Nr 4 do Instrukcji.

2. Materiały i dokumenty niejawne o klauzuli „zastrzeżone” mogą być udostępnione osobom, które spełniają następujące warunki:

- 1) posiadają ważne poświadczenie bezpieczeństwa a w razie jego braku pisemne upoważnienie wydane przez wojewodę, zgodnie z art. 21 ust. 4 ustawy, którego wzór określa załącznik Nr 1 do Instrukcji;
- 2) odbyły szkolenie w zakresie ochrony informacji niejawnych;
- 3) zajmują stanowisko związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone” i realizują zadania, które wymagają dostępu do tych informacji – zwane dalej „osobami uprawnionymi”.

3. Dyrektor komórki organizacyjnej, w których przetwarzane są dokumenty niejawne, wyznacza pracowników, którzy mają mieć dostęp do informacji niejawnych, w tym pracowników sekretariatu, spełniających warunki wskazane w ust. 2 pkt 1 i 2, odpowiedzialnych za rejestrowanie, przetwarzanie i przechowywanie informacji niejawnych o klauzuli „zastrzeżone” leżących w dyspozycji wydziału.

4. Dyrektorzy komórek organizacyjnych, w których przetwarzane są dokumenty niejawne, zobowiązani są do zgłaszania pełnomocnikowi ochrony zatrudnienie, zwolnienie lub przeniesienie na stanowisko pracownika, którego zakres obowiązków wymaga dostępu do informacji niejawnych o klauzuli „zastrzeżone”.

5. Zadanie przetwarzania informacji niejawnych, w tym rejestrowanie dokumentów „zastrzeżonych”, muszą być ujęte w zakresie obowiązków, odpowiedzialności i uprawnień pracowników wyznaczonych do ich wykonania.

6. W przypadku zmiany osoby, o której mowa w ust. 3 i 5, w wyniku zmiany zakresu obowiązków lub rozwiązania stosunku pracy, sporządza się protokół przekazania dokumentacji ewidencyjnej, materiałów i dokumentów niejawnych o klauzuli „zastrzeżone” osobie wyznaczonej przez dyrektora wydziału, spełniającej warunki ust. 2 pkt 1 i 2, którego wzór stanowi załącznik Nr 2 do Instrukcji.

7. W sytuacji braku wyznaczenia osoby uprawnionej, dyrektor wydziału pobiera za pokwitowaniem, w protokole wymienionym w ust. 6, dokumenty „zastrzeżone”.

8. W przypadku czasowej nieobecności osoby, o której mowa w ust. 3 dopuszcza się przekazania dokumentacji „zastrzeżonej” innej osobie wyznaczonej przez dyrektora wydziału spełniającej warunki określone w ust. 2

9. Protokół wymieniony w ust. 6 sporządzany jest w 2 egzemplarzach. Egzemplarz pierwszy przechowywany jest w wydziale, egzemplarz drugi przekazuje się do kierownika Kancelarii Tajnej Urzędu.

10. W razie likwidacji lub podziału wydziału, ust. 5, 6 i 8 stosuje się odpowiednio.

§ 7. Wobec stażystów, którzy w trakcie odbywania stażu mieliby styczność i dostęp do informacji niejawnych o klauzuli „zastrzeżone”, musi zostać spełniony zapis § 6 ust. 1 - 4 Instrukcji.

Klasyfikowanie, nadawanie, zmiana lub zniesienie klauzuli „zastrzeżone”

§ 8. Informacjom niejawnym nadaje się klauzulę "zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy 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 Rzeczypospolitej Polskiej.

§ 9. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

§ 10. 1. Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności. Osoba, o której mowa w § 9 może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

2. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, o której mowa § 9, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony, o których mowa § 8.

3. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców materiału niejawnego. Odbiorcy materiału, którzy

przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności.

4. Zgodę, o której mowa w ust. 2 udziela się w odrębnym dokumencie podlegającym rejestracji i przechowywaniu. Dopuszcza się także wyrażenie zgody przez zamieszczenie stosownej adnotacji bezpośrednio na dokumencie papierowym, a w przypadku dokumentu elektronicznego – w jego metryce.

5. Skreśleń i adnotacji umieszczanych w celu zmiany klauzuli tajności mogą dokonywać wyłącznie osoby uprawnione, o których mowa w § 6 ust. 1 - 2.

6. Szczegółowe zasady nadawania, zmiany lub zniesienia klauzuli tajności, jak również dokumentowania tych czynności określa rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.

Przyjmowanie i rejestrowanie dokumentów niejawnych o klauzuli „zastrzeżone”

§ 11. 1. Korespondencja niejawna o klauzuli „zastrzeżone” może wpływać do Urzędu za pośrednictwem operatorów pocztowych, przesyłek kurierskich lub być dostarczona osobiście przez nadawcę korespondencji.

2. Z uwagi na funkcjonowanie w Urzędzie systemu Elektronicznego Zarządzania Dokumentacją, dalej „EZD”, stanowiącego podstawowy sposób dokumentowania przebiegu załatwiania spraw oraz wykonywania czynności kancelaryjnych do przyjmowania i rejestrowania korespondencji niejawnej stosuje się zapisy § 40 ust. 1, 3 i ust. 8 i § 41 „Szczegółowych zasad zarządzania dokumentacją w Pomorskim Urzędzie Wojewódzkim w Gdańsku” stanowiącą załącznik Nr 1 do Zarządzenia Wojewody Pomorskiego z dnia 10 stycznia 2024 r. „w sprawie ustanowienia systemu teleinformatycznego do elektronicznego zarządzania dokumentacją jako podstawowego sposobu dokumentowania przebiegu załatwiania spraw i wykonywania czynności kancelaryjnych, zasad użytkowania systemu EZD oraz powołania Zespołu ds. obsługi systemu EZD w Pomorskim Urzędzie Wojewódzkim w Gdańsku”.

3. W przypadku przesyłek wpływających do Urzędu, w tym przesyłek przekazanych na informatycznych nośnikach danych, zawierających kopertę wewnętrzną, na której umieszczono klauzulę tajności i przyjęciu jej w Kancelarii Ogólnej Urzędu, nie podlega ona otwarciu ani skanowaniu w systemie EZD. Zgodnie z postanowieniami § 43 pkt 4 „Szczegółowych zasad [...]”, o których mowa w ust. 2, przesyłka wpływająca jest rejestrowana w systemie EZD i otrzymuje unikatowy identyfikator (RPW). Na kopertę nanoszony jest kod kreskowy z właściwym numerem.

4. W przypadku przesyłek niejawnych dostarczonych osobiście przez nadawców do sekretariatów wydziałów, należy je przekazać niezwłocznie do Zespołu ds. Ochrony Informacji Niejawnych, celem rejestracji.

5. Wszystkie przesyłki niejawne z Kancelarii Ogólnej Urzędu, wraz z nieotwartą kopertą wewnętrzną, przekazuje się do Zespołu do Spraw Ochrony Informacji Niejawnych.

6. W przypadku wpływu do Urzędu pisma niejawnego o klauzuli „zastrzeżone” – z pominięciem Zespołu ds. Ochrony Informacji Niejawnych – lub w przypadku nieposiadania przez osobę odbierającą korespondencję niejawną odpowiedniego upoważnienia bądź poświadczenia bezpieczeństwa, o otrzymaniu takiej korespondencji należy niezwłocznie powiadomić Pełnomocnika ochrony lub kierownika Kancelarii Tajnej.

7. W przypadku otwarcia w Kancelarii Ogólnej Urzędu koperty wewnętrznej oznaczonej klauzulą „zastrzeżone” zamieszcza się adnotację „otwarto w Kancelarii Ogólnej” podając imię i nazwisko pracownika oraz datę. Następnie korespondencję w stanie zamkniętym należy przekazać wg postanowień ust. 5.

8. Przyjmując przesyłkę niejawną, przed jej rejestracją należy sprawdzić:

- 1) prawidłowość adresu;
- 2) całość pieczęci i opakowania;
- 3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy;
- 4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie przesyłek lub w książce doręczeń;
- 5) zgodność liczby stron lub innych jednostek miary materiałów oraz liczby załączników z liczbą oznaczoną na poszczególnych materiałach;

9. W przypadku stwierdzenia w przesyłce braku dokumentów lub załączników, albo innych niezgodności, w tym uszkodzenia przesyłki lub stwierdzenia śladów jej otwarcia, osoba pobierająca dokument sporządza w dwóch egzemplarzach protokół niezgodności lub uszkodzenia przesyłki. Jeden egzemplarz protokołu przekazuje się nadawcy drugi kierownikowi Kancelarii Tajnej Urzędu. Wzór Protokołu uszkodzenia przesyłki stanowi załącznik Nr 8.

10. Fakt sporządzenia protokołu, o którym mowa w ust. 9, odnotowuje się w odpowiednim urzędzeniu ewidencyjnym w rubryce „Informacje uzupełniające/Uwagi”.

§ 12. 1. Informacje niejawne o klauzuli "zastrzeżone", wpływające do Urzędu oraz wytwarzane w Urzędzie, podlegają niezwłocznemu zaewidencjonowaniu w Dzienniku ewidencyjnym prowadzonym przez pracownika wskazanego w § 6 ust. 3. Wzór dziennika ewidencyjnego stanowi załącznik Nr 2 do rozporządzenia Rady

Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.

2. Rejestracji w Dzienniku ewidencyjnym właściwego wydziału podlega również każdy dokument niejawny elektroniczny wpływający do Urzędu za pomocą systemów OPAL, SKR-Z, CATEL.

3. Do ewidencji dokumentów niejawnych oznaczonych klauzulą „zastrzeżone”, prowadzi się urządzenia ewidencyjne:

- 1) Rejestr Dzienników Ewidencji i Teczek (RDEiT) – służy do ewidencjonowania urzędów ewidencyjnych wskazanych poniżej w pkt. 2, 3 i 4 oraz teczek rzeczowych spraw niejawnych (tzw. rejestr matka);
- 2) Dziennik Ewidencyjny (DE) – służy do rejestrowania korespondencji otrzymywanej (wchodzącej), dokumentacji wykonanej i wysyłanej (wychodzącej);
- 3) Dziennik Pracy Systemu Teleinformatycznego (DPST) – w przypadku pracy w systemach teleinformatycznych STI-PUW, SKR-Z, CATEL, wymagane jest prowadzenie DPST, w którym odnotowuje się czynności związane z pracą na systemie. Wzór dziennika stanowi załącznik Nr 6.
- 4) Książka Doręczeń Przesyłek Miejsowych (KDPM) – służy do bezpośredniego przekazywania korespondencji zastrzeżonej adresatom w obiegu wewnętrznym pomiędzy wydziałami, jak również w obiegu zewnętrznym, pomiędzy jednostkami organizacyjnymi w obrębie tej samej miejscowości;
- 5) Rejestr Wydanych Przedmiotów (RWP) – służy do ewidencjonowania wydanych nośników informacji oraz innych przedmiotów.
- 6) Wykaz Przesyłek Nadanych (WPN) – służy jako dowód przekazania przesyłek przewoźnikowi, który usprawnia proces nadawania korespondencji i jest podstawą ewidencji wysyłki dla nadawcy. Wystawiany jest przez nadawcę w dwóch egzemplarzach, a jego przyjęcie i potwierdzenie przez kuriera następuje przez podpis i pieczęć na obu kopiach. Wzór WPN stanowi załącznik Nr 7.

§ 13. 1. Kierownik Kancelarii Tajnej lub inny upoważniony pracownik niezwłocznie rejestruje przyjęte materiały w odpowiednim dzienniku lub rejestrze.

2. Kierownik Kancelarii Tajnej lub inny upoważniony pracownik przekazuje albo udostępnia zarejestrowane materiały adresatowi lub upoważnionej przez adresata osobie, za pokwitowaniem w Dzienniku ewidencyjnym, rubryce nr 14.

3. W Kancelarii Tajnej i w sekretariatach wydziałów nie otwiera się przesyłek oznaczonych „do rąk własnych”. W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu przesyłki; w rubryce „Informacje uzupełniające/Uwagi” odnotowuje się, że przesyłka była oznaczona „do rąk własnych”.

4. Z chwilą zwrotu do kancelarii przesyłki, o której mowa w ust. 3, kierownik Kancelarii Tajnej lub inny upoważniony pracownik uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

5. Wskazany na piśmie adresat dokonuje pisemnej dekretacji wskazując imiennie pracownika odpowiedzialnego merytorycznie za załatwienie sprawy lub kierownika komórki organizacyjnej upoważnionego do wyznaczenia takiego pracownika. Po dokonaniu dekretacji dokument zwracany jest kierownikowi Kancelarii Tajnej.

6. W przypadku konieczności zapoznania się z treścią dokumentu zastrzeżonego przez kilku pracowników tej samej komórki organizacyjnej lub pracowników kilku różnych komórek organizacyjnych Urzędu, konieczne jest rozszerzenie dekretacji oraz wskazane założenie Karty Zapoznania.

7. Kierownik Kancelarii Tajnej odmawia udostępnienia dokumentów osobie niespełniającej warunków dopuszczenia do pracy na stanowisku związanym z dostępem do informacji niejawnych i powiadamia o tym fakcie ostatniego dekretującego, który wskazał taką osobę – w celu zmiany dekretacji. W przypadku odmowy lub braku możliwości zmiany dekretacji, Kierownik Kancelarii Tajnej powiadamia o tym fakcie Pełnomocnika.

8. W razie konieczności przekazania dokumentu innemu pracownikowi należy to zrobić za pośrednictwem Kancelarii Tajnej. Kierownik Kancelarii Tajnej przekazuje dokument zgodnie z dekretacją, po dokonaniu właściwych zapisów w Dzienniku ewidencyjnym. Fakt przekazania dokumentu innemu pracownikowi należy zrobić za pośrednictwem upoważnionego pracownika sekretariatu, który przekazuje dokument zgodnie z dekretacją, po dokonaniu właściwych zapisów w Dzienniku ewidencyjnym.

9. Dokumenty adresowane lub dekretowane na dyrektora komórki organizacyjnej wymienionej w § 4. ust. 1. przekazywane są za Książką Doręczeń Przesyłek Miejsowych do właściwego sekretariatu, celem ich rejestracji.

10. Pracownik, który zapoznał się z treścią dokumentu zastrzeżonego, dokonuje stosownej adnotacji stwierdzającej ten fakt bezpośrednio na dokumencie oraz Dzienniku ewidencyjnym w rubryce nr 14.

11. Za właściwe zabezpieczenie dokumentu zastrzeżonego przed nieuprawnionym dostępem odpowiada pracownik, który pobrał go z Kancelarii Tajnej / sekretariatu komórki wymienionej w § 4. ust. 1.

§ 14. 1. Otrzymałą albo wysyłaną przesyłkę bądź wytworzony dokument lub inny materiał rejestruje się w Dzienniku ewidencji odpowiednio w kolejności otrzymania, wysłania lub wytworzenia.

2. Rejestracji, o których mowa w ust. 1, dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym. Zmian w dzienniku ewidencji dokonuje się kolorem czerwonym, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej zmiany.

3. W przypadku anulowania pozycji w dzienniku ewidencji podaje się powód anulowania, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej anulowania. Anulowania pozycji w Dzienniku ewidencji dokonuje się kolorem czerwonym.

4. Zabrania się wycierania, zamazywania lub nadpisywania zapisów dokonanych w dziennikach ewidencji.

§ 15. 1. Podczas przenoszenia, przekazywania (do dekretacji, do realizacji, do wysyłania) dokumentów i materiałów niejawnych o klauzuli „zastrzeżone”, należy zachować wszelkie środki ostrożności, aby nie dopuścić do ich kradzieży, nieuprawnionego ujawnienia lub zniszczenia.

2. Zabrania się pozostawiania dokumentów i materiałów niejawnych bez nadzoru, przenoszenia ich bez włożenia do nieprzezroczystej teczki, przekazywania ich osobom postronnym i wynoszenia poza Urząd.

Wytwarzanie, oznaczanie, przetwarzanie i przechowywanie dokumentów niejawnych o klauzuli „zastrzeżone”

§ 16. 1. Informacje niejawne o klauzuli „zastrzeżone”, wytworzone w Urzędzie w formie dokumentu, mogą być sporządzane jedynie na komputerach, które uzyskały akredytację bezpieczeństwa teleinformatycznego. Zabrania się wytwarzania oraz przetwarzania dokumentów niejawnych o klauzuli „zastrzeżone” na stacjonarnym sprzęcie komputerowym nieposiadającym akredytacji bezpieczeństwa teleinformatycznego.

2. W wyjątkowych sytuacjach dopuszcza się sporządzenie dokumentu odręcznie lub na maszynie do pisania (bez pamięci).

3. Wytwarzanie i przetwarzanie dokumentów niejawnych o klauzuli „zastrzeżone” może odbywać się wyłącznie na komputerowym stanowisku pracy STI-PUW znajdującym się w Kancelarii Tajnej lub na laptopach systemu niejawnego SKR-Z lub CATEL znajdującymi się w Kancelarii Tajnej oraz wyznaczonych pomieszczeniach WBiZK, zgodnie z zasadami zawartymi w SWB oraz PBE.

4. Dokument wytworzony na komputerowym stanowisku teleinformatycznym STI-PUW, SKR-Z lub CATEL, zarówno w wersji elektronicznej przeznaczonej do

wysłania niejawną pocztą elektroniczną, jak i w postaci wydruku (odwzorowania cyfrowego), należy zarejestrować w Dzienniku ewidencyjnym.

5. Każdą czynność wykonywaną przez użytkownika systemu na komputerowym stanowisku pracy STI-PUW, SKR-Z lub CATEL, należy odnotować w Dzienniku pracy systemu teleinformatycznego (odpowiednio: STI-PUW, SKR-Z lub CATEL). Wzór dziennika pracy systemu teleinformatycznego stanowi załącznik Nr 6 do Instrukcji.

6. Treści dokumentów niejawnych, o klauzuli „zastrzeżone”, wytworzonych lub przetworzonych w postaci dokumentów elektronicznych lub skanów nie umieszcza się w systemie EZD.

§ 17. 1. Dokumenty o klauzuli „zastrzeżone” są wykonywane przez pracownika merytorycznie odpowiedzialnego za jego opracowanie. Praca z dokumentem zastrzeżonym, w tym wykonanie, odbywa się w komórce organizacyjnej, jeśli warunki pracy umożliwiają zapewnienie ochrony przed jego nieuprawnionym ujawnieniem lub zapoznaniem się z nim przez osobę do tego nieuprawnioną.

2. Jeżeli w komórce organizacyjnej Urzędu nie ma wymaganych warunków, wówczas dokument zastrzeżony musi być wykonany w pomieszczeniu Kancelarii Tajnej.

§ 18. Dla ujednolicenia oraz wskazania sposobu oznaczania materiałów i dokumentów niejawnych stosuje się zapisy § 22, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności, przygotowano wzór Szaty graficznej dla pism niejawnych o klauzuli „zastrzeżone”, która stanowi załącznik Nr 3 do niniejszej instrukcji.

§ 19. 1. Na wykonanie kopii, odpisów, wyciągów i tłumaczeń dokumentów i materiałów niejawnych o klauzuli „zastrzeżone” wymagana jest pisemna zgoda osoby, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału lub adresat materiału, o ile nie wprowadzono na materiale ograniczeń dotyczących kopiowania, odpisów, wyciągów tego materiału. Kopii, wydruków, odpisów, wyciągów i tłumaczeń dokonuje osoba wskazana w dekretacji uprawnionego przełożonego.

2. Wykonanie kopii, odpisów, wyciągów, tłumaczeń dokumentów i materiałów niejawnych o klauzuli „zastrzeżone” odbywa się w sposób gwarantujący ich zabezpieczenie przed nieuprawnionym ujawnieniem, na podstawie rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.

3. Zgodę, o której mowa w ust. 1 umieszcza się na ostatniej stronie dokumentu – oryginału.

4. Wytworzenie dokumentu w wyniku kopiowania, wydruku, odpisu, wyciągu albo wypisu, musi zawierać informację o nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument, liczbie egzemplarzy dokumentu wytworzonego, dacie wytworzenia dokumentu, numerze, pod jakim wytworzony dokument został zarejestrowany w Dzienniku ewidencyjnym, które nanosi się na ostatnią stronę oryginału dokumentu lub w jego metryce, w przypadku dokumentu elektronicznego.

5. Na wszystkich stronach dokumentu wytworzonego w wyniku kopiowania (wydruku) umieszcza się napis: „Kopia”, „Wydruk”, „Odpis”, „Wyciąg” albo „Wypis”.

6. Wykonane kopie, wydruki, wyciągi, odpisy, wypis również w formie cyfrowej, podlegają rejestracji w Dzienniku ewidencyjnym dokumentów niejawnych.

§ 20. Zarejestrowane dokumenty niejawne umieszcza się w teczce rzeczowej, założonej zgodnie z klasyfikacją rzeczową wykazu akt (JRWA) i przechowuje oddzielnie od spraw „jawnych”.

§ 21. Każdy wykonany dokument niejawny, nawet w postaci odwzorowania cyfrowego, musi posiadać: klauzulę tajności, numer egzemplarza (egz. pojedynczy), sygnaturę literowo-cyfrową (numer ewidencyjny), numer strony oraz liczbę stron całego dokumentu. Ponadto: nazwę jednostki lub komórki organizacyjnej, nazwę miejscowości i datę podpisania dokumentu, imię i nazwisko lub nazwę stanowiska adresata, stanowisko oraz imię i nazwisko osoby uprawnionej do jego podpisania, imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.

§ 22. 1. Korzystanie z laptopów systemu SKR-Z lub CATEL wymaga, niezależnie od przestrzegania procedur PBE, realizacji zapisów § 8. ust. 3. Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych, tj. „Przetwarzanie informacji niejawnych o klauzuli „zastrzeżone” w systemach teleinformatycznych odbywa się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu, w warunkach uwzględniających wyniki procesu szacowania ryzyka, o którym mowa w art. 49 ust. 1 ustawy”.

2. W pomieszczeniach, w których znajduje się laptop systemu SKR-Z lub CATEL w trakcie opracowywania dokumentów niejawnych mogą przebywać wyłącznie osoby uprawnione.

3. Zabrania się opracowywania w systemie SKR-Z i CATEL informacji niejawnych w obecności osób nieuprawnionych.

4. Zabrania się udostępniania osobom trzecim, nieposiadającym uprawnień do pracy w systemie teleinformatycznym, urządzeń systemu SKR-Z lub CATEL.

§ 23. Użytkownicy systemu SKR-Z / CATEL odpowiadają w szczególności za:

1. Zapewnienie fizycznego bezpieczeństwa powierzonego mu urządzenia dostępowego, tokena Yubikey, karty użytkownika, włączając w to kategoryczny zakaz powierzania urządzeń systemu SKR-Z innym osobom.

2. Poufność danych – w przypadku konieczności zdeponowania telefonu należy wyłączyć go lub zablokować kodem blokady. Niedopuszczalne jest zdeponowanie tokena Yubikey wraz z telefonem w jednym miejscu.

3. Poufność i bezpieczeństwo wykorzystywanych przez siebie PIN-ów oraz haseł wykorzystywanych do uruchamiania urządzeń i realizacji połączeń.

4. Prawidłową, zgodną z zapisami dokumentacji BTI, eksploatację systemu i jego urządzeń.

5. Poufność i bezpieczeństwo przetwarzanych w systemie informacji niejawnych. Praca w trybie niejawnym dopuszczalna jest tylko w warunkach uniemożliwiających dostęp do informacji niejawnych osobom nieupoważnionym.

6. Zgłaszanie poprzez Helpdesk NASK / ABW wszelkich zauważonych nieprawidłowości oraz incydentów, jak również powiadomienia Pełnomocnika ochrony.

7. Poufność danych – w przypadku utraty telefonu, laptopa, tokena Yubikey, podejrzenia ujawnienia lub ujawnienie haseł dostępu lub hasła pomocy technicznej osobom nieuprawnionym, podejrzenia wystąpienia innego niż ww. incydentu – natychmiastowe zgłoszenie wystąpienia incydentu bezpieczeństwa operatorom Helpdesk NASK / ABW, wykorzystując powierzone mu urządzenie dostępowe lub korzystając z dowolnego innego środka łączności, np. telefonu komórkowego, jak również natychmiastowe powiadomienie Pełnomocnika ochrony.

§ 24. 1. Użytkownikiem systemu SKR-Z / CATEL może być osoba posiadająca co najmniej Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone”, „NATO Restricted” i „Restreint UE / EU Restricted” oraz Zaświadczenie stwierdzające odbycie szkolenia z zakresu ochrony informacji niejawnych krajowych i międzynarodowych.

2. Wnioski o dopuszczenie użytkownika do korzystania z systemu, aktualizację lub modyfikację konta użytkownika istniejącego w systemie, rezygnację i wyłączenie dostępu do systemu SKR-Z / CATEL przygotowuje kierownik Kancelarii Tajnej po uprzedniej akceptacji Pełnomocnika ochrony.

3. Zatwierdzony przez kierownika jednostki organizacyjnej wniosek przesyłany jest do NASK za pośrednictwem Zespołu ds. Ochrony Informacji Niejawnych.

4. Kierownik Kancelarii Tajnej prowadzi aktualny wykaz użytkowników systemu SKR-Z / CATEL.

§ 25. 1. Użytkownikom telefonów systemu SKR-Z bezwzględnie zakazuje się:

- 1) Zmiany karty SIM zainstalowanej w terminalu systemu SKR-Z oraz wykorzystywania ww. karty SIM w jakichkolwiek innych urządzeniach.
- 2) Dokonywania jakichkolwiek napraw terminali SKR-Z lub ingerencji w ich oprogramowanie oraz powierzania ww. czynności jakimkolwiek nieautoryzowanym podmiotom zewnętrznym.
- 3) Samowolnego oddawania terminali do naprawy do serwisów zewnętrznych.
- 4) Brakowania i niszczenia/utyliczacji terminali mobilnych.
- 5) Udostępniania osobom trzecim otrzymanego terminala SKR-Z lub tokena Yubikey.
- 6) Pozostawiania niezabezpieczonych kodem PIN lub hasłem terminali bez nadzoru.
- 7) Łączenia w sposób stały telefonu oraz tokena Yubikey np.: poprzez przymocowywanie tokena Yubikey do terminala mobilnego.
- 8) Jakiegokolwiek umieszczania kodu PIN na terminalu mobilnym.

§ 26. 1. Zapisywanie wykonanych na stanowisku teleinformatycznym STI-PUW w Kancelarii Tajnej plików zawierających informacje niejawne o klauzuli „zastrzeżone” na informatyczny nośnik danych odbywa się zgodnie z procedurami PBE i wykonywane jest wyłącznie przez Administratora Systemu Teleinformatycznego na nośnikach (CD-R lub DVD+R) wydawanych i rejestrowanych w Kancelarii Tajnej.

2. Do każdego informatycznego nośnika danych dołączana jest metryka w formie papierowej wykonana przez Administratora Systemu Teleinformatycznego w 2 egzemplarzach. Jeden egzemplarz metryki wysyłany jest wraz z nośnikiem do adresata, drugi pozostaje w aktach sprawy.

3. Informatyczny nośnik danych zawierający informacje niejawne podlega rejestracji w Dzienniku ewidencyjnym.

Wysyłanie i doręczanie dokumentów niejawnych o klauzuli „zastrzeżone”

§ 27. 1. Materiały i dokumenty zawierające informacje niejawne o klauzuli „zastrzeżone” przeznaczone do wysyłki w postaci listów i paczek, nadaje się jako przesyłki „polecone – za zwrotnym potwierdzeniem odbioru”. Pakuje się je w dwie nieprzezroczyste koperty (w przypadku listów) i dwie warstwy nieprzezroczystego papieru pakowego (w przypadku paczek), które oznacza się następująco:

- 1) na kopercie wewnętrznej:

a) u góry i dołu koperty w jej środkowej części umieszcza się klauzulę tajności (odręcznie lub poprzez odciski pieczęci),

b) imię i nazwisko osoby pakującej przesyłkę wraz z podpisem oraz datę kopertowania,

c) w lewym górnym rogu – nazwę jednostki organizacyjnej nadawcy i numer pisma (sygnatury), pod którym zarejestrowano je w Dzienniku ewidencyjnym,

d) dokładną nazwę i adres odbiorcy,

e) na odwrocie koperty, we wszystkich miejscach łączenia koperty/paczki – stawia się pieczęć nagłówkową komórki organizacyjnej. Tak opieczętowaną kopertę/paczkę należy, w miejscach łączenia, zakleić przezroczystą taśmą samoprzylepną.

2) na kopercie zewnętrznej:

a) Koperta zewnętrzna podlega rejestracji w rejestrze korespondencji wychodzącej w systemie Elektronicznego Zarządzania Dokumentacją (EZD) PUW, zgodnie z § 42 „Szczegółowych zasad zarządzania dokumentacją (...)”, o których mowa w § 11 ust. 2 niniejszej instrukcji. Na kopercie zewnętrznej nie umieszcza się żadnych oznaczeń ani pieczęci wskazujących na niejawną charakter przesyłki. Podając sygnaturę pisma nie wskazuje się numeru z dziennika ewidencyjnego dokumentów o klauzuli „zastrzeżone”.

b) Przesyłki wymienione w ust. 1 przekazuje się celem wysłania do Kancelarii Ogólnej za Wykazem Przesyłek Nadanych, którego wzór i wymogi formalne reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. (Dz. U. z 2011 r. nr 271 poz. 1603) w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.

c) Przesyłki wymienione w ust. 1 mogą być wydane przedstawicielowi adresata, który przedstawi upoważnienie do ich odbioru i pokwituje ten fakt w Księżce Doręczeń Przesyłek Miejskowych lub za Wykazem Przesyłek Nadanych, którego numer zapisuje się w kolumnie 16 Dziennika ewidencyjnego. Wzór Wykazu Przesyłek Nadanych stanowi załącznik Nr 7 do Instrukcji.

§ 28. 1. Wysyłka dokumentu niejawnego w formie cyfrowej odbywa się z zachowaniem zasad ochrony informacji niejawnych, tj. dokument musi być zarejestrowany i podpisany, a fakt nadania korespondencji elektronicznej odnotowany w Dzienniku ewidencyjnym w rubrykach Adnotacje.

2. Korespondencja w formie cyfrowej wysyłana za pośrednictwem Systemu SKR-Z / CATEL musi zawierać w tytule wysyłanego maila oznaczenie klauzuli tajności: „zastrzeżone” oraz tytuł korespondencji.

Przegląd, zniesienie klauzuli tajności na dokumentach niejawnych o klauzuli „zastrzeżone”

§ 29. 1. Przeglądu dokumentów niejawnych o klauzuli „zastrzeżone” dokonuje się nie rzadziej niż raz na 5 lat, w celu utrzymania lub zniesienia z nich klauzuli tajności.

2. Zniesienie klauzuli tajności na dokumentach i materiałach o klauzuli „zastrzeżone” jest możliwe wyłącznie w przypadku ustania ustawowych przesłanek ochrony, o których mowa w art. 5 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209) oraz po wyrażeniu pisemnej zgody przez osobę, która nadała klauzulę tajności lub jej przełożonego.

3. Osoba, która nadaje klauzulę tajności może określić datę, po której nastąpi zniesienie lub zmiana klauzuli tajności. Po upływie tego okresu materiały zawierające informacje „zastrzeżone” mogą zostać przekazane do archiwum zakładowego

4. Przy znoszeniu klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu dokumentu i materiału, a w szczególności:

1) Oznaczenia zniesienia klauzuli tajności na dokumencie nieelektronicznym utrwalonym w formie pisma dokonuje się następująco:

a) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;

b) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis „Zniesiono klauzulę tajności” oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę prawną dokonania czynności;

2) Oznaczenie zniesienia klauzuli tajności dokumentu elektronicznego o klauzuli „zastrzeżone” umieszcza się w jego metryce.

5. Skreśleń i adnotacji, o których mowa w ust. 4 pkt 1 i 2 dokonuje wykonawca dokumentu i materiału.

6. Skreśleń i adnotacji, o których mowa w ust. 4 pkt 1 i 2, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

7. O fakcie dokonania zniesienia klauzuli tajności należy poinformować wszystkich odbiorców dokumentów lub materiałów, z których zniesiono klauzulę.

8. Odbiorcy dokumentu lub materiału, którzy przekazali je kolejnym odbiorcom są odpowiedzialni za poinformowanie ich o zniesieniu klauzuli tajności.

§ 30. 1. Po dokonaniu zniesienia klauzuli tajności na dokumentach niejawnych w komórkach organizacyjnych dokonuje się przeglądu dokumentacji jawnej, celem oceny jej praktycznego zastosowania dla pracy tych komórek.

2. Po zniesieniu klauzuli teczki aktowe przechowuje się w komórkach organizacyjnych, w których zostały wytworzone dokumenty, przez dwa lata, licząc od pierwszego stycznia roku następującego po roku zakończenia spraw, których akta znajdują się w tezcze. Po upływie tego okresu teczki aktowe przekazuje się do archiwum zakładowego, w trybie i na warunkach określonych w instrukcji archiwizacyjnej.

3. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców materiału. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności

4. Do archiwizowania dokumentacji i spraw „jawnych”, ostatecznie zakończonych stosuje się przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2020 r. poz. 164 oraz z 2025 r. poz. 1173, z późn. zm.) oraz rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (Dz. U. z 2015 r. poz. 1743, z późn. zm.). Działania związane z archiwizacją podlegają uzgodnieniu z Kierownikiem Oddziału „Kancelaria i Archiwum Zakładowe” Urzędu.

5. Archiwizacji dzienników ewidencyjnych oraz rejestrów dzienników ewidencji i teczek można dokonywać w sytuacji, gdy wszystkie odpowiednie rubryki dzienników i rejestrów zostały wypełnione:

- 1) adnotacją o zniesieniu klauzuli tajności na dokumentach i materiałach;
- 2) adnotacją o przekazaniu akt do Archiwum Zakładowego, potwierdzonego protokołem zdawczo-odbiorczym Archiwum Zakładowego, lub
- 3) adnotacją o dokonaniu ich zniszczenia potwierdzonego protokołem.

Przechowywanie, ochrona i niszczenie dokumentów oznaczonych klauzulą „zastrzeżone”

§ 31. 1. Dokumenty oznaczone klauzulą tajności „zastrzeżone”:

- 1) gromadzone są przez pracowników upoważnionych do dostępu do tych informacji w teczkach akt z klauzulą „zastrzeżone” zgodnie z jednolitym rzeczowym wykazem akt; nie należy ich przechowywać razem z dokumentami jawnymi, chyba, że stanowią integralną część dokumentacji; w przypadku spraw ostatecznie zakończonych, gdy dokument nadal jest chroniony,teczka akt z dokumentami jest przechowywana do czasu zniesienia klauzuli tajności;
- 2) podlegają obowiązkowej ochronie przed kradzieżą i nieuprawnionym ujawnieniem;
- 3) przechowywane są w szafach metalowych lub zamkniętym na klucz meblu biurowym;
- 4) drzwi do pomieszczeń, w których są one przechowywane wyposażone są w zamek zamykany na klucz, bez możliwości wejścia osób nieupoważnionych po godzinach pracy;
- 5) klucz od szafy metalowej lub mebla biurowego, w którym przechowywane są dokumenty niejawne, zabezpiecza się w sposób gwarantujący dostęp tylko osobie uprawnionej, zapewniający jego bezpieczeństwo;
- 6) po zakończeniu pracy, pracownik Urzędu zobowiązany jest do zamknięcia drzwi na wszystkie zamki. Klucze do urządzeń biurowych, po zakończonym dniu pracy muszą być zabezpieczone przez pracownika w miejscu niedostępnym i nieznanym powszechnie;
- 7) zabrania się wynoszenia kluczy poza Urząd, jak również udostępniania ich osobom nieuprawnionym.
- 8) zabrania się samodzielnego dokonywania wymiany kluczy bez uzyskania zgody Pełnomocnika Ochrony;

2. Informacje zastrzeżone podlegają ochronie do czasu zniesienia klauzuli tajności.

3. W przypadku spraw ostatecznie zakończonych, gdy dokument jest nadal chroniony, teczkę akt o klauzuli „zastrzeżone” przechowuje się do chwili zniesienia klauzuli tajności.

4. Niszczenie dokumentów o klauzuli tajności „zastrzeżone”:

- 1) niszczenie materiałów i dokumentów niejawnych o klauzuli „zastrzeżone” może nastąpić po ustaniu ich przydatności służbowej i wyłącznie na podstawie zgody osoby uprawnionej do podpisania dokumentu lub jej przełożonego;
- 2) dokumenty niejawne o klauzuli „zastrzeżone” podlegają zniszczeniu w sposób uniemożliwiający odtworzenie ich treści. Czynności tej dokonuje się przy użyciu dopuszczonych do użytku w Urzędzie niszczarek biurowych, spełniających

odpowiednie normy bezpieczeństwa dla dokumentów niejawnych (zalecany poziom bezpieczeństwa to co najmniej P-5);

- 3) materiały niejawne oznaczone klauzulą „zastrzeżone”, które utraciły praktyczne znaczenie i dla których minął okres przechowywania, winny być, po otrzymaniu zgody właściwego archiwum państwowego zniszczone w obecności dwóch pracowników posiadających dostęp do informacji niejawnych w niszczarce w sposób uniemożliwiający odtworzenie ich treści;
- 4) fakt zniszczenia zarejestrowanego dokumentu niejawnego odnotowuje się w Dzienniku ewidencyjnym przez przekreślenie na czerwono pozycji określającej niszczonego materiał oraz wpisanie w rubryce „Informacje uzupełniające / Uwagi” daty zniszczenia, a także umieszczenie informacji o zgodzie właściwego archiwum, imienia, nazwiska oraz czytelnego podpisu pracownika dokonującego tej czynności.

5. Niszczenie kopii, odpisów, tłumaczeń, materiałów pomocniczych o klauzuli tajności „zastrzeżone”:

- 1) materiały niejawne zarejestrowane w dzienniku ewidencyjnym lub innym pomocniczym urządzeniu ewidencyjnym prowadzonym przez Kancelarię Tajną, np. kopie, odpisy, tłumaczenia, materiały pomocnicze (kalki, taśmy) podlegają bieżącemu niszczeniu przez osobę sporządzającą i kierownika Kancelarii Tajnej. Zniszczenie materiału niejawnego odnotowuje się w dzienniku ewidencyjnym dokonując wpisu „Zniszczono dnia.....” i potwierdza czytelnymi podpisami sporządzającego materiał niejawny oraz kierownika kancelarii niejawnej;
- 2) zniszczenie kopii, odpisu, wypisu, wyciągu lub tłumaczenia należy odnotować dodatkowo na dokumencie, z którego kopię, odpis, wypis, wyciąg lub tłumaczenie wykonano;
- 3) zniszczenie wydruku z elektronicznego nośnika danych lub dokumentu elektronicznego przetwarzanego w systemie teleinformatycznym należy odnotować odpowiednio w metryce nośnika, jeżeli jest do niego dołączona, albo na piśmie, do którego załącznikiem jest nośnik, lub, jeżeli jest to możliwe, w metadanych dokumentu elektronicznego;
- 4) zniszczenia brudnopisów, wydruków próbnych, błędnych kopii lub notatek roboczych posiadających oznaczenie „zastrzeżone”, które nie podlegały rejestracji w urządzeniach ewidencyjnych, dokonuje bezpośrednio pracownik je wytwarzający, stosując się do wymogów określonych w ust. 4, pkt 2 – 4.

6. Niszczenie informatycznych nośników danych (m.in. dyski optyczne, pamięci flash, płyty CD/DVD,), na których przetwarzano informacje niejawne o klauzuli „zastrzeżone”, może zostać przeprowadzone wyłącznie przez Zespół ds. Ochrony Informacji Niejawnych po wcześniejszym sporządzeniu protokołu zniszczenia. Niszczenie nośników elektronicznych wymaga ich fizycznego uszkodzenia (np. przewiercenia) lub zmielenia w specjalistycznych urządzeniach niszczących (np.

niszczarka z poziomem bezpieczeństwa co najmniej P-5, kat. O) i odbywa się zgodnie z zapisanymi Procedurami Bezpiecznej Eksploatacji STI-PUW.

Organizacja spotkań o charakterze niejawnym

§ 32. Organizacja spotkań niejawnych wymaga ścisłego przestrzegania Ustawy o ochronie informacji niejawnych. Obejmuje to weryfikację uprawnień uczestników, przygotowanie bezpiecznego i odpowiednio zabezpieczonego przed podsłuchem pomieszczenia oraz kontrolowany obieg i rejestrację wszelkich materiałów omawianych w trakcie spotkania.

§ 33. 1. W przypadku konieczności zorganizowania spotkania, w trakcie którego ustnie będą omawiane informacje klasyfikowane jako „zastrzeżone”, uczestnicy spotkania są niezwłocznie informowani o jego niejawnym charakterze.

2. W spotkaniu, o którym mowa w ust. 1 mogą uczestniczyć wyłącznie osoby spełniające warunki dopuszczenia do pracy na stanowiskach związanych z dostępem do informacji niejawnych, których zakres obowiązków obejmuje sprawy omawiane na spotkaniu.

3. Uczestnicy spotkania o charakterze niejawnym potwierdzają swoją tożsamość oraz celowość udziału (zasada need-to-know – wiedzy niezbędnej do wykonania zadania) oraz przedstawiają posiadane dostępy do informacji niejawnych wraz z aktualnym zaświadczeniem ze szkolenia z zakresu ochrony informacji niejawnych.

4. Spotkanie o charakterze niejawnym nie może być utrwalane na magnetycznych lub cyfrowych nośnikach obrazu i dźwięku.

5. Protokoły i notatki ze spotkania niejawnego oznacza się klauzulą „zastrzeżone” i dokonuje ich rejestracji z zachowaniem przepisów.

§ 34. 1. Spotkanie o charakterze niejawnym można zorganizować jedynie w zamkniętej sali spełniającej wymagania ochrony fizycznej, Strefie ochronnej III.

2. Przed spotkaniem należy przeprowadzić kontrolę przeciwinwigilacyjną (brak urządzeń rejestrujących lub nagrywających).

3. W trakcie spotkania należy zapewnić stałą kontrolę dostępu, uniemożliwiającą podgląd z zewnątrz, wgląd lub podsłuch przez osoby niepowołane.

4. Do pomieszczenia, w którym odbywa się spotkanie o charakterze niejawnym obowiązuje zakaz wnoszenia telefonów komórkowych, laptopów oraz

innych niedozwolonych nośników danych umożliwiających rejestrację obrazu lub dźwięku.

Postanowienia końcowe i odpowiedzialność

§ 35. Każdy pracownik Urzędu posiadający dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone” na zajmowanym stanowisku jest zobowiązany do zapoznania się z treścią niniejszej instrukcji.

§ 36. Każdy pracownik Urzędu posiadający na zajmowanym stanowisku dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone”, zobowiązany jest powiadomić bezpośredniego przełożonego i Pełnomocnika Ochrony o wszelkich nieprawidłowościach związanych z naruszeniem zapisów niniejszej Instrukcji.

§ 37. Za naruszenie postanowień niniejszej instrukcji, w szczególności za nieuprawnione ujawnienie informacji niejawnych o klauzuli „zastrzeżone”, podlega się odpowiedzialności dyscyplinarnej lub służbowej, uregulowanej w odrębnych przepisach.

§ 38. W sprawach nieuregulowanych w niniejszej instrukcji, stosuje się odpowiednie przepisy zawarte w aktach prawnych wymienionych na wstępie.

Załącznik Nr 1. Wzór Upoważnienia do dostępu do informacji niejawnych o klauzuli

/miejsowość, data/

.....
Nazwa jednostki organizacyjnej upoważniającej osobę
do dostępu do informacji niejawnych o klauzuli „zastrzeżone”

/numer sprawy/

**UPOWAŻNIENIE DO DOSTĘPU DO INFORMACJI NIEJAWNYCH O KLAUZULI
„ZASTRZEŻONE”**

Nr

Na podstawie art. 21 ust. 4 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2025 r., poz. 1209, ze zm.) upoważniam do dostępu do informacji niejawnych oznaczonych klauzulą tajności „**zastrzeżone**” następującą osobę:

1. Imię (imiona):
2. Nazwisko (w tym przybrane):
3. Nr PESEL:
4. Imię ojca:

Niniejsze upoważnienie jest ważne do chwili jego odwołania, nie dłużej jednak niż do chwili:

- 1) ustania stosunku pracy łączącego osobę upoważnioną z Pomorskim Urzędem Wojewódzkim w Gdańsku;*
- 2) rozwiązania lub wygaśnięcia umowy zlecenia, na podstawie której osoba upoważniona wykonuje czynności na rzecz Pomorskiego Urzędu Wojewódzkiego w Gdańsku;*
- 3) zakończenia stażu odbywanego przez osobę upoważnioną w Pomorskim Urzędzie Wojewódzkim w Gdańsku, w tym jego wcześniejszego przerwania.*

.....
Pieczęć i podpis kierownika jednostki organizacyjnej

* – niepotrzebne skreślić

„zastrzeżone”.

Załącznik Nr 2. Wzór protokołu zdawczo-odbiorczego.

Nr sprawy.....

/miejscowość, data/

PROTOKÓŁ ZDAWCZO-ODBIORCZY

Sporządzony w związku ze zmianą na stanowisku

1. Zdający:
2. Przyjmujący:
3. Przekazaniu podlegają zdeponowane i zarejestrowane w /nazwa komórki organizacyjnej/
4. Wykaz przekazywanych dokumentów / materiałów:
 - 1)
 - 2)
 - 3)
 - 4)

Protokół sporządzono w 3 egzemplarzach:

Egz. Nr 1 – przekazujący

Egz. Nr 2 – przyjmujący

Egz. Nr 3 – Kancelaria Tajna

Przekazujący:

Przyjmujący:

/podpis/

/podpis/

„ZASTRZEŻONE”

Pomorski Urząd Wojewódzki
w Gdańsku
Wydział / Biuro / Zespół

Nr egz. lub Egz. pojedynczy
/umieszczany na każdej stronie/

Sygnatura literowo-cyfrowa
IN-Z-15478/2026/1311.1.XY*
/numer pisma – umieszczany na każdej stronie/

„Jawne” po odłączeniu załączników
lub inne dyspozycje co do dokumentu

Adresat

/lub adresaci wg rozdzielnika/

dot.:

TREŚĆ PISMA

Na ostatniej stronie pod treścią pisma umieszcza się:

Załączników na stronach:

Zał. Nr – „ZASTRZEŻONE” Nr, Tytuł lub rodzaj załączonego materiału, na ... stronach –
do zwrotu lub tylko adresat

STANOWISKO

imię i nazwisko

osoby uprawnionej do podpisania dokumentu

Wykonano w ... egzemplarzach:

Egz. Nr 1 – adresat

Egz. Nr 2 – ad acta

lub wykonano w egzemplarzu pojedynczym;

Wykonał: imię i nazwisko

Str. ... / ...

„ZASTRZEŻONE”

Załącznik Nr 3. Przykład szaty graficznej pisma niejawnego.

* – na sygnaturę cyfrowo-literową składają się:

1) Literowe oznaczenie komórki organizacyjnej;

- 2) Symbol oznaczenia klauzuli tajności „Z”;
- 3) Numer, pod którym dokument został zarejestrowany w Dzienniku ewidencyjnym i pełny rok;
- 4) Inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu i jego przynależności do określonej sprawy: numer JRWA, numer sprawy, inicjały wytwórcy.

Załącznik Nr 4. Wzór Wniosku o Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone”.

.....
/miejscowość, data/

Wojewoda Pomorski

za pośrednictwem

Pełnomocnika Wojewody ds. Ochrony Informacji Niejawnych

W związku z zajmowaniem stanowiska, które łączy się z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone”, na podstawie art. 21 ust. 4 w związku z art. 15 ust. 1 pkt 8 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209) proszę o wydanie upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone” dla /imię i nazwisko, stanowisko/.

.....
/podpis przełożonego/

Załącznik Nr 5. Wzór karty zapoznania się z dokumentem.

KARTA ZAPOZNANIA SIĘ Z DOKUMENTEM NR _____

Lp.	UDOSTĘPNIENIE DOKUMENTU			Uwagi
	Imię i nazwisko osoby, której dokument udostępniono	data	podpis	
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

Załącznik Nr 6. Wzór Dziennika pracy systemu teleinformatycznego.

Dziennik Pracy Systemu Teleinformatycznego
(STI-PUW / SKR-Z / CATEL)

Lp.	Data		Imię i nazwisko osoby wytwarzającej dokument / wykonującej czynności w	Nazwa dokumentu, klauzula tajności, opis czynności wykonywanych na stanowisku	Podpis osoby wykonującej czynności	Uwagi Wydruk
	/ godz. rozpoczęcia pracy w	/ godz. zakończenia pracy w				
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						

Załącznik Nr 7. Wzór Wykazu Przesyłek Nadanych.

				/miejscowość, data/
..... (pieczęć nagłwkowa jednostki organizacyjnej)				
WYKAZ NR/..... PRZESYŁEK NADANYCH				
przekazanych przez (nazwa i adres jednostki organizacyjnej wysyłającego)				
do wysłania przez (nazwa przewoźnika lub nazwisko doręczyciela)				
Lp.	Numer przesyłki	Rodzaj przesyłki (list, paczka itp.)	Do kogo adresowany	Uwagi
1.		(zpo)		
2.				
3.				
4.				
Ogółem przesyłek: (liczbowo) (słownie)				
..... (podpis sporządzającego wykaz)				
..... (podpis doręczającego)				
..... (podpis przyjmującego)				
..... (data i godzina przyjęcia)				
mp. (pieczęć przewoźnika)				

Załącznik Nr 8. Wzór Protokołu niezgodności lub uszkodzenia przesyłki

Wzór protokołu w sprawie uszkodzenia przesyłki stanowi załącznik nr 1 do Rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne:

..... (miejscowość, data)	
(pieczęć nagłówkowa przewoźnika)	Egz. nr
PROTOKÓŁ Nr W SPRAWIE USZKODZENIA PRZESYŁKI	
My niżej podpisani oświadczamy, że w dniu, o godz., przy rozpakowaniu pakietu/pojemnika* nr, nadanego przez W stwierdzono uszkodzenie (określenie rodzaju przesyłki)	
nr adresowanego do	
Uszkodzenie przesyłki nastąpiło w wyniku (rodzaj i przyczyna uszkodzenia)	
.....	
Wyżej wymieniona przesyłka została przepakowana i zabezpieczona celem niedopuszczenia do dalszych uszkodzeń i doręczona odbiorcy wraz z egzemplarzem nr 1 niniejszego protokołu.	
Uszkodzenie przesyłki wskazuje/nie wskazuje* na możliwość ujawnienia jej treści.	
Podpis przewoźnika:	
Przyczyny odmowy przyjęcia przesyłki przez adresata:	
..... (imię i nazwisko)	
Wyk. w 3 egz. Egz. nr 1 — adresat Egz. nr 2 — nadawca Egz. nr 3 — aa	
* Niepotrzebne skreślić	