

ZARZĄDZENIE NR 44/24
WÓJTA GMINY BRUDZEŃ DUŻY
z dnia 18 grudnia 2024 roku

w sprawie: wprowadzenia dokumentacji dotyczącej ochrony informacji niejawnych w Urzędzie Gminy Brudzeń Duży.

Na podstawie art. 43 ust. 3-5 w związku z art. 15 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 z późn. zm.) oraz art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465 z późn. zm.) zarządza się, co następuje:

§ 1.

W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych w Urzędzie Gminy Brudzeń Duży wprowadzam:

- 1) **„PLAN OCHRONY INFORMACJI NIEJAWNYCH, w tym w razie wprowadzenia stanu nadzwyczajnego”**, stanowiący załącznik nr 1 do niniejszego zarządzenia,
- 2) **„INSTRUKCJĘ dot. SPOSOBU I TRYBU PRZETWARZANIA INFORMACJI NIEJAWNYCH o klauzuli „Zastrzeżone” i „Poufne” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony”** stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuje się wszystkich pracowników Urzędu Gminy Brudzeń Duży do zapoznania się z niniejszym zarządzeniem. Oświadczenie o zapoznaniu się należy potwierdzić własnoręcznym podpisem.

§ 3.

Wykonanie Zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych w Urzędzie Gminy Brudzeń Duży.

§ 4.

Traci moc wcześniejsze Zarządzenie nr 126/16 Wójta Gminy Brudzeń Duży z dnia 26 października 2016 r.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania tj. 18 grudnia 2024 roku.

Załącznik nr 1 do Zarządzenia 44/24
Wójta Gminy Brudzeń Duży
z dnia 18 grudnia 2024 r.

PLAN OCHRONY INFORMACJI NIEJAWNYCH

w tym w razie wprowadzenia stanu nadzwyczajnego

Nazwa i dane Jednostki organizacyjnej	
Nazwa	Urząd Gminy Brudzeń Duży
Adres	ul. Toruńska 2, 09-414 Brudzeń Duży
e - mail	sekretariat@brudzen.pl
Telefon	24 360 47 20

Dokument	
Podstawa prawna Akt wprowadzający	§ 9 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. 2012 r. poz. 683 ze zm.), Zarządzenie nr .../2024 Wójta Gminy ws. wprowadzenia dokumentacji dot. ochrony informacji niejawnych w Urzędzie Gminy Brudzeń Duży
Sporządził:	Pełnomocnik Ochrony Tadeusz Borowicki
Zatwierdził:	Wójt Gminy Brudzeń Duży Michał Twardy
data sporządzenia:	17 grudnia 2024 r.
data aktualizacji:	

Sporządził

17.12.2024 r.
data, podpis Pełnomocnika Ochrony

ZATWIERDZIŁ

.....
data, podpis Wójta Gminy Brudzeń Duży

SPIS TREŚCI

Wstęp	2
Definicje pojęć używanych w dokumencie	3
1. Klasyfikacja informacji niejawnych. Przedmiot ochrony w Urzędzie Gminy	4
2. Opis stref ochronnych, pomieszczeń i obszarów, w których przetwarzane są informacje niejawne, w tym określenie stosowanej do nich kontroli dostępu	5
3. Procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w obszarze przetwarzania informacji niejawnych	7
4. Ocena ryzyka zagrożeń i zastosowane środki bezpieczeństwa fizycznego	8
5. Procedury bezpieczeństwa dla obszaru przetwarzania informacji niejawnych	10
6. Polityka kluczy do pomieszczeń i szaf w obszarze przetwarzania informacji niejawnych	11
7. Procedury reagowania osób odpowiedzialnych za ochronę informacji niejawnych w przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych	12
8. Plany awaryjne ochrony informacji niejawnych w sytuacjach szczególnych, w tym zasady postępowania w razie wprowadzenia stanu nadzwyczajnego	13
9. Odpowiedzialność karna dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych	15
10. Okresy ochronne dla dokumentów niejawnych	15
11. Uwagi końcowe	15
Literatura	16
Załączniki	17 - 22

WSTĘP

Plan Ochrony Informacji Niejawnych w Urzędzie Gminy Brudzeń Duży opracowany został na podstawie wytycznych wynikających z art. 15 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych – zwanej dalej **Ustawą** (t.j. Dz. U. z 2024 r. poz. 632 ze zm.) i zawiera on wymagane dokumenty, 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 – zwanym dalej **Rozporządzeniem** (Dz. U. z 2012 r. poz. 683 z późn. zm.).

Wójt Gminy Brudzeń Duży dokłada wszelkich starań, aby przetwarzanie informacji niejawnych w Urzędzie odbywało się zgodnie z przepisami prawa. W trosce o ten stan rzeczy wprowadza się system ochrony informacji niejawnych, obejmujący m.in. środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności przetwarzanych informacji niejawnych.

Zgodnie z postanowieniami zawartymi w art. 15 ust.1 pkt 5 tejże Ustawy do jednego z zadań Pełnomocnika ds. Ochrony Informacji Niejawnych należy m.in. opracowywanie i aktualizowanie planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego akceptowanego przez Wójta (kierownika jednostki organizacyjnej) i nadzorowanie jego realizacji.

Niniejszy Plan Ochrony Informacji Niejawnych określa tryb i zasady postępowania z informacjami niejawnymi w Urzędzie Gminy Brudzeń Duży oraz zapewnia jednolity sposób postępowania z tymi informacjami.

Definicje używanych pojęć

Na użytek niniejszego dokumentu:

- **Ustawa** – oznacza ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 632 ze zm.)
- **Rozporządzenie** – oznacza Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r, poz. 683 z późn. zm.)
- **Rękojmia zachowania tajemnicy** – zdolność osoby do spełnienia ustawowych wymogów dla zabezpieczenia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem
- **IN** – oznacza informacje niejawne podlegające ochronie w procesie ich przetwarzania
- **Dokument** – każda utrwalona informacja niejawna
- **Materiał** – dokument lub przedmiot chroniony jako informacja niejawna
- **Przetwarzanie** [informacji niejawnych] – wszelkie operacje wykonywane na informacjach niejawnych, w szczególności: wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie
- **UG [Urząd]** – Urząd Gminy Brudzeń Duży, jednostkę pomocniczą Gminy (organu samorządu terytorialnego), o której mowa w art. 1 ust. 2 ustawy o ochronie informacji niejawnych
- **Wójt** – Wójt Gminy Brudzeń Duży
- **Pełnomocnik Ochrony** – Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy
- **Plan ochrony** – niniejszy Plan ochrony informacji niejawnych w Urzędzie Gminy

§ 1

Klasyfikacja informacji niejawnych. Przedmiot ochrony w UG.

Informacje niejawne są to dane o charakterze poufnym, których nieuprawnione ujawnienie jest zabronione, bowiem ich odtajnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne.

Adekwatnie do wagi poufności stosuje się klauzule tajności informacji niejawnych:

ŚCISLE TAJNE *ściśle tajne*, jeśli ich nieuprawnione ujawnienie spowoduje **wyjątkowo poważną szkodę** dla Rzeczypospolitej Polskiej przez to, że: zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;

TAJNE *tajne*, jeśli ich nieuprawnione ujawnienie spowoduje **poważną szkodę** dla Rzeczypospolitej Polskiej przez to, że: uniemożliwi realizację zadań związanych z ochroną suwerenności, lub porządku konstytucyjnego Rzeczypospolitej Polskiej;

POUFNE *poufne*, jeśli ich nieuprawnione ujawnienie spowoduje **szkodę** dla Rzeczypospolitej Polskiej przez to, że: utrudni prowadzenie bieżącej polityki zagranicznej RP;

ZASTRZEŻONE *zastrzeżone*, jeśli 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 Rzeczypospolitej Polskiej.

Przedmiotem ochrony w Urzędzie Gminy Brudzeń Duży są informacje niejawne z nadaną klauzulą „Zastrzeżone”, a także „Poufne” w rozumieniu Ustawy (przy czym założeniem jest, że informacje „Poufne” mogą wystąpić w UG potencjalnie i wyjątkowo, w zależności od sytuacji geopolitycznej) wraz z pomieszczeniem, w którym zabezpieczone i chronione są materiały niejawne, a także sposób przetwarzania i przechowywania tych informacji niejawnych.

Dostęp do informacji niejawnych w Urzędzie Gminy mogą mieć tylko osoby uprawnione, tj. które posiadają stosowne poświadczenie bezpieczeństwa do dostępu do informacji niejawnych albo otrzymały pisemne upoważnienie Wójta do informacji niejawnych wydane w oparciu o odbyte aktualne szkolenie z zakresu ochrony IN przeprowadzone przez Pełnomocnika Ochrony.

Osoby, którym nadano upoważnienie Wójta do dostępu do informacji niejawnych w ramach realizacji swych obowiązków służbowych, daje rękojmię zachowania tajemnicy.

Zgodnie z treścią art. 14 ust. 1 Ustawy, za ochronę informacji niejawnych, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony w jednostce organizacyjnej, w której są one przetwarzane, odpowiada Wójt Gminy Brudzeń Duży (jako kierownik jednostki).

Za zapewnienie przestrzegania przepisów dotyczących ochrony informacji niejawnych, a także przeprowadzania szkoleń w zakresie ochrony informacji niejawnych wśród osób zatrudnionych w Urzędzie Gminy Brudzeń Duży odpowiada Pełnomocnik ds. Ochrony Informacji Niejawnych, który służbowo podlega bezpośrednio Wójtowi Gminy Brudzeń Duży.

Bezpośredni nadzór nad realizacją zadań w procesie ochrony IN w Urzędzie sprawują kierownicy komórek organizacyjnych (referatów), a także osoba Inspektora ds. informatyzacji.

§ 2

Opis stref ochronnych, pomieszczeń i obszarów, w których przetwarzane są informacje niejawne, w tym określenie stosowanej do nich kontroli dostępu

1. Charakterystyka obiektu

Budynek, w którym znajduje się siedziba Urzędu Gminy Brudzeń Duży, znajduje się w Brudzeniu Dużym przy ul. Toruńskiej 2. Budynek jest II-kondygnacyjny i zawierający piwnicę. Właścicielem i administratorem budynku jest Gmina Brudzeń Duży.

Budynek jest objęty stałą całodobową ochroną (monitoringu) przez wyspecjalizowaną agencję „Solid Security” w Płocku (realizująca usługę za pomocą Centrum monitorowania alarmów).

Poszczególne kondygnacje budynku zajmowane są przez różne komórki organizacyjne Urzędu, zaś w piwnicy zorganizowany jest magazyn sprzętu OC oraz archiwum zakładowe. Przy budynku znajdują się miejsca postojowe samochodów pracowniczych i interesantów.

W sąsiedztwie ok. 15 m. przy parkingu znajduje się parterowy budynek Posterunku Policji w Brudzeniu Dużym Komendy Miejskiej Policji w Płocku.

2. Wydzielenie stref ochronnych

Ze względu na charakter instytucji publicznej, jaką jest Urząd Gminy Brudzeń Duży, interesanci mają swobodny dostęp z wejścia do budynku Urzędu do korytarzy i większości pokoi, będących miejscem ich obsługi, do których są zazwyczaj kierowani przy wejściu przez pracownika biura podawczego w sekretariacie UG.

Jednocześnie powierzchnie wspólne (korytarze) UG są objęte własnym systemem monitoringu wizyjnego w całym budynku.

Wszystkie pomieszczenia są zamykane na klucz. Część z nich jest zabezpieczana dodatkowo, do których należą serwerownia oraz pokój, w którym przetwarzane są informacje niejawne oraz zabezpieczone w szafie pancерnej, a w niej dodatkowo w kasecie metalowej.

W siedzibie UG funkcjonują strefy ochronne:

- **strefa ochronna III** – obszar korytarzy i pomieszczeń, w którym ruch jest kontrolowany przez całodobowy system monitoringu wizyjnego oraz w dzień przez urzędujących pracowników (*obszar ten pokrywa się ze strefą bezpieczeństwa przetwarzania danych osobowych*),
- **strefa ochronna II** – wydzielony pokój osoby funkcyjnej, będącego też miejscem pracy Pełnomocnika Ochrony, w którym są przetwarzane i przechowywane materiały niejawne „Zastrzeżone”, a także „Poufne” (zabezpieczone w szafie pancерnej), do którego wejście (ze strefy III) jest kontrolowane i do którego wstęp mają osoby tylko w obecności ww. osób w nim rezydujących.

Nie utworzono strefy ochronnej I (specjalnej strefy ochronnej), tj. obejmującej pomieszczenie kancelarii niejawnej z funkcjonującym elektronicznym systemem zabezpieczeń TI i systemem alarmowym i ciągłego monitoringu poddanym, gdyż nie ma takiej potrzeby.

3. Opis pomieszczenia przetwarzania IN

Pomieszczenie, w którym przetwarzane i przechowywane są materiały niejawne oznaczone klauzulą „Zastrzeżone” / „Poufne”, stanowiące strefę ochronną II, usytuowane jest w pokoju nr 6 na parterze UG. Miejszem przetwarzania IN jest wydzielona część pokoju wyposażona w szafę pancerną (wewnątrz której jest dodatkowo zamykana kasetka metalowa). Pomieszczenie to jest miejscem pracy Pełnomocnika Ochrony. Klucze do szafy pancernej oraz wewnętrznej kasety są przechowywane w ustalonym miejscu znanym Pełnomocnikowi i najwyższemu kierownictwu. Wstęp do miejsca przetwarzania IN istnieje podwójnie kontrolowany dostęp, bowiem pokój jest współużytkowany przez innego pracownika upoważnionego przez Wójta do dostępu do IN, który jednocześnie pełni rolę wzmocnionej kontroli dostępu (oprócz monitoringu) do miejsca przetwarzania IN oraz zapewnienia zamykania drzwi wejściowych do pokoju na klucz.

Materiały niejawne zabezpieczone są przed nieuprawnionym dostępem poprzez zastosowanie środków fizycznych i technicznych, tj. materiały o klauzuli „Zastrzeżone” są zamknięte w pokoju w szafie pancernej, zaś „Poufne” w zamkniętej kasecie metalowej wewnątrz tej szafy.

4. System kontroli dostępu do miejsca przetwarzania IN

Wszystkie funkcjonujące pomieszczenia w Urzędzie są zamykane na klucz, zaś korytarze są objęte całodobowym monitoringiem. Zgodnie z polityką kluczy stosowaną w Urzędzie Gminy (pobieranie i zdawanie kluczy) dostęp do pokoju nr 6 mają: Pełnomocnik Ochrony i pracownik uprawniony (stałe w pokoju rezydujący), a także Wójt Gminy z uprawnienia organu.

Wstęp do pomieszczenia, w którym przetwarzane są i przechowywane w szafie pancernej informacje niejawne, jest podwójnie kontrolowany i przebywanie w nim jest możliwe jedynie w obecności Pełnomocnika Ochrony lub współużytkującego pracownika UG.

Dzięki podwójnej kontroli dostępu oraz systemowi podwójnego zamykania dokumentów w szafie pancernej w pokoju nr 6, proces przetwarzania i przechowywanie informacji niejawnych w UG odbywa się w sposób bezpieczny w strefach ochronnych, przy tym:

- w przypadku dokumentów z klauzulą „Zastrzeżone” - **w strefie ochronnej II lub III** (czasowo)
- w przypadku dokumentów z klauzulą „Poufne” - **w strefie ochronnej II** (wyłącznie)

spełniając tym samym wymogi odpowiednio § 7 ust. 3 i 4 Rozporządzenia dla informacji „Zastrzeżonych” i „Poufnych”, stąd nie ma potrzeby wydzielania specjalnych stref ochronnych.

§ 3

Procedury zarządzania uprawnieniami do wejścia i przebywania w obszarze przetwarzania informacji niejawnych

Zgodnie z opisanymi wyżej strefami ochronnymi, dostęp do miejsca przetwarzania informacji niejawnych (pokój nr 6) jest zabezpieczony podwójnie (fizycznie i technicznie).

1. Uprawnienia stałego dostępu do pomieszczenia przetwarzania IN w obszarze ochronnym strefy II mają: Wójt Gminy, Pełnomocnik Ochrony oraz osoba w nim rezydująca (posiadająca upoważnienie Wójta Gminy do dostępu do informacji niejawnych o klauzuli „Poufne”).
2. Pozostali pracownicy Urzędu mogą przebywać w pomieszczeniu przetwarzania jedynie w celu i czasie przewidzianym na realizację swych zadań służbowych w towarzystwie wskazanych wyżej osób (posiadających uprawnienia stałego dostępu do pomieszczenia przetwarzania). Upoważnienia dostępu do IN o klauzuli „Zastrzeżone” posiada ok. 15% załogi (w przypadku dokumentów z klauzulą „Poufne” są to pojedyncze osoby funkcyjne i kierownictwo Urzędu).
3. W wyjątkowych przypadkach (uzasadnionych faktem pełnienia obowiązków służbowych) w obszarze ochronnym mogą przebywać tzw. goście, posiadający specjalne upoważnienia oraz poświadczenie bezpieczeństwa: pracownicy służb lub organów ścigania, kontrolerzy badający funkcjonowanie systemu ochrony informacji niejawnych, funkcjonariusze ABW.
4. Interesanci przybywający do UG są informowani i kierowani (przez pracownika sekretariatu) do miejsc odpowiednich dla załatwienia sprawy. Interesanci nie mogą być kierowani do miejsca przetwarzania IN bez uprzedzenia Pełnomocnika Ochrony lub osób uprawnionych do stałego dostępu do pomieszczenia przetwarzania. W sprawach dotyczących informacji niejawnych, o miejscu przyjęcia interesanta decyduje Pełnomocnik Ochrony.
5. Sprzątanie lub prace remontowe w pomieszczeniu przetwarzania może się odbywać jedynie w czasie i pod kontrolą osób uprawnionych do przebywania w pomieszczeniu. W tym czasie dokumenty niejawne są zabezpieczone w sposób opisany wyżej (zamknięte na klucz w szafie pancerniej oraz w kasecie wewnątrz niej) uniemożliwiający przypadkowe ujawnienie ich treści.

§ 4

Ocena ryzyka zagrożeń i zastosowane środki bezpieczeństwa fizycznego

Bezpieczeństwo materiałów niejawnych powinno być zapewnione zgodnie z zasadami:

- a) *poufności* – działania mające na celu zapewnienie ochrony IN a także ograniczenie zbędnego ich rozpowszechniania (dostęp do IN ograniczony do kręgu osób posiadających co najmniej stosowne upoważnienia i ukończone szkolenia)
- b) *integralności* – działania mające na celu zapewnienie, że IN nie zostanie zniekształcona (zachowa legalną postać oryginalną)
- c) *dostępności* – informacja musi być dostępna w założonym czasie dla osób upoważnionych
- d) *rozliczalności* – określenie odpowiedzialności za udostępnianie i przechowywanie IN oraz ustalenie aktualnego miejsca znajdowania się materiału niejawnego i kto się z nim zapoznał
- e) *autentyczności* – zapewnienie weryfikacji tożsamości osób, którym udostępniane są IN oraz zgodności z autentycznymi dokumentami uprawniającymi.

Dla zabezpieczenia informacji niejawnych i prawidłowego ich przetwarzania należy stosować środki bezpieczeństwa fizycznego odpowiednio do poziomu zagrożeń, aby uniemożliwić osobom nieuprawnionym dostęp do tychże informacji lub ich utratę.

W celu doboru właściwych środków bezpieczeństwa fizycznego została przeprowadzona analiza wszystkich istotnych czynników mających wpływ na bezpieczeństwo przetwarzania informacji „zastrzeżonych” w UG, w wyniku czego ustalony został **poziom zagrożeń**.

Określenie poziomu zagrożeń na podstawie analizy i oceny istotności czynników zagrożeń jest indywidualną oceną znaczenia następujących rodzajów zagrożeń:

- I. zagrożenia naturalne, których źródła nie leżą w zachowaniu człowieka (np. awarie)
- II. zagrożenia związane z umyślnym lub nieumyślnym działaniem człowieka.

Szczegółowa analiza wszystkich czynników mogących mieć wpływ na bezpieczeństwo IN przetwarzanych w UG zawiera się w cz. I odrębnego dokumentu niniejszego Planu ochrony „**Określenie poziomu zagrożeń i dobór środków bezpieczeństwa fizycznego**”, stanowiący Załącznik nr 1.

W wyniku tej oceny istotności czynników zagrożeń został określony **poziom zagrożeń 10 pkt** (w skali 7 – 16 pkt) dla warunków przetwarzania informacji „Zastrzeżonych” oraz „Poufnych” w Urzędzie Gminy Brudzeń Duży, czyli poziom zagrożeń o wartości **NISKI**.

Dla tak określonego poziomu zagrożeń zostały dobrane odpowiednie środki bezpieczeństwa fizycznego obejmujące podstawowe (oceniane punktami) kategorie „K” środków wymaganych dla danego poziomu zabezpieczeń w odniesieniu do danych klauzul tajności IN. Ocena dobranych zabezpieczeń w Urzędzie Gminy dla informacji niejawnych z klauzulą tajności „Poufne” (w tym „Zastrzeżone”) według wymaganych kategorii środków bezpieczeństwa jest wysoka i wynosi **17 pkt** (na wymóg minimalnego kryterium 11 pkt – dla IN „Poufnych”).

Szczegółowy dobór kategorii środków bezpieczeństwa fizycznego dla UG zawiera się w cz. II ww. Załącznika 1 „*Określenie poziomu zagrożeń i dobór środków bezpieczeństwa fizycznego*”.

Zapewnienie poufności, dostępności i integralności informacji niejawnych osiągnięto poprzez:

- zapewnienie właściwego przetwarzania informacji niejawnych
- umożliwienie zróżnicowania dostępu do IN dla pracowników zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebę dostępu do informacji chronionych
- wykrywanie i udaremnianie nieuprawnionych działań
- uniemożliwianie wtargnięcia osób nieuprawnionych (zarówno w sposób niezauważony, jak i z użyciem siły) do pomieszczenia, w którym przetwarzane są informacje niejawne.

W efekcie przeprowadzonych analiz i ocen ryzyka zagrożeń, została określona i zastosowana kombinacja kategorii środków zabezpieczeń fizycznych:

1. bariery fizyczne – istniejące środki chroniące granice miejsca przetwarzania informacji niejawnych, w szczególności: ściany, okna, drzwi;
2. stała kontrola dostępu do obszaru ochronnego - gwarantująca, że dostęp do pomieszczenia przetwarzania jest fizycznie możliwy tylko przez osoby posiadające stosowne uprawnienia;
3. osoby, którym powierzono przetwarzanie informacji niejawnych o klauzuli „Zastrzeżone” w strefie III, muszą posiadać upoważnienie kierownika jednostki w oparciu o odbyte szkolenie z zakresu ochrony IN;
4. osoby upoważnione i przebywające w pomieszczeniu przetwarzania informacji niejawnych o klauzuli „Poufne” w strefie II muszą posiadać rzeczywistą potrzebę uzyskania dostępu do informacji niejawnych;
5. szafy z zawartością dokumentów niejawnych „Zastrzeżonych” w strefie III muszą być zamknięte, szczególnie dokładnie zamknięte po zakończonej pracy, jak i zamknięty pokój;
6. budynek i znajdujące się w nim korytarze należące do siedziby UG podlegają ochronie poprzez funkcjonujący system monitoringu wizyjnego budynku Urzędu;

7. w uzasadnionych przypadkach (podyktowanych względami wymogu dłuższego okresu czasu do wykonania zadań w oparciu o dostęp do IN) dokumenty o klauzuli „Zastrzeżone” mogą być wydawane poza obszar ochronny II (do obszaru strefy III), pod warunkiem posiadania przez ich odbiorcę przedmiotowych uprawnień w zakresie IN oraz zapewnienia pełnej ochrony dokumentów poprzez bezpieczne ich przechowywanie w zamkniętych szafach.

§ 5

Procedury bezpieczeństwa dla obszaru przetwarzania informacji niejawnych

W Urzędzie Gminy przetwarza się informacje niejawne o klauzuli tajności „Zastrzeżone” oraz (w przypadkach wyjątkowych) „Poufne”. Miejszem ich przetwarzania co do zasady jest obszar wydzielony w pokoju nr 6, stanowiący siedzibę Pełnomocnika Ochrony, do którego dostęp jest kontrolowany i monitorowany (wyjątkiem może być czasowe wypożyczenie „zastrzeżonych”) . Materiały niejawne są przechowywane w miejscu przetwarzania w zamkniętych szafach.

1. Bieżący nadzór nad dostępem do miejsca przetwarzania ma Pełnomocnik Ochrony, a także pracownik współużytkujący pokój nr 6.
2. Stały dostęp do miejsca przetwarzania posiada ww. pracownik, Pełnomocnik Ochrony oraz Wójt Gminy. Inne osoby mogą w nim przebywać warunkowo, jedynie w obecności tychże wskazanych osób posiadających uprawnienie stałego dostępu.
3. W obszarze ochronnym podczas przetwarzania IN mogą przebywać wyłącznie:
 - i) osoby zatrudnione lub wykonujące zlecenia na rzecz UG, które posiadają uprawnienia dostępu do informacji niejawnych po odbyciu przedmiotowego szkolenia,
 - ii) inne osoby uprawnione specjalnie, jak: kontrolerzy wykonujący swe zadania służbowe, pracownicy służb lub organów ścigania – posiadający stosowne upoważnienia, w tym poświadczenia bezpieczeństwa.
4. Weryfikacji zewnętrznych upoważnień kontrolujących funkcjonariuszy dokonują Wójt Gminy i Pełnomocnik Ochrony.
5. Możliwe jest wypożyczenie dokumentów z klauzulą „Zastrzeżone” osobom upoważnionym do ich przetwarzania w swych pomieszczeniach strefy III. Fakt

wypożyczenia i zwrotu jest notowany (nazwa dokumentu, osoba wypożyczająca, czas wypożyczenia i czas zwrotu).

6. W przypadku formalnego wydania dokumentów pracownikom uprawnionym do przetwarzania IN w swych pomieszczeniach poza strefę II, Pełnomocnik Ochrony prowadzi bieżący nadzór nad tą pracą wraz z kontrolą sposobu zabezpieczenia chronionych dokumentów w pomieszczeniach.
7. Udostępnienie dokumentów osobom uprawnionym do zapoznania się następuje jedynie w tym zakresie, jaki jest przedmiotem kontroli oraz celu przetwarzania.
8. Wejścia do obszaru ochronnego są kontrolowane. Kontrolę przebywania osób w miejscu przetwarzania prowadzi Pełnomocnik Ochrony oraz pracownik współużytkujący pokój.
9. Nie jest możliwy wstęp do pomieszczenia, w którym przechowywane są dokumenty zawierające informacje niejawne, poza godzinami pracy Urzędu.
10. Sprzątanie w obszarze ochronnym odbywa się tylko po zakończeniu pracy z dokumentami niejawnymi. Oczywiście w czasie sprzątania materiały niejawne są zabezpieczone w szafie zamkniętej na klucz, nie może bowiem w żadnym przypadku dojść do choćby przypadkowego dostępu do informacji niejawnych.

§ 6

Polityka kluczy do pomieszczeń i szaf w obszarze przetwarzania informacji niejawnych

W Urzędzie Gminy nie ma portierów dyżurujących całą dobę, którzy pełniliby rolę ochrony pomieszczeń lub rolę zarządzających kluczami, za to funkcjonuje monitoring wizyjny.

Zgodnie z funkcjonującymi w Urzędzie zasadami *polityki kluczy*:

- Klucze do pomieszczeń biurowych przechowywane są w zamkniętej szafce objętej zasięgiem monitoringu i pod kontrolę dyżurującego pracownika Sekretariatu.
- Klucze zapasowe zamknięte są w osobnej szafce w innym zamkniętym pomieszczeniu
- Pobrania kluczy i otwarcia danych pomieszczeń urzędu dokonują upoważnieni pracownicy.
- Od momentu pobrania kluczy na osobach użytkujących pokoje (miejsce pracy) spoczywa pełna odpowiedzialność za ochronę tych pomieszczeń biurowych do zakończenia pracy (pracownicy ci są również odpowiedzialni za ochronę kluczy do biurek i szaf biurowych).
- Po zakończeniu pracy pomieszczenia są zamykane przez osobę opuszczającą pomieszczenie jako ostatnią. Pomieszczenia są zamykane na klucz, także przy każdym opuszczeniu go pustego w trakcie pracy (uniemożliwienie dostępu do danych osobom nieupoważnionym).
- Pomieszczenie stanowiące obszar ochronny II (miejsce pracy Pełnomocnika Ochrony - pokój współużytkowany przez uprawnionego pracownika), zamykane jest wyjątkowo

dbale, zaś klucze do szafy pancерnej i kasety metalowej są chowane w miejscu wiadomym jedynie Pełnomocnikowi Ochrony i kierownictwu Urzędu Gminy.

- Dla potrzeb czynności związanych ze sprzątaniami wykorzystywane są klucze do pokoi zdane przez pracowników po zakończeniu pracy. Osoby sprzątające przejmują klucze i po zakończeniu sprzątania chowają klucze do zamkniętej szafki metalowej objętej zasięgiem monitoringu.
- W obszarze ochronnym II sprzątanie odbywa się pod warunkiem, że w tym czasie materiały niejawnе są zamknięte w metalowej szafie.
- W razie utraty (zagubienia) kluczy do pomieszczeń i miejsc przechowywania dokumentów, należy niezwłocznie powiadomić o tym zdarzeniu Wójta Gminy i wymienić zamki.

§ 7

Procedury reagowania osób odpowiedzialnych za ochronę informacji w przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych

Za organizację systemu ochrony informacji niejawnych w Urzędzie odpowiada Wójt Gminy, jako kierownik jednostki.

Zadania określone ustawą o ochronie informacji niejawnych w imieniu Wójta Gminy wykonuje Pełnomocnik Ochrony, będąc osobą odpowiedzialną za przestrzeganie przepisów prawa oraz zasad systemu ochrony informacji niejawnych w UG.

Uwzględniając przypadki zagrożenia ochrony IN, działania Pełnomocnika Ochrony obejmują:

- Sprawowanie nadzoru nad przestrzeganiem przepisów prawa i realizacją zadań określonych w Planie Ochrony,
- Sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania zasad dostępu do tych informacji w odniesieniu do wszystkich komórek organizacyjnych UG.
- Pełnomocnik Ochrony przeprowadza kontrolę okresową z ewidencji materiałów i obiegu dokumentów, a w razie konieczności – kontrolę problemową, sporządzając protokół.

W razie ujawnienia informacji niejawnych przez podległych pracowników, upoważniona osoba zawiadamia na piśmie Pełnomocnika Ochrony, podając okoliczności i przyczyny ujawnienia informacji niejawnej (jakiej) lub jakie naruszenie przepisów nastąpiło.

- 1) Pełnomocnik Ochrony bez zbędnej zwłoki podejmuje działania zmierzające do wyjaśnienia przyczyn tego naruszenia, winnych temu osób i ograniczenia jego negatywnych skutków.
- 2) W przypadku stwierdzenia naruszenia przepisów o ochronie IN Pełnomocnik Ochrony przedkłada Wójtowi Gminy pisemną informację i wnioski do podjęcia decyzji.
- 3) Wobec pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych, dopuszczają się uchybień poprzez niewłaściwe zabezpieczenie dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym – mogą być zastosowane sankcje służbowe i dyscyplinarne.
- 4) Wójt Gminy określa stopień szkody z punktu widzenia interesu społecznego (lub stopień niebezpieczeństwa ujawnienia tajemnicy) i decyduje o ewentualnej karze dyscyplinarnej wobec osób winnych (i podejmuje decyzje, co do ewentualnie utraconych dokumentów).
- 5) Usytuowanie miejsca przetwarzania w strefie II z kontrolowanym wejściem do pokoju sprawia, że miejsce to jest stale kontrolowane. Pełnomocnik Ochrony użytkujący to miejsce ochrony (wraz z osobą współużytkującą ów pokój), swą obecnością sprawują stałą kontrolę obszaru ochronnego, by nie doszło do „wtargnięcia” doń osób nieuprawnionych podczas przetwarzania informacji niejawnych (osoby nieuprawnione lub interesanci są zapraszani w bezpieczne miejsce). W przypadku zauważenia śladów włamania do obszaru ochronnego podczas nieobecności Pełnomocnika Ochrony, zawiadamia się o tym fakcie Wójta Gminy i Pełnomocnika ochrony oraz właściwe służby ochrony państwa.

§ 8

Plany awaryjne ochrony informacji niejawnych w sytuacjach szczególnych, w tym zasady postępowania w razie wprowadzenia stanu nadzwyczajnego

W przypadku wprowadzenia stanu nadzwyczajnego istnieje szczególny obowiązek zabezpieczenia informacji niejawnych oznaczonych klauzulą „Zastrzeżone” oraz „Poufne” przetwarzanych w Urzędzie Gminy Brudzeń Duży.

Za stan nadzwyczajny w rozumieniu niniejszego dokumentu uważa się określone w art. 228 Konstytucji RP sytuacje: *stan wojenny*, *stan wyjątkowy* lub *stan klęski żywiołowej*. Każdy rodzaj stanu nadzwyczajnego może być wprowadzony tylko w drodze ustawy lub rozporządzenia, które podlegają dodatkowemu podaniu do publicznej wiadomości.

1. Plan ten określa zasady postępowania w sytuacji konieczności zabezpieczenia materiałów niejawnych w razie wprowadzenia stanu nadzwyczajnego. Zasady postępowania z materiałami zawierającymi informacje niejawne w czasie wystąpienia stanu nadzwyczajnego służą celowi zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych w UG.

2. Zabezpieczenie dokumentów niejawnych dokonuje się poprzez ich przeniesienie w inne bezpieczniejsze pomieszczenie, bądź ewakuowanie ich na zewnątrz w miejscu zapewniającym większe bezpieczeństwo w zaistniałej sytuacji zagrożenia, stosownie do występującego ryzyka.

3. Ewakuacja dokumentów następuje na podstawie pisemnego polecenia Wójta Gminy. Koordynatorem ewakuacji jest Pełnomocnik Ochrony. Merytoryczni pracownicy zobowiązani są na żądanie Pełnomocnika Ochrony do udzielenia natychmiastowej pomocy w zakresie: przeniesienia materiałów niejawnych oraz zabezpieczenia dokumentów po ewakuacji.

4. Za zabezpieczenie dokumentów o klauzuli „Zastrzeżone” znajdujących się w danym czasie na stanowiskach pracy odpowiada pracownik, który z uprawnienia jest jego użytkownikiem.

5. Ewakuacji materiałów niejawnych z zagrożonych pomieszczeń należy dokonać stosownie do stopnia i miejsca zagrożenia: korytarzami do głównego lub awaryjnego wyjścia z budynku albo przez okna przy bezwzględnym zagwarantowaniu bezpiecznego odbioru materiałów na zewnątrz budynku.

6. Miejsce zabezpieczenia materiałów niejawnych ustala osoba decydująca o ewakuacji. Nadzór i ochronę transportu do miejsca przechowywania sprawują osoby wyznaczone przez Wójta Gminy (w przypadku ewakuacji na zewnątrz np. Policja, jednostki innych służb).

7. Materiały niejawne po ewakuacji należy odpowiednio zabezpieczyć (oprócz zamknięcia pomieszczeń, ewentualne zaplombowanie i w miarę możliwości stały nadzór na nimi).

8. Przed ewakuacją sporządza się (jak jest to