Załącznik Nr 1 do Zarządzenia
nr 331/2020 Wójta Gminy Lubawa
z dnia 15.09.2020 r.

Zatwierdzam

……

*/Kierownik Jednostki/*

# PLAN OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY LUBAWA

**OPRACOWAŁA:**

*Pełnomocnik Ochrony Informacji Niejawnych*

**Żaneta Senkowska**

**SPIS TREŚCI**

## ZAŁĄCZNIKI DO PLANU OCHRONY INFORMACJI NIEJAWNYCH

1. **SPOSÓB OZNACZANIA DOKUMENTÓW NIEJAWNYCH ORAZ UMIESZCZANIA KLAUZUL NA TYCH DOKUMENTACH**
2. **WZORY PISM I UPOWAŻNIEŃ**
3. **PROTOKÓŁ OCENY DOKUMENTACJI ARCHIWALNEJ**
4. **SPIS DOKUMENTACJI NIEARCHIWALNEJ PRZEZNACZONEJ NA MAKULATURĘ LUB ZNISZCZENIE**
5. **PROTOKÓŁ KOMISYJNEGO ZNISZCZENIA DOKUMENTÓW NIEARCHIWALNYCH**

# I. AKTY PRAWNE ZWIĄZANE Z OCHRONA INFORMACJI NIEJAWNYCH

- Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. ( Dz. U. z 2019 r. poz. 742 t. j.)
- Rozporządzenie Prezesa 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 2011 r. nr 276 r. poz. 1631)
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa ( Dz. U. z 2010 r. nr 258 poz. 1754)
- 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)
- 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)
- Rozporządzenie Prezesa Rady Ministrów z dnia 29 sierpnia 2005 r. w sprawie wysokości i trybu pobierania, przez służbę ochrony państwa, opłat za przeprowadzenie postępowania bezpieczeństwa przemysłowego, sprawdzeń oraz postępowań sprawdzających ( Dz. U. 2005 r. nr 174 poz. 1447)
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne ( Dz. U. 2011 r. nr 271 poz. 1603)
- Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności (Dz. U. 2011 r. nr 288 poz. 1692)

## II. DEFINICJE W ROZUMIENIU PLANU OCHRONY INFORMACJI NIEJAWNYCH

Informacjom niejawnym nadaje się klauzule **„POUFNE”**, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) Utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
2) Utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
3) Zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
4) Utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) Utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
6) Zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
7) Wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Informacjom niejawnym nadaje się klauzulę **„ZASTRZEŻONE”**, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonanie 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.

1) Rękojmia zachowania tajemnicy- zdolność osoby di spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
2) Dokumentem- jest każda utrwalona informacja niejawna;
3) Materiałem- jest dokument lub przedmiot jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część;
4) Jednostka organizacyjną- jest podmiot wymieniony w art. 1 ust. 2 ustawy o ochronie informacji niejawnych;
5) Systemem teleinformatycznym- jest system, teleinformatyczny w rozumieniu art. 2 pkt. 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002, nr 144, poz. 1204 z późn. zm.);
6) Siecią teleinformatyczną- jest organizacyjne i techniczne połączenie systemów teleinformatycznych;
7) Akredytacją bezpieczeństwa teleinformatycznego- jest dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie;
8) Dokumentacją bezpieczeństwa systemu lub sieci informatycznej- są Szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie;
9) Ryzykiem- jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

10) Szacowaniem ryzyka- jest całościowy proces analizy i oceny ryzyka;
11) Zarządzaniem ryzyka- są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnienie ryzyka;
12) Kancelaria niejawna- wydzielone, wyodrębnione pomieszczenie przeznaczone do ewidencjonowania, opracowywania, przechowywania dokumentów niejawnych oznaczonych klauzulą „poufne";
13) Pracownik kancelarii niejawnej- osoba wyznaczona przez kierownika jednostki do prowadzenia kancelarii niejawnej.

## III. POSTANOWIENIA OGÓLNE

1. Plan ochrony informacji niejawnych w Urzędzie Gminy Lubawa określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami.
2. Plan ochrony informacji niejawnych opracowany został na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 t. j.) oraz zawiera wymagane elementy, o których mowa w §9 ust. 1 i 2 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. 2012 poz. 683).
3. Przedmiotem ochrony w Urzędzie Gminy Lubawa są informacje niejawne oznaczone klauzulą **„zastrzeżone".**
4. Pion ochrony informacji niejawnych tworzą osoby w składzie:
   - pełnomocnik ochrony informacji niejawnych,
   - pracownik kancelarii niejawnej,
   - inspektor bezpieczeństwa teleinformatycznego,
   - administrator bezpieczeństwa informacji.

## IV. OPIS POMIESZCZEŃ LUB OBSZARÓW DLA INFORMACJI NIEJAWNYCH O KLAUZULI „ZASTRZEŻONE", W TYM OKREŚLENIE ICH GRANIC I WPROWADZONEGO SYSTEMU KONTROLI

1. Charakterystyka obiektu.
   Budynek Urzędu Gminy Lubawa, Fijewo 73, 14-260 Lubawa, w którym znajduje się Kancelaria Niejawna jest trzykondygnacyjny, wolno stojący, konstrukcji murowanej. Pomieszczenia biurowe od pozostałych pomieszczeń oddzielają ścianki działowe. Urząd Gminy Lubawa jest właścicielem budynku. Pomieszczenia w obiekcie zajmowane są przez Urząd Gminy Lubawa, Ośrodek Pomocy Społecznej Gminy Lubawa i Filię Powiatowego Urzędu Pracy w Iławie.
2. Pomieszczenia do przetwarzania informacji niejawnych oraz system kontroli dostępu.
   Informacje niejawne o klauzuli „zastrzeżone" przetwarza się w Budynku B w pomieszczeniu numer 20A - Kancelarii Niejawnej na parterze, a przechowuje w sejfie.

# V. OCENA ZAGROŻEN ZEWNĘTRZNYCH I WEWNĘTRZNYCH

## 1.1 OCENA ZAGROŻEŃ ZEWNĘTRZNYCH

Zagrożeniami zewnętrznymi dla Urzędu Gminy Lubawa:

- możliwość napadu przez zorganizowanie grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
- możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości i ochronie mienia urzędu.

## 1.2 SYMPTOMY MOGĄCE ŚWIADCZYĆ O PRZYGOTOWANIU NAPADU LUB WŁAMANIA DO BUDYNKU

- Wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniem urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym" spotkaniu,
- Nawiązaniem rozmów przez osoby postronne z pracownikami,
- Podszywaniem się pod byłych pracowników urzędu i przejawianie zainteresowaniem tym, co się po latach zmieniło,
- Interesowaniem się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- Obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki itp.,
- Rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- Celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
- Próby pozyskania do grup przestępczych, pracowników urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe)

## 1.3 WNIOSKI

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

1) Systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
2) Pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
3) Stosować zasadę niedopuszczenia osób niepowołanych do otwarcia sejfu,
4) Wykonywanie prac porządkowych, remontowych itp. W strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

### 2.1. OCENA ZAGROŻEŃ WEWNĘTRZNYCH

- próby zaboru dokumentów lub mienia przez pracowników urzędu,
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- byli pracownicy urzędu zwolnieni dyscyplinarnie,
- rozpoznanie organizacji pracy Urzędu Gminy celem łatwiejszej pracy grup przestępczych na terenie urzędu,
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione,

### 2.2. WNIOSKI

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności poprzedzające ewentualne możliwości zaistnienia zagrożeń:

1) Zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,
2) Prowadzenie szczególnego nadzoru nad próbami kserowania, kopiowania bez zgody przełożonego,
3) Uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
4) Zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez kierownika jednostki.

## VI. PRZEDMIOT OCHRONY

1. Informacje niejawne oznaczone klauzulą:
   - „zastrzeżone”,
   - pomieszczenia w których są przechowywane i opracowywane materiały niejawne

## VII. EWIDENCJA INFORMACJI NIEJAWNYCH

1. Dokumenty niejawne o klauzuli „zastrzeżone” mogą być ewidencjonowane na zasadach określonych przez kierownika jednostki, opisanych w Planie Ochrony Informacji Niejawnych,
2. Dokumenty niejawne wpływające do Urzędu ewidencjonuje się w dzienniku ewidencyjnym
3. Dokumenty niejawne wytworzone – wychodzące z Urzędu rejestruje się w dzienniku ewidencyjnym,

4. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu ewidencjonuje się w odrębnej pozycji dziennika ewidencyjnego,
5. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego o klauzuli „ zastrzeżone" powinien by ć poprzedzony skrótem literowym „Z",
7. Ewidencjonowaniu podlegają wszystkie dokumenty niejawne oznaczone klauzulą „zastrzeżone"
8. Sposób właściwego opisania dokumentu niejawnego został przedstawiony w załączniku do Planu Ochrony Informacji Niejawnych,
9. Prowadzi się równie Rejestr Dzienników służący do ewidencjonowania książek i dzienników ewidencyjnych, rejestrów.
10. Pracownik kancelarii niejawnej przyjmuje przesyłki za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.

    Przyjmując przesyłkę, sprawdza się:
    1) prawidłowość adresu;
    2) całość opakowania;
    3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy;
11. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi - pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik - kolejny egzemplarz protokołu przekazuje się tak e jemu.
12. Pracownik kancelarii niejawnej :
    1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
    2) ustala, czy liczba załączników i stron jest zgodna z liczb ą oznaczoną na poszczególnych dokumentach.
13. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa w pk.12, pracownik kancelarii niejawnej sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.
14. Pracownik kancelarii niejawnej odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt. 11 i 13, w odpowiednim dzienniku lub rejestrze w rubryce "Informacje uzupełniające/Uwagi".

## VIII. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH

W systemie teleinformatycznym w ramach identyfikacji ryzyka wdrożono poniższe zabezpieczenia. Zabezpieczenie jest to środek o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko. Poprzez wdrożenie poniższego zbioru zabezpieczeń zapewniono bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym. Wykaz zabezpieczeń wdrożonych w systemie teleinformatycznym BSK przedstawiono poniżej.

1) Budynek „B" Urzędu Gminy Lubawa został zabezpieczony Systemem Sygnalizacji Włamania i Napadu (SSWiN).
2) Za rozbrajanie/uzbrajanie systemu alarmowego odpowiadają uprawnieni pracownicy Urzędu wyznaczeni pisemnie przez kierownika jednostki organizacyjnej. Każda osoba uprawniona do rozbrajania/uzbrajania systemu alarmowego posiada indywidualny kod.
3) Stan systemu, w tym generowane ostrzeżenia i alarmy, jest całodobowo monitorowany przez koncesjonowaną firmę ochrony „Solid Security".
4) Po otrzymaniu sygnału alarmowego z chronionego obiektu firma ochrony „Solid Security", w pierwszej kolejności zawiadamia telefonicznie upoważnionego przez kierownika jednostki organizacyjnej pracownika Urzędu. Zawiadomiony pracownik potwierdza konieczność przyjazdu grupy patrolowo-interwencyjnej.
5) W przypadku włamania lub próby włamania w pomieszczeniu nr 20A (lokalizacja BSK) zawiadamiany jest telefonicznie: pełnomocnik ochrony, a w następnej kolejności pracownik Kancelarii Niejawnej. Zawiadomiona osoba ma obwiązek przyjazdu na miejsce i sprawdzenia stanu ochrony informacji niejawnych.
6) Drzwi do pokoju 20A są to drzwi aluminiowe. Okno zabezpieczone jest roletą antywłamaniową, zasłoniętą na stałe.
7) Stanowisko systemu BSK zostało tak zlokalizowane, że po wejściu do pokoju nr 20A niemożliwy jest bezpośredni wgląd w monitor stanowiska BSK.
8) W pokoju nr 20A znajduje się szafa metalowa, w której przechowywane jest stanowisko BSK. Szafa metalowa (sejf), w której przechowywane jest stanowisko BSK (laptop) to szafa metalowa wzmocniona klasy -B-. Nr świadectwa kwalifikacji 1402000, producentem szafy jest Tech Mark, nazwa szafy: 1D1PKSNB, nr fabr.: 0230501, data produkcji: 29.05.2001 r.
9) Pokój nr 20A (lokalizacja BSK) po zakończeniu pracy sprawdza się w celu upewnienia, że informacje niejawne zostały właściwie zabezpieczone.
10) Pracownik Kancelarii Niejawnej identyfikuje wszystkie osoby wchodzące do pokoju nr 20A i sprawuje nadzór w zakresie uprawnionego wejścia do pomieszczenia.
11) Prawo wejścia do pokoju nr 20A posiadają wyłącznie uprawnione osoby na podstawie listy osób uprawnionych, zatwierdzonej przez pełnomocnika ds. ochrony informacji niejawnych. Wszystkie inne osoby są nieuprawnione do samodzielnego przebywania w pokoju nr 20A i mogą wejść do pokoju nr 20A wyłącznie za zgodą osoby uprawnionej i pod jej nadzorem.

12) Prowadzona jest papierowa ewidencja wejść/wyjść dla wszystkich osób wchodzących/wychodzących do/z do pokoju nr 20A. Osoba wchodząca do pokoju wpisuje się w ewidencji wejść/wyjść.
13) System kontroli dostępu do pokoju nr 20A oparty jest na zamkniętych na klucz drzwiach wraz z ewidencją wydanych kluczy, na ewidencji papierowej wejść/wyjść dla wszystkich osób wchodzących, na elektronicznej ewidencji uzbrojenia/rozbrojenia systemu alarmowego, na identyfikacji przez pracownika Kancelarii Niejawnej w zakresie uprawnionego wejścia do pokoju nr 20A oraz na okresowej i losowej kontroli pełnomocnika ochrony w zakresie uprawnionego wejścia do pokoju nr 20A.
14) Prowadzona jest papierowa ewidencja wydanych kluczy użytkowych i zapasowych do drzwi wejściowych do pokoju nr 20A i szafy metalowej w pokoju nr 20A, w której przechowywane jest stanowisko BSK.
15) Klucze użytkowe i zapasowe do pokoju nr 20A wydawane są tylko uprawnionym osobom na podstawie listy osób uprawnionych. Uprawnienia do pobierania kluczy nadaje pełnomocnik ochrony, który decyduje o dodaniu/wykreśleniu z listy osób uprawnionych do pobierania kluczy użytkowych i zapasowych.
16) Prawo pobrania kluczy użytkowych i zapasowych do szafy metalowej, w której przechowywane jest stanowisko BSK w pokoju nr 20A posiada wyłącznie pracownik Kancelarii Niejawnej oraz pełnomocnik ochrony.
17) Prowadzona jest regularna konserwacja i inwentaryzacja sprzętu. Konserwacja prowadzona jest zgodnie z zaleceniami producenta. Prowadzony jest rejestr sprzętu teleinformatycznego. Sprzęt jest monitorowany pod względem sprawności i na bieżąco naprawiany.
18) W celu zminimalizowania tego zjawiska system BSK posiada wbudowaną baterię w komputer (laptop), która pozwala zabezpieczyć pracę komputera do 60 minut od wyłączenia zasilania.
19) Przeprowadzane są cyklicznie szkolenia z bezpieczeństwa. Tematyka szkoleń obejmuje: zasady bezpiecznej pracy z elektronicznymi nośnikami danych, zagrożenia dla systemu teleinformatycznego, fizyczne zabezpieczenie komputera, ochrona antywirusowa, prawne aspekty ochrony informacji niejawnych, zagadnienia ochrony fizycznej.
20) System operacyjny i użytkowane aplikacji zostały skonfigurowane w sposób umożliwiający prowadzenie elektronicznej ewidencji zdarzeń.
21) W systemie wdrożono procedurę zarządzania zmianami i aktualizacjami systemu teleinformatycznego. W przypadków wystąpienia błędów konfiguracyjnych lub oprogramowania wdrażane są na bieżąco poprawki. Zainstalowane są najnowsze aktualizacje systemu operacyjnego i użytkowanego oprogramowania dystrybuowane przez producentów oprogramowania.
22) System teleinformatyczny objęty jest procesem zarządzania ryzykiem dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie. Proces zarządzania ryzykiem obejmuje procesy: szacowanie ryzyka dla bezpieczeństwa informacji niejawnych; postępowanie z ryzykiem; akceptację ryzyka; przegląd, monitorowanie i informowanie o ryzyku.

23) Wdrożono w systemie teleinformatycznym oprogramowanie antywirusowe. Prowadzona jest regularna aktualizacja definicji wirusów.
24) Ustawiono w systemie teleinformatycznym prawa dostęp, które określają czy dany użytkownik ma dostęp do określonego obiektu i co może z nim zrobić.
25) W systemie teleinformatycznym włączono tylko niezbędne funkcjonalności, niezbędne do prawidłowej realizacji zadań. Wyłączono zbędne protokoły i usługi.
26) Prowadzone są regularne testy bezpieczeństwa systemu teleinformatycznego sprawdzające wdrożone zabezpieczenia, konfiguracje systemu teleinformatycznego, podatności sytemu.
27) Wdrożono identyfikację i uwierzytelnienie użytkownika w systemie teleinformatycznym. Uwierzytelnienie użytkownika w systemie polega na podaniu indywidualnej nazwy konta (loginu) i hasła dostępu. Obowiązuje bezwzględny zakaz zapisywania przez użytkowników systemu indywidualnych haseł dostępu.
28) W systemie teleinformatycznym wdrożono procedury zarządzania incydentami bezpieczeństwa. W przypadku wystąpienia incydentu następuję odpowiednio szybka reakcja na incydent. Incydenty są ewidencjonowane, po każdym poważnym incydencie następuje szacowanie ryzyka i wdrażane są środki ochrony przeciwdziałające przyszłym incydentom.
29) Wykonywany jest okresowo audyt bezpieczeństwa, podczas audytu administrator systemu wspólnie z inspektorem bezpieczeństwa teleinformatycznego sprawdzają stan zabezpieczeń, poprawność wykonywania procedur.
30) Inspektor bezpieczeństwa teleinformatycznego na bieżąco prowadzi kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.
31) Sprzęt teleinformatyczny został oplombowany przez inspektor bezpieczeństwa teleinformatycznego. Plomby są ewidencjonowane, stan plomb jest kontrolowany okresowo przez inspektora bezpieczeństwa teleinformatycznego. Nie istnieje możliwość bezśladowego otwarcia obudowy urządzenia.
32) Wprowadzono wymóg stosowania złożonych haseł przez użytkowników i administratorów. Hasła nie mogą zawierać znaczącej części nazwy konta użytkownika ani pełnej nazwy użytkownika; Muszą mieć długość przynajmniej 12 znaków; Muszą zawierać znaki należące do trzech z następujących czterech kategorii: Wielkie litery od A do Z; Małe litery od a do z; 10 cyfr podstawowych (od 0 do 9); Znaki niealfabetyczne (na przykład: !, $, #, %).
33) W przypadku pozostawienia komputera przez zalogowanego użytkownika przez określony czas (tzw. czas bezczynności), nastąpi blokada sesji (konta) użytkownika. W celu kontynuowania pracy użytkownik musi odblokować sesję (konto) swoim hasłem.
34) Login i hasło Administratora systemu służące do uwierzytelniania w systemie operacyjnym oraz systemie BIOS/UEFI zdeponowano w zapieczętowanych kopertach w szafie metalowej zamykanej na klucz w pokoju nr 20A (Kancelaria Niejawna).
35) Dysk twardy, na którym przechowywane są informacje niejawne został zarejestrowany jako materiał niejawny i prawidłowo oznaczony klauzulą tajności „zastrzeżone” i sygnaturą literowo-cyfrową.

36) Wszyscy użytkownicy i administratorzy pracują na własnych kontach w systemie operacyjnym. Konta użytkowników posiadają ograniczone uprawnienia, wyłączono zbędne funkcjonalności dla tych kont.
37) Komputer został ustawiony w taki sposób, aby nie było możliwości podglądu przez osoby nieuprawnione.
38) Przeprowadzono konfigurację BIOS/UEFI: zabezpieczono hasłem; wyłączono zbędne usługi, porty, protokoły; ustawiono sekwencję uruchamiania wyłącznie z dysku twardego.

## IX. DOSTĘP DO INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „poufne" lub „zastrzeżone" mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.

2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „poufne" może nastąpić:
   - po uzyskaniu przez pracownika poświadczenia bezpieczeństwa po przeprowadzonym przez Pełnomocnika ochrony zwykłym postępowaniu sprawdzającym,
   - po przeszkoleniu danej osoby w zakresie ochrony informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia o przeszkoleniu.
3. Uzyskanie uprawnień dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić:
   - po uzyskaniu przez pracownika upoważnienia dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone" wydanego przez kierownika jednostki,
   - po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.
4. **Zwykłe postępowanie sprawdzające** wobec pracowników jednostki w związku z dostępem do informacji niejawnych oznaczonych klauzulą „poufne" na pisemne polecenie kierownika jednostki przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych.
5. Osoba podlegająca procedurze postępowania sprawdzającego zobowiązana jest do: wypełnienia określonej przepisami ustawy ankiety bezpieczeństwa osobowego, wypełnienia ankiety w sposób dokładny i zgodny z prawdą.
6. Odmowa poddania się postępowaniu sprawdzającemu ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych o klauzuli „poufne", a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji oznaczonych klauzulą „poufne" może skutkować:
   - przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi o klauzuli „poufne",
   - rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,
   - niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się

zatrudnienie w Urzędzie.

## X. KANCELARIA NIEJAWNA

System teleinformatyczny BSK zlokalizowany jest w pokoju nr 20A (Kancelaria Niejawna) na parterze w budynku „B" Urzędu Gminy Lubawa, Fijewo 73, 14-260 Lubawa. Szczegółowa lokalizacja systemu BSK została przedstawiona na rysunkach nr 3 i 5.

Do pokoju nr 20A prowadzi jedno wejście z korytarza. Drzwi do pokoju 20A są to drzwi aluminiowe. Okno zabezpieczone jest roletą antywłamaniową, zasłoniętą na stałe. Pokój nr 20A sąsiaduje bezpośrednio z korytarzem, toaletą oraz pom. biurowym Ośrodka Pomocy Społecznej. Pokój nr 20A stanowi Kancelarię Niejawną.

Stanowisko systemu BSK zostało tak zlokalizowane, że po wejściu do pokoju nr 20A niemożliwy jest bezpośredni wgląd w monitor stanowiska BSK.

W pokoju nr 20A znajduje się szafa metalowa, w której przechowywane jest stanowisko BSK. Szafa metalowa (sejf), w której przechowywane jest stanowisko BSK (laptop) to szafa metalowa wzmocniona klasy -B-. Nr świadectwa kwalifikacji 1402000, producentem szafy jest Tech Mark, nazwa szafy: 1D1PKSNB, nr fabr.: 0230501, data produkcji: 29.05.2001 r.

Pokój nr 20A (lokalizacja BSK) po zakończeniu pracy sprawdza się w celu upewnienia, że informacje niejawne zostały właściwie zabezpieczone.

Pracownik Kancelarii Niejawnej identyfikuje wszystkie osoby wchodzące do pokoju nr 20A i sprawuje nadzór w zakresie uprawnionego wejścia do pomieszczenia.

Prawo wejścia do pokoju nr 20A posiadają wyłącznie uprawnione osoby na podstawie listy osób uprawnionych, zatwierdzonej przez pełnomocnika ds. ochrony informacji niejawnych. Wszystkie inne osoby są nieuprawnione do samodzielnego przebywania w pokoju nr 20A i mogą wejść do pokoju nr 20A wyłącznie za zgodą osoby uprawnionej i pod jej nadzorem.

Pomieszczenie nr 20A zabezpieczone jest czujką ruchu systemu alarmowego. Szczegółowy opis systemu alarmowego przedstawiono w rozdziale V.1 „Bezpieczeństwo fizyczne – Opis lokalizacji systemu".

Prowadzona jest papierowa ewidencja wejść/wyjść dla wszystkich osób wchodzących/wychodzących do/z do pokoju nr 20A. Osoba wchodząca/wychodzących do/z pokoju wpisuje się w ewidencji wejść/wyjść. Ewidencję wejść/wyjść prowadzi pracownik Kancelarii Niejawnej. Nadzór nad prawidłowością wpisów w ewidencji wejść/wyjść sprawuje pełnomocnik do spraw ochrony informacji niejawnych oraz inspektor bezpieczeństwa teleinformatycznego. Ewidencja prowadzona jest w formie papierowego rejestru, który zawiera: imię i nazwisko osoby wchodzącej, datę, godzinę wejścia i wyjścia, powód wejścia, uwagi oraz podpis osoby wchodzącej.

System kontroli dostępu do pokoju nr 20A oparty jest na zamkniętych na klucz drzwiach wraz z ewidencją wydanych kluczy, na ewidencji papierowej wejść/wyjść dla wszystkich osób wchodzących, na elektronicznej ewidencji uzbrojenia/rozbrojenia systemu alarmowego, na identyfikacji przez pracownika Kancelarii Niejawnej w zakresie uprawnionego wejścia do

pokoju nr 20A oraz na okresowej i losowej kontroli pełnomocnika ochrony w zakresie uprawnionego wejścia do pokoju nr 20A.

Prowadzona jest papierowa ewidencja wydanych kluczy użytkowych i zapasowych do drzwi wejściowych do pokoju nr 20A i szafy metalowej w pokoju nr 20A, w której przechowywane jest stanowisko BSK. Klucze użytkowe przechowywane są w plombowanych woreczkach (każdy zestaw w oddzielnym woreczku) w metalowej kasetce zamykanej na klucz w pokoju nr 2A w piwnicy budynku „B" (miejsce pracy pełnomocnika ochrony). Klucz do kasetki z kluczami użytkowymi jest pod stałym nadzorem pełnomocnika ochrony. Pełnomocnik ochrony wydaje klucze użytkowe i prowadzi ewidencję wydanych kluczy użytkowych. Klucze zapasowe przechowywane są w plombowanych woreczkach (każdy zestaw w oddzielnym woreczku) w metalowej kasetce zamykanej na klucz w pokoju nr 4 w budynku „A" na parterze (miejsce pracy Sekretarza Gminy). Klucz do kasetki z kluczami zapasowymi jest pod stałym nadzorem Sekretarza Gminy. Sekretarz Gminy wydaje klucze zapasowe i prowadzi ewidencję wydanych kluczy zapasowych. Klucze użytkowe i zapasowe do pokoju nr 20A wydawane są tylko uprawnionym osobom na podstawie listy osób uprawnionych. Uprawnienia do pobierania kluczy nadaje pełnomocnik ochrony, który decyduje o dodaniu/wykreśleniu z listy osób uprawnionych do pobierania kluczy użytkowych i zapasowych. Prawo pobrania kluczy użytkowych i zapasowych do szafy metalowej, w której przechowywane jest stanowisko BSK w pokoju nr 20A posiada wyłącznie pracownik Kancelarii Niejawnej oraz pełnomocnik ochrony. Każda osoba pobierająca klucz, wpisuje się do ewidencji pobrań kluczy, która zawiera liczbę porządkową, datę i godzinę pobrania klucza, nr klucza, datę i godzinę zdania klucza, imię i nazwisko osoby pobierającej/zdającej, podpis, uwagi. Klucze zapasowe wydawane są tylko w wyjątkowych sytuacjach, m.in. zgubienie klucza użytkowego, uszkodzenie klucza użytkowego. Klucze zapasowe ma prawo pobrać również uprawniony członek komisji, na pisemne polecenie kierownika jednostki organizacyjnej, w celu komisyjnego otwarcia pomieszczenia nr 20A. Kontrolę w zakresie poprawności wpisów w książce ewidencji kluczy prowadzi pełnomocnik do spraw ochrony informacji niejawnych oraz inspektor bezpieczeństwa teleinformatycznego. Pomieszczenie nr 20A nie pozostaje nigdy bez nadzoru osoby uprawnionej, w przypadku opuszczenia pomieszczenia przez osobę uprawnioną, zamykane jest na klucz. Zabronione jest dorabianie kluczy do pomieszczenia nr 20A bez pisemnej zgody kierownika jednostki organizacyjnej. Zabronione jest pozostawianie kluczy do pomieszczenia nr 20A bez dozoru.

## XI. ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH

1. Udostępnianie pracownikowi informacji niejawnych oznaczonych klauzula „poufne" uwarunkowane jest posiadaniem właściwego i ważnego poświadczenia osobowego .

2. Udostępnianie informacji niejawnych oznaczonych klauzulą „zastrzeżone" określonej osobie może nastąpić w oparciu o ważne Poświadczenie Bezpieczeństwa lub pisemne upoważnienie kierownika jednostki - wzór upoważnienia stanowi załącznik do Planu Ochrony Informacji Niejawnych.

## XII. WYKONYWANIE DOKUMENTÓW NIEJAWNYCH Z WYKORZYSTANIEM SPRZETU KOMPUTEROWEGO

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.
3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada kierownik jednostki organizacyjnej, który w szczególności:
    - zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;
    - realizuje ochronę fizyczną, elektromagnetyczną systemu lub sieci.
    - zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej;
    - dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
    - zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
    - zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne”.
4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

- umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie ochronnej, zwanej równie „strefą kontrolowanego dostępu” w zależności od:
    a) klauzuli tajności,
    b) ilości,
    c) zagrożeń dla poufności, integralności lub dostępności- informacji niejawnych
- zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
    a) nieuprawnionym dostępem,
    b) podglądem,
    c) podsłuchem.

5. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.
    - Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.
    - Utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.
6. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych, lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.
7. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej

    1) kierownik jednostki organizacyjnej lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnie ń osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;

    2) administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a tak e zapewnia ich właściwe wykorzystanie.
8. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.
9. Systemy i sieci teleinformatyczne, w których maj ą być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.
10. Akredytacji udziela się na czas określony , nie dłuższy ni 5 lat.
11. Akredytacja, o której mowa następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.
12. ABW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

13. ABW udziela albo odmawia udzielenia akredytacji, o której mowa w pkt.12 , w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie.
14. Potwierdzeniem udzielenia przez ABW akredytacji, o której mowa w pkt. 13, jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.
15. Świadectwo, o którym mowa w pkt. 14, wydaje si ę na podstawie:
    1) zatwierdzonej przez ABW dokumentacji bezpieczeństwa systemu teleinformatycznego,
    2) wyników audytu bezpieczeństwa systemu teleinformatycznego prowadzonego przez ABW.
16. ABW może odstąpić od przeprowadzenia audytu bezpieczeństwa systemu teleinformatycznego, o którym mowa w pkt 15 ppkt 2, jeżeli system jest przeznaczony do przetwarzania informacji niejawnych o klauzuli „poufne".

17. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

18. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w pkt. 17, kierownik jednostki organizacyjnej przekazuje ABW dokumentację bezpieczeństwa systemu teleinformatycznego.
19. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zalecenia informuje ABW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.
20. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla

bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.

21. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW , bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
22. Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
23. Podstawą dokonywania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.
24. Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
25. Bez konieczności przeprowadzania badań i oceny Szef ABW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” urządzenia lub narzędzia kryptograficzne, jeżeli otrzymały stosowny certyfikat wydany przez krajową władzę bezpieczeństwa państwa będącego członkiem NATO lub Unii Europejskiej lub inny uprawniony organ w NATO lub w Unii Europejskiej.
26. Kierownik jednostki organizacyjnej wyznacza:

1) pracownika lub pracowników pionu ochrony pełniących funkcję **INSPEKTORA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO**, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;

2) osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych „**ADMINISTRATOREM SYSTEMU".**

27. W sytuacjach wymagających konsultacji lub uzgodnień kierownik jednostki może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zaleceń w zakresie bezpieczeństwa teleinformatycznego.

28. Stanowiska lub funkcje administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub pełnić osoby, posiadające poświadczenia bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemach lub sieciach teleinformatycznych, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez służby ochrony państwa.

29. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji Pełnomocnika ochrony informacji niejawnych.

**KOPIE ZAPASOWE:**

1. Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów niejawnych.
2. Sposób przechowywania zapasowych kopii jest identyczny jak przechowywanie dokumentów wykonanych w formie tradycyjnej (pismo), w przypadku gdy nośnikiem informacji jest materiał inny niż pismo, klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny sposób, bezpośrednio, a jeżeli jest to niemożliwe - na ich obudowie lub opakowaniu.

## XIII. GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym podziałem akt,

2. Dokumenty ostatecznie załatwione wymagają wszycia w teczkę pism, po zakończeniu roku kalendarzowego, klauzule niejawności teczek określa się według dokumentu o najwyższej klauzuli tajności,
3. Dokumenty niejawne o klauzuli „poufne" muszą być przechowywane w kancelarii niejawnej. W szczególnie uzasadnionych przypadkach dokumenty te mogą być przechowywane poza kancelarią, kierownik jednostki organizacyjnej lub inna upoważniona przez niego osoba mogą wyrazić pisemną zgodę na przechowywanie dokumentów poza pomieszczeniami kancelarii, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do tej klauzuli, na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów,
4. Dokumenty niejawne o klauzuli „zastrzeżone" są przechowywane w kancelarii niejawnej lub na stanowiskach pracy w meblach biurowych zamykanych na klucz.

## XIV. OZNACZENIE, NADAWANIE, ZMIANIA I ZNOSZENIE KLAUZULI NIEJAWNOŚCI MATERIAŁOM NIEJAWNYM

1. Materiał oznacza się klauzulą tajności w sposób wyraźny i w pełnym brzmieniu.
2. W przypadku gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności bądź gdy niektóre z tych części są jawne, wyodrębnione części oddziela się oznaczeniem odpowiedniej klauzuli tajności wskazanej w pełnym brzmieniu lub określeniem „jawne". Części materiału zawierające tekst lub obraz oddziela się przez odpowiednie ich oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu. 3. Jeżeli poszczególnym częściom materiału zostały nadane różne klauzule tajności, materiał oznacza się klauzulą tajności co najmniej równą najwyższej klauzuli tajności, jaką nadano części materiału.
3. Wprowadza się następujące symbole oznaczenia klauzul tajności:
   1) „00" — dla klauzuli „ściśle tajne";
   2) „0" — dla klauzuli „tajne";
   3) „Pf" — dla klauzuli „poufne";
   4) „Z" — dla klauzuli „zastrzeżone".
4. Dokument elektroniczny oznacza się w ten sposób, że jego metryka zawiera następujące informacje:
   1) klauzulę tajności;
   2) sygnaturę literowo-cyfrową, o której mowa w § 5 ust. 1 pkt 1 lit. c;
   3) nazwę jednostki lub komórki organizacyjnej;

4) datę rejestracji dokumentu;

5) w przypadku dokumentu, któremu nadano bieg korespondencyjny, wskazanie adresatów przez podanie imion i nazwisk lub nazw ich stanowisk;

6) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane;

7) stanowisko, imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do podpisania dokumentu;

8) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę;

9) nazwę nadaną dokumentowi lub określenie, czego dokument dotyczy.

5. Pełną nazwę klauzuli tajności nanosi się, o ile to możliwe, na dokumencie elektronicznym.
6. W przypadku dokumentu elektronicznego o klauzuli „zastrzeżone" § 5 ust. 2 stosuje się odpowiednio.
7. Na dokumencie nieelektronicznym można zamieścić dyspozycję dotyczącą:
   1) braku zgody na kopiowanie lub tłumaczenie części albo całości dokumentu;
   2) braku zgody na udzielanie informacji o treści dokumentu;
   3) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu.
8. W przypadku dokumentu elektronicznego dyspozycję, o której mowa w ust. 1, można zamieścić w jego metryce.
9. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych, na materiałach zawierających informacje niejawne można nanosić w sposób czytelny, widoczny i trwały dodatkowe oznaczenia, inne niż te, o których mowa w § 5—7.
10. Na dokumencie nieelektronicznym stanowiącym załącznik na pierwszej stronie umieszcza się dodatkowo informację: „Załącznik nr ... do dokumentu nr ... z dnia ...".
11. Jeżeli wraz z dokumentem przesyła się załączniki zawierające informacje niejawne, to:

    1) dokument oznacza się klauzulą tajności nie niższą niż najwyższa klauzula tajności załączników;

    2) na dokumencie — jeżeli po trwałym odłączeniu załączników dokument jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt 1 — na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności albo klauzuli tajności dokumentu po odłączeniu załączników.
12. W przypadku dokumentu elektronicznego informacje, o których mowa w ust. 1 i 2, umieszcza się odpowiednio w jego metryce.

13. Informację, o której mowa w ust. 1, umieszcza się, w miarę możliwości, na materiałach innych niż dokumenty.
14. Na materiałach innych niż dokumenty, o których mowa w § 5 i 6, klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, w szczególności na ich obudowie lub opakowaniu.
15. Materiał, który ze względu na organizację obiegu informacji niejawnych nie podlega rejestracji, oznacza się w sposób zapewniający jednoznaczną identyfikację jego klauzuli tajności, w szczególności przez jej umieszczenie na materiale.
16. Utrwalanie informacji niejawnych w formie dźwięku lub obrazu poprzedza się i kończy informacją o nadanej klauzuli tajności, o ile istnieją takie możliwości.
17. Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach klauzule tajności umieszcza się pośrodku, na górze i na dole zewnętrznych ścianek okładki oraz — jeżeli jest — na stronie tytułowej.
18. Zgody na zniesienie lub zmianę klauzuli tajności udziela się w odrębnym dokumencie podlegającym rejestracji lub przez oznaczenie w postaci umieszczenia informacji:
    1) na dokumencie — w przypadku dokumentu nieelektronicznego;
    2) w metryce dokumentu — w przypadku dokumentu elektronicznego.
19. Oznaczenia zniesienia klauzuli tajności na dokumencie nieelektronicznym utrwalonym w formie pisma dokonuje się następująco:
    1) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
    2) 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 dokonania czynności.
20. Oznaczenia zmiany klauzuli tajności na dokumencie, o którym mowa w ust. 1, dokonuje się następująco:
    1) skreśla się wszystkie dotychczasowe oznaczenia klauzuli tajności;
    2) nad skreślonymi oznaczeniami klauzul tajności umieszcza się oznaczenie nowej klauzuli tajności;
    3) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.

21. Skreśleń i adnotacji, o których mowa w ust. 1 i 2, dokonują: pracownik kancelarii tajnej, kierownik archiwum lub jego zastępca, kierownik innej niż kancelaria tajna komórki, w której są rejestrowane materiały niejawne, albo inne osoby upoważnione przez nich lub przez kierownika jednostki organizacyjnej.
22. Skreśleń i adnotacji, o których mowa w ust. 1 i 2, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.
23. Oznaczenie zmiany lub zniesienia klauzuli tajności dokumentu elektronicznego umieszcza się w jego metryce. W przypadku, o którym mowa w § 6 ust. 2, oznaczenie umieszcza się, o ile to możliwe, na dokumencie.
24. W przypadku materiałów, o których mowa w § 10 i 11, przepis § 13 stosuje się odpowiednio, z uwzględnieniem sposobu oznakowania tych materiałów.
25. Na dokumencie nieelektronicznym wytworzonym w wyniku kopiowania lub tłumaczenia umieszcza się:

    1) w przypadku kopii — na pierwszej stronie sygnaturę, o której mowa w § 5 ust. 1 pkt 1 lit. c;

    2) w pozostałych przypadkach — odpowiednio oznaczenia, o których mowa w § 5;

    3) na wszystkich stronach:

    a) w przypadku kopiowania napis „Wydruk", „Kopia", „Odpis", „Wyciąg" albo „Wypis",

    b) w przypadku tłumaczenia napis „Tłumaczenie z języka (nazwa języka)" oraz podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tłumaczenia;

    4) na ostatniej stronie w przypadku kopiowania dodatkowo potwierdzenie zgodności z oryginałem zawierające:

    a) napis „Za zgodność",

    b) odcisk pieczęci z nazwą jednostki lub komórki organizacyjnej, w której wytworzono dokument,

    c) podpis, imię i nazwisko lub inne oznaczenie wskazujące kierownika jednostki lub komórki organizacyjnej, w której dokonano kopiowania, albo osobę przez niego upoważnioną.
26. Wytworzenie dokumentu w wyniku kopiowania lub tłumaczenia dokumentu nieelektronicznego odnotowuje się na ostatniej stronie dokumentu kopiowanego lub tłumaczonego przez umieszczenie informacji o:

1) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;
2) liczbie egzemplarzy dokumentu wytworzonego;
3) dacie wytworzenia dokumentu;
4) numerze, pod jakim wytworzony dokument został zarejestrowany.

27. Informacje, o których mowa w ust. 2 pkt 1—3, umieszcza się przed wytworzeniem dokumentu w wyniku kopiowania lub tłumaczenia, natomiast numer, pod jakim został on zarejestrowany, umieszcza się po wytworzeniu.
28. W przypadku kopiowania lub tłumaczenia dokumentu elektronicznego informacje, o których mowa w ust. 2 pkt 1—4, umieszcza się w jego metryce.
29. W metryce dokumentu elektronicznego wytworzonego w wyniku kopiowania lub tłumaczenia umieszcza się:
    1) informacje, o których mowa w § 6;
    2) odpowiednio informację: „Odwzorowanie cyfrowe", „Kopia", „Odpis", „Wyciąg", „Wypis" albo „Tłumaczenie z języka (nazwa języka)";
    3) imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą kopiowania albo tłumaczenia.
30. W przypadku dokumentu o klauzuli „zastrzeżone" dopuszcza się odstąpienie od umieszczenia oznaczeń, o których mowa w ust. 1 pkt 3 i 4, ust. 2 i 4 oraz ust. 5 pkt 2 i 3.
31. W przypadku wytwarzania dokumentów w wyniku kopiowania lub tłumaczenia materiałów archiwalnych zgromadzonych w archiwach państwowych albo archiwach wyodrębnionych nie dokonuje się czynności, o których mowa w ust. 2, z tym że do materiałów archiwalnych dołącza się kartę informacyjną, na której każdorazowo umieszcza się informację o wytworzeniu dokumentów w wyniku kopiowania lub tłumaczenia, z uwzględnieniem informacji, o których mowa w ust. 2.
32. Materiały zawierające informacje niejawne wykorzystywane w urządzeniach lub systemach przeznaczonych do wykonywania czynności operacyjno-rozpoznawczych, w szczególności urządzenia, części urządzeń lub informatyczne nośniki danych, nie podlegają oznaczeniu w sposób określony w przepisach rozporządzenia.

## XV. ZASADY DOSTĘPU DO INFORMACJI NIEJAWNYCH

1. Informacje niejawne stanowiące oznaczone klauzulą „poufne" lub „zastrzeżone" mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności,
2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „poufne" może nastąpić:

- po przeprowadzeniu zwykłego postępowania sprawdzającego wobec kandydata do dostępu do tych informacji,
- po uzyskaniu przez daną osobę poświadczenia bezpieczeństwa ,
- po przeszkoleniu danej osoby w zakresie przepisów o ochronie informacji niejawnych i uzyskaniu właściwego zaświadczenia o przeszkoleniu.

3. Zwykłe postępowanie sprawdzające w związku z dostępem do informacji niejawnych o klauzuli „poufne" na pisemne polecenie kierownika jednostki organizacyjnej przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych ,
4. Osoba podlegająca postępowaniu sprawdzającemu zwykłemu zobowiązana jest do:

- wypełnienia określonej przepisami ankiety bezpieczeństwa osobowego, w sposób dokładny i zgodny z prawdą,
- odbyć szkolenie z zakresu znajomości przepisów ustawy o ochronie informacji niejawnych prowadzone przez Pełnomocnika .

5. Odmowa poddania się postępowaniu sprawdzającemu ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji niejawnych o klauzuli „poufne" może skutkować:

- przeniesieniem danej osoby na stanowisko nie związane z dostępem do informacji niejawnych,
- rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,
- niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się o zatrudnienie w Urzędzie.

6. Kierownik jednostki organizacyjnej może wyrazić w formie pisemnej zgodę na udostępnienie informacji niejawnych o klauzuli „poufne" osobie która jest zatrudniona lub wykonuje prace zlecone , wobec której wszczęto zwykłe postępowanie sprawdzające,
7. Kierownik jednostki organizacyjnej uzyskuje dostęp do informacji niejawnych oznaczonych klauzulą „poufne" po uzyskaniu Po świadczenia Bezpieczeństwa oraz uzyskaniu

zaświadczenia stwierdzającego odbycie szkolenia z zakresu przepisów ustawy o ochronie informacji niejawnych,

8. Postępowanie sprawdzające wobec kierownika jednostki , w przypadku potrzeby uzyskania uprawnień dostępu do informacji niejawnych oznaczonych klauzulą „poufne" przeprowadza Agencja Bezpieczeństwa Wewnętrznego,

9. Szkolenie kierownika jednostki w związku z przewidywanym dostępem do informacji niejawnych oznaczonych klauzulą „poufne" organizuje pełnomocnik ochrony wydając stosowne zaświadczenie,

10. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić:

- po uzyskaniu przez daną osobę upoważnienia nadanego przez kierownika jednostki ,
- po przeszkoleniu danej osoby w zakresie przepisów o ochronie informacji niejawnych i uzyskaniu właściwego zaświadczenia o przeszkoleniu.

## XVI. NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1. Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej,
2. Zadania określone ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 t. j.) w imieniu kierownika jednostki wykonuje pełnomocnik do spraw ochrony informacji niejawnych poprzez:
    a. sprawowanie nadzoru nad przestrzeganiem przepisów zawartych w Planie Ochrony Informacji Niejawnych,
    b. sprawowanie nadzoru w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnianiem do dostępu do tych informacji.

## XVII. ODPOWIEDZIALNOŚĆ KARNA, DYSCYPLINARNA I SŁUŻBOWA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

1. Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji został określony przepisami Kodeksu Karnego (Ustawa z dnia 6 czerwca 1997r.,Kodeks Karny, Dz.U. z dnia 2 sierpnia 1997 r.) w art. 266.

§1 Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową , podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2 Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.".

1. Wobec pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczania dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane sankcje służbowe i dyscyplinarne.

## XVIII. ARCHIWIZOWANIE, GROMADZENIE I NISZCZENIE MATERIAŁÓW NIEJAWNYCH.

1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w Rozporządzeniu Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych.(Dz. U. Nr 167, poz.1375,z dnia 9 października 2002 r.),
2. Zasady postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w rozporządzeniu Prezesa Rady Ministrów z dnia 26 lutego 2010 roku ( Dz. U. Nr 34 poz. 181),
3. Dokumentacja wytwarzana i gromadzona dzieli się na :

1) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;
2) dokumentację niearchiwalną - inną dokumentację, niestanowiącą materiałów archiwalnych.

4. Rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania, wytwarzanej i gromadzonej zawierają jednolite rzeczowe wykazy akt,
5. Wykazy akt o których mowa w stanowi ą podstawę gromadzenia dokumentacji w akta spraw.

6. Dokumentacja niearchiwalna, podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt.

7. Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę

8. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody.

9. Zgodę, o której mowa wyraża dyrektor miejscowo właściwego archiwum państwowego

10. Wniosek o wyrażenie zgody na brakowanie dokumentacji niearchiwalnej należy złożyć dyrektorowi miejscowo właściwego archiwum państwowego.

11. Do wniosku o zgodę jednorazową dołącza się:

1) protokół oceny dokumentacji niearchiwalnej,
2) spis dokumentacji niearchiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie, albo spis dokumentacji technicznej niearchiwalnej przeznaczonej na makulaturę lub zniszczenie,

12. Protokół oraz spis dokumentacji niearchiwalnej, sporządza komisja powołana przez kierownika jednostki, w której skład wchodzą: osoba kierująca lub prowadząca archiwum zakładowe albo składnicę akt oraz przedstawiciele komórek organizacyjnych, których dokumentacja niearchiwalna podlega brakowaniu oraz pracownika kancelarii niejawnej,

13. W przypadku trudności w ocenie brakowanej dokumentacji niearchiwalnej można zwrócić się do miejscowo właściwego archiwum państwowego o przeprowadzenie ekspertyzy.

14. Urząd przechowuje w archiwum zakładowym dokumenty brakowania, o których mowa wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokółami jej zniszczenia.

15. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu,

16. Materiały archiwalne powinny być ułożone wewnątrz teczek w kolejności spraw, a w ramach sprawy - chronologicznie, poczynając od pierwszego pisma wszczynającego sprawę. Poszczególne strony akt znajdujących się w teczce powinny być opatrzone kolejną numeracją.

**Opisanie materiałów archiwalnych polega na umieszczeniu na wierzchniej stronie każdej teczki:**

1) nazwy jednostki organizacyjnej i komórki organizacyjnej, w której materiały powstały;

2) znaku akt, to jest symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego według wykazu akt, obowiązującego w jednostce organizacyjnej;

3) tytułu teczki, to jest nazwy hasła klasyfikacyjnego według wykazu akt, obowiązującego w danej jednostce organizacyjnej, i informacji o rodzaju materiałów archiwalnych, znajdujących się w teczce;

4) rocznych dat krańcowych, to jest dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce;

5) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo-odbiorczym;

6) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A);

7) liczby stron w teczce.

17. Czynności związane z brakowaniem materiałów niearchiwalnych, wobec których archiwum państwowe wyraziło zgodę jest dokumentowany przez sporządzenie protokołu komisyjnego zniszczenia dokumentów niearchiwalnych.

18. Protokół komisyjnego zniszczenia materiałów niearchiwalnych sporządzany jest w dwóch egzemplarzach , z czego jeden egzemplarz należy przesłać do właściwego archiwum państwowego.

## XIX. PRZECHOWYWANIE KLUCZY I PIECZĘCI

Ustala się zasady gospodarki kluczami i pieczęciami:

1. Po zakończeniu pracy, pracownik materiałów niejawnych zamyka sejf oraz drzwi wejściowe kancelarii.
2. Klucze od sejfu oraz kancelarii niejawnej po zakończeniu pracy należy złożyć w Budynku B, w pomieszczeniu 2A, w plombowanym woreczku w metalowej kasetce zamykanej na klucz w miejscu niewidocznym.
3. Tworzy się zapasowy komplet kluczy od pomieszczeń kancelarii niejawnej.
4. Zapasowy komplet kluczy należy umieścić w zamykanym na klucz, metalowym pojemniku i plombowanym woreczku na klucze.

5. Tak przygotowany komplet kluczy zapasowych należy złożyć jednym z pomieszczeń Urzędu.
6. Pracownik kancelarii niejawnej po przybyciu do urzędu, przed otwarciem kancelarii powinien sprawdzić, czy nie zostały w żaden sposób naruszone zamki drzwi do kancelarii niejawnej oraz sejf znajdujący się w pomieszczeniu.

# ZAŁĄCZNIKI

DO PLANU OCHRONY INFORMACJI NIEJAWNYCH

**ZAŁĄCZNIK Nr 1 do Planu Ochrony Informacji Niejawnych-** *sposób oznaczania dokumentów niejawnych oznaczonych klauzulą poufne i zastrzeżone oraz umieszczenia klauzuli na tych dokumentach*

**Na każdej stronie umieszcza się:**

a) na środku, jako pierwszy element nagłówku strony, klauzulę tajności,

b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”,

c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany, i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy,

d) numer strony oraz liczbę stron całego dokumentu,

e) na środku jako ostatni element w stopce strony, klauzulę tajności;

**Na pierwszej stronie umieszcza się również:**

a) nazwę jednostki lub komórki organizacyjnej,

b) nazwę miejscowości i datę podpisania dokumentu,

c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”;

**Na ostatniej stronie pod treścią umieszcza się również:**

a) liczbę załączników,

b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,

c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane, oraz liczbę stron każdego załącznika kub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,

d) w przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat” – jeżeli załączniki mają być przekazane adresatowi

bez pozostawienia ich w aktach, lub napis „do zwrotu" – jeżeli załączniki mają zostać zwrócone nadawcy,

e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,

f) liczbę wykonanych egzemplarzy,

g) adresatów poszczególnych egzemplarzy dokumentu lub adnotację „adresaci według rozdzielnika",

h) dyspozycję „ad acta" w przypadku egzemplarza pozostającego w aktach nadawcy,

i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.

**W przypadku dokumentu, o którym mowa w ust. 1, o klauzuli „zastrzeżone" dopuszcza się odstąpienie od umieszczenia oznaczeń, o których mowa w ust. 1 pkt 1 lit. b oraz pkt 3 lit. f – i.**

*źródło: Rozporządzenie 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)*

**ZAŁĄCZNIK Nr 2 do Planu Ochrony Informacji Niejawnych**

# WZORY
# PISM I UPOWAŻNIEŃ

**SPIS TREŚCI**

# POŚWIADCZENIE BEZPIECZEŃSTWA NR_____

Na podstawie art. 28 pkt. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742) po przeprowadzeniu na wniosek/polecenie*

_____

*(nazwa wnioskodawcy albo stanowisko osoby , która poleciła przeprowadzenie postępowania*)*

przez_____

*(nazwa i adres siedziby organu , który przeprowadzi ł postępowanie)*

zwykłego/poszerzonego* postępowania sprawdzającego, stwierdza się, że Pani(Pan)

_____

*(imię i nazwisko, data urodzenia)*

**daje rękojmię zachowania tajemnicy**

w zakresie dostępu do informacji niejawnych oznaczonych klauzulą

_____ - na okres do: _____
(nazwa klauzuli tajności) (termin ważności)

_____ - na okres do:* _____
(nazwa klauzuli tajności) (termin ważności)*

_____ - na okres do:* _____
(nazwa klauzuli tajności) (termin ważności)*

_____

_____

(miejscowość i data) mp. (podpis i imienna pieczątka osoby upoważnionej)

**niepotrzebne skreślić*

# ZAŚWIADCZENIE NR__

## stwierdzające odbycie szkolenia
## w zakresie ochrony informacji niejawnych

Stwierdza się, że Pani (Pan):

- imię i nazwisko _____

- nr PESEL _____

odbyła (odbył) szkolenie w zakresie ochrony:

- informacji niejawnych,*****
- informacji niejawnych Organizacji Traktatu Północnoatlantyckiego,*****
- informacji niejawnych Unii Europejskiej,*****

na podstawie przepisów ustawy z dnia 5 sierpnia 201 0 r. o ochronie informacji

niejawnych (Dz.U. z 2019 r. poz. 742), zorganizowane przez pełnomocnika do

spraw ochrony informacji niejawnych w:

---

( nazwa i adres siedziby jednostki organizacyjnej)

.....

……

(miejscowość i data) (podpis i imienna pieczątka pełnomocnika lub jego zastępcy)

*****Niepotrzebne skreślić

……..

Miejscowość, data

……

Nazwa jednostki organizacyjnej

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

Na podstawie art. 21 ust. 4 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742) 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 wydane jest na okres:

- 

Dostęp do informacji niejawnych o klauzuli „zastrzeżone może nastąpić po odbyciu szkolenia w zakresie przepisów ustawy o ochronie informacji niejawnych

.....

Pieczątka i podpis kierownika jednostki organizacyjnej

Opracowała:

.....

Podpis i imienna pieczątka upoważnionej osoby

…….

Miejscowość i data

……

Nazwa jednostki organizacyjnej wnioskującej o przeprowadzenie poszerzonego postępowania sprawdzającego

L.dz. …….

**WYDZIAŁ ZAMIEJSCOWY W OLSZTYNIE**
**DELEGATURY ABW W BIAŁYMSTOKU**

Adres:
ul. Partyzantów 17
10-524 Olsztyn

**WNIOSEK O PRZEPROWADZENIE**

**POSZERZONEGO POSTĘPOWANIA SPRAWDZAJĄCEGO**

Na podstawie art. 23 ust. 2 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742) wnoszę o przeprowadzenie poszerzonego postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa, upoważniającego do dostępu do informacji niejawnych o klauzuli poufne, dla kandydata na pełnomocnika ochrony informacji niejawnych w Urzędzie Gminy Lubawa, wobec:

1. Imię
2. Nazwisko
3. Nr PESEL
4. Aktualne miejsce zatrudnienia
5. Miejsce zatrudnienia i stanowisko w nim zajmowane, z którym może łączyć się dostęp do informacji niejawnych[1]
6. Rodzaj umowy zatrudnienia w miejscu, o którym mowa w pkt 5[2]
7. Okres obowiązywania umowy zatrudnienia, o której mowa w pkt. 6[3]

[1] Miejsce i stanowisko pracy związane z dostępem do informacji niejawnych, które osoba sprawdzana ma zajmować po otrzymaniu poświadczenia bezpieczeństwa.
[2] W przypadku kandydata do pracy należy wpisać „kandydat".
[3] W przypadku umowy bezterminowej należy wpisać „na czas nieokreślony", umowy terminowej należy wpisać np. „na okres próbny od …. do ….", „na czas określony od ….. do ……".

……..

*Pieczątka i podpis kierownika jednostki organizacyjnej*
*lub osoby upoważnionej do obsady stanowiska lub zlecenia prac*

**Załącznik**:

Załącznik – tylko adresat – przekazana przez osobę sprawdzaną zaklejona koperta zawierająca wypełnioną ankietę bezpieczeństwa osobowego / wypełniona przez osobę sprawdzaną ankieta bezpieczeństwa osobowego**

* Należy wpisać odpowiednią klauzulę lub klauzule tajności

** Niepotrzebne skreślić

Miejscowość i data ……

……

Nazwa jednostki organizacyjnej

Pełnomocnik ds. Ochrony Informacji Niejawnych
w……

**POLECENIE WSZCZĘCIA ZWYKŁEGO POSTĘPOWANIA SPRAWDZAJĄCEGO**

Na podstawie art. 23 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742) polecam przeprowadzenie zwykłego postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa, upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą tajności „poufne" wobec:

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

……..

/*Pieczątka i podpis kierownika jednostki organizacyjnej/*

Miejscowość i data ……

**.....**

Nazwa jednostki organizacyjnej występującej o sprawdzenie
osoby upoważnianej do dostępu do informacji niejawnych

L.dz…….

**DYREKTOR**

**Delegatury Agencji Bezpieczeństwa**

**Wewnętrznego**

Wykaz adresów Delegatur ABW

znajduje się na stronie:

www.abw.gov.pl

**WNIOSEK O SPRAWDZENIE W EWIDENCJACH I KARTOTEKACH NIEDOSTĘPNYCH POWSZECHNIE**

Na podstawie art. 25 ust. 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) wykonując nałożone zadania w związku z przeprowadzanym zwykłym postępowaniem sprawdzającym wobec następującej osoby:

5. Nr PESEL
6. Nazwisko (w tym przybrane)
7. Imię (imiona)
8. Imię ojca
9. Imię matki
10. Nazwisko rodowe matki
11. Data urodzenia
12. Miejsce urodzenia
13. Adres zameldowania
14. Adres zamieszkania

proszę o poinformowanie, czy Agencja Bezpieczeństwa Wewnętrznego posiada informacje, które mają wpływ na wynik postępowania.

……..……..

Pieczątka i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

Miejscowość i data……

.....

nazwa jednostki organizacyjnej

L.dz…….

**Krajowy Rejestr Karny**
**Biuro Informacyjne**
Ul. Czerniakowska 100
00-454 Warszawa
lub
**Punkt Informacyjny**
**Krajowego Rejestru Karnego**
przy Sądzie Powszechnym

Na podstawie art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2019, poz. 1158 t.j.) oraz art. 25 ust. 1 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), w załączeniu przekazuję zapytanie, stanowiące załącznik nr 2 do rozporządzenia Ministra Sprawiedliwości z dnia 7 listopada 2003 r. w sprawie udzielenia informacji o osobach oraz o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym Rejestrze Karnym (Dz. U. z 2003, Nr 198, poz. 1930 z późn. zm.) dotyczący:

15. Imię (imiona)
16. Nazwisko (w tym przybrane)
17. Nr PESEL
18. Imię ojca

Zapytanie proszę odesłać na adres:……

……

*Pieczątka i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony*

**MINISTERSTWO SPRAWIEDLIWOŚCI**
**BIURO INFORMACYJNE**
**KRAJOWEGO REJESTRU KARNEGO**

Nazwa i adres podmiotu kierującego zapytanie oraz numer urządzenia służącego do automatycznego odbioru informacji

Data wpływu

miejsce na znaki opłaty sądowej*)

Data wystawienia .....

## ZAPYTANIE O UDZIELENIE INFORMACJI O OSOBIE**)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |

Numer PESEL

……..……

numer paszportu albo innego dokumentu stwierdzającego tożsamość***)

1. Nazwisko rodowe .....
2. Nazwisko (w tym przybrane) .....
3. Imiona .....
4. Imię ojca ..... 5. Imię matki .....
6. Data urodzenia …..... 7. Nazwisko rodowe matki .....
8. Miejsce urodzenia ..... 9. Obywatelstwo .....
10. Miejsce zamieszkania .....
11. Wskazanie postępowania, w związku z którym zachodzi potrzeba uzyskania informacji o osobie

    .....

    .....

12. Rodzaj danych, które mają być przedmiotem informacji o osobie:

    ❒1. Kartoteka karna

    ❒2. Kartoteka Nieletnich

    ❒3. Kartoteka Osób Pozbawionych Wolności oraz Poszukiwanych Listem Gończym**)

13. Zakres danych, które mają być przedmiotem informacji o osobie

.....
(podpis osoby uprawnionej)

Miejscowość i data……

……

nazwa jednostki organizacyjnej

**ZGODA NA UDOSTĘPNIENIE INFORMACJI NIEJAWNYCH O KLAUZULI „POUFNE" OSOBIE WOBEC KTÓREJ WSZCZĘTO POSTĘPOWANIE SPRAWDZAJĄCE ZWYKŁE**

Postępowanie sprawdzające zostało wszczęte w dniu ……

Na podstawie art. 34 ust. 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) wyrażam zgodę na udostępnienie informacji niejawnych oznaczonych klauzulą tajności „poufne" następującej osobie:

1. Imię (imiona)
2. Nazwisko (w tym przybrane)
3. Nr PESEL
4. Imię ojca
5. Imię matki
6. Nazwisko rodowe matki
7. Data urodzenia
8. Miejsce urodzenia

……..……

Pieczątka i podpis kierownika jednostki organizacyjnej

## KARTA INFORMACYJNA- DODATKOWE INFORMACJE

Zgodnie z art. 73 ust. 1 ustawy o ochronie informacji niejawnych, zwanej dalej „ustawą", Agencja Bezpieczeństwa Wewnętrznego prowadzi ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne" i wyższej oraz ewidencję osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa. Ewidencję te prowadzimy głównie w oparciu o dane przekazywane do ABW przez pełnomocników ochrony na podstawie art. 15 ust. 1 pkt 9 ustawy.

Dla tych celów wykorzystywana jest tzw. karta informacyjna, której wzór opracowano w Departamencie Ochrony Informacji Niejawnych ABW. Wypełnione karty pełnomocnicy przesyłają do DOIN, Delegatur ABW lub Wydziałów Zamiejscowych Delegatur ABW zgodnie z właściwością terytorialną.

Kierując się głównie względami praktycznymi rozszerzamy możliwości wypełniania przez Państwa ustawowych obowiązków wynikających z art. 15 ust. 1 pkt 9 ustawy.

Informacje niezbędne do prowadzenia ewidencji, o której mowa w art. 73 ust. 1 ustawy pełnomocnicy mogą przekazywać do ABW wybierając jeden z poniżej wskazanych sposobów:

1. Na dotychczasowych zasadach, wypełnioną i podpisaną kartę informacyjną (link do wzoru) przesyła się do Departamentu Ochrony Informacji Niejawnych, właściwej Delegatury ABW lub Wydziału Zamiejscowego Delegatur ABW - https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/organizacja-ochrony-in/145,dok.html#2a. Decyduje aktualne miejsce zamieszkania osoby, której dotyczy karta. W przypadku informacji na temat zakończonego postępowania sprawdzającego kartę należy przesłać do tej jednostki ABW, która dokonała sprawdzenia danej osoby w trybie art. 25 ust. 2 ustawy.

2. Wypełnioną i podpisaną kartę informacyjną można zeskanować i skan ten przesłać drogą elektroniczną na adres mailowy właściwej terytorialnie Delegatury ABW lub Wydziału Zamiejscowego Delegatury ABW – (link do adresów e-mail DABW) – lub w przypadku osób zamieszkałych w granicach administracyjnych m. st. Warszawy oraz następujących powiatów województwa mazowieckiego: grodziski, legionowski, miński, nowodworski, otwocki, piaseczyński, pruszkowski, pułtuski, warszawski zachodni, wołomiński, wyszkowski, sochaczewski, żyrardowski do Departamentu Ochrony Informacji Niejawnych ABW na adres

e-mail doin@abw.gov.pl Pełnomocnik otrzyma mailowo potwierdzenie wpłynięcia karty do ABW. Za zasadne uznaje się, aby zwrotny mail z ABW dołączyć do oryginału karty, jako potwierdzenie realizacji przez pełnomocnika ochrony ustawowego obowiązku. Zakres terytorialny Delegatur ABW oraz Wydziałów Zamiejscowych Delegatur ABW wygląda następująco:

- Delegatura ABW w Białymstoku – województwo podlaskie, z województwa mazowieckiego powiaty: makowski, ostrołęcki, ostrowski, sokołowski, węgrowski oraz miasto na prawach powiatu Ostrołęka, z województwa warmińsko – mazurskiego powiaty: ełcki, olecki, gołdapski;

    - Wydział Zamiejscowy w Olsztynie – z województwa warmińsko - mazurskiego powiaty: bartoszycki, braniewski, działdowski, giżycki, iławski, kętrzyński, lidzbarski, mrągowski, nidzicki, nowomiejski, olsztyński, ostródzki, piski, węgorzewski, szczycieński oraz miasto na prawach powiatu Olsztyn, z województwa mazowieckiego powiaty: ciechanowski, mławski, przasnyski, żuromiński;

*(miejscowość, data)*

# KARTA INFORMACYJNA

## A. NAZWA JEDNOSTKI ORGANIZACYJNEJ, W KTÓREJ SPORZĄDZONO KARTĘ

***Pełna nazwa jednostki organizacyjnej***

***Kraj*** | ***Województwo (lub inna główna jednostka podziału terytorialnego)*** | ***Kod pocztowy*** | ***Miejscowość***

***Ulica*** | ***Nr domu*** | ***Nr lokalu***

## B. DANE OSOBY, KTÓREJ DOTYCZY KARTA

***Nazwisko 1*** – ***Nazwisko 2*** | ***Imię 1*** | ***Imię 2***

***PESEL*** | ***Imię ojca*** | ***Data urodzenia (dzień, miesiąc, rok)*** | ***Miejsce urodzenia (miejscowość, kraj)***

## C. ADRES ZAMIESZKANIA LUB POBYTU

***Kraj*** | ***Województwo (lub inna główna jednostka podziału terytorialnego)*** | ***Kod pocztowy*** | ***Miejscowość***

***Ulica*** | ***Nr domu*** | ***Nr lokalu***

## D. MIEJSCE ZATRUDNIENIA

***Pełna nazwa jednostki organizacyjnej***

***Kraj*** | ***Województwo (lub inna główna jednostka podziału terytorialnego)*** | ***Kod pocztowy*** | ***Miejscowość***

***Ulica*** | ***Nr domu*** | ***Nr lokalu***

## E. MIEJSCE PODJĘCIA PRACY ZLECONEJ

***Pełna nazwa jednostki organizacyjnej***

***Kraj*** | ***Województwo (lub inna główna jednostka podziału terytorialnego)*** | ***Kod pocztowy*** | ***Miejscowość***

***Ulica*** | ***Nr domu*** | ***Nr lokalu***

## F. INFORMACJA NA TEMAT DOPUSZCZENIA BĄDŹ ODMOWY DOPUSZCZENIA DO INFORMACJI NIEJAWNYCH

***Sygnatura akt postępowania sprawdzającego**** | ***Nazwa dokumentu*****

***Nr dokumentu*** | ***Klauzula tajności*** | ***Data wydania (dzień, miesiąc, rok)*** | ***Data ważności (dzień, miesiąc, rok)***

Data wydania i nr poświadczenia bezpieczeństwa

pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

Data wydania i nr zaświadczenia o szkoleniu oin wydanym

pełnomocnikowi ochrony lub zastępcy pełnomocnika ochrony

*Imię i nazwisko Pełnomocnika ochrony albo Z-cy*
*Pełnomocnika ochrony*

- * Należy wypełnić, jeśli postępowanie zostało przeprowadzone
- ** Rodzaje dokumentów: „poświadczenie bezpieczeństwa”, „odmowa wydania poświadczenia”, „cofnięcie poświadczenia”, „zgoda na udostępnienie zgodnie z art. 34 ust. 9”

**ZAŁĄCZNIK Nr 3 do Planu Ochrony Informacji Niejawnych-** *protokół oceny dokumentacji niearchiwalnej*

.....

*(nazwa jednostki organizacyjnej)*

## PROTOKÓŁ OCENY DOKUMENTACJI NIEARCHIWALNEJ

Komisja w składzie:

.....
*imię i nazwisko, stanowisko*

.....
*imię i nazwisko, stanowisko*

.....
*imię i nazwisko, stanowisko*

dokonała oceny i wydzielenia przeznaczonej do przekazania na makulaturę lub zniszczenie dokumentacji niearchiwalnej w ilości .....mb i stwierdziła, że stanowi ona dokumentację niearchiwalną dla celów praktycznych jednostki organizacyjnej, oraz że upłynęły terminy jej przechowywania określone w jednolitym rzeczowym wykazie akt.

Przewodniczący komisji: .....

Członkowie komisji : .....

.....

.....

Załączniki:

.....kart spisu

.....pozycji spisu

**ZAŁĄCZNIK Nr 4 do Planu Ochrony Informacji Niejawnych-** *spis dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie*

.....

*nazwa i adres jednostki organizacyjnej*

**SPIS DOKUMENTACJI NIEARCHIWALNEJ**

**PRZEZNACZONEJ NA MAKULATURĘ LUB ZNISZCZENIE**

| L.p. | TYTUŁ TECZKI | SYMBOL Z WYKAZU RZECZOWEGO | DATY SKRAJNE | UWAGI |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**ZAŁĄCZNIK Nr 5 do Planu Ochrony Informacji Niejawnych-** *protokół komisyjnego zniszczenia dokumentów niearchiwalnych*

**PROTOKÓŁ**

**KOMISYJNEGO ZNISZCZENIA DOKUMENTÓW NIEARCHIWALNYCH**

W dniu ..... komisja w składzie:

1.Przewodniczący komisji.....

*(kierownik lub pracownik archiwum zakładowego)*

2. Członek komisji.....

*(przedstawiciel komórek org., których dokumenty s ą brakowane),*

3. Członek komisji.....

*(Pełnomocnik ochrony lub pracownik pionu ochrony),*

dokonała zniszczenia dokumentów niearchiwalnych, w oparciu o zgodę Archiwum Państwowego – pismo nr..... z dnia..... wydaną na podstawie Protokołu oceny dokumentacji niearchiwalnej oraz Spis dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie, pismo nr..... z dnia.....

Dokumenty zostały komisyjnie zniszczone w dniu..... przez (*spalenie, zmielenie itp*.)

**Podpisy członków komisji:**

1. *Przewodniczący komisji.....*
2. *Członek komisji.....*
3. *Członek komisji.....*

# OŚWIADCZENIE

**Oświadczam, że zapoznałem/zapoznałam się z Planem Ochrony Informacji Niejawnych w Urzędzie Gminy Lubawa oraz zobowiązuję się do przestrzegania jego postanowień.**

| L.p. | Imię i Nazwisko | Stanowisko | Podpis |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |
| 9. | | | |
| 10. | | | |
| 11. | | | |
| 12. | | | |
| 13. | | | |
| 14. | | | |
| 15. | | | |
| 16. | | | |
| 17. | | | |
| 18. | | | |
| 19. | | | |
| 20. | | | |

| | | | |
|---|---|---|---|
| **21.** | | | |
| **22.** | | | |
| **23.** | | | |
| **24.** | | | |
| **25.** | | | |
| **26.** | | | |
| **27.** | | | |
| **28.** | | | |
| **29.** | | | |
| **30.** | | | |
| **31.** | | | |
| **32.** | | | |
| **33.** | | | |
| **34.** | | | |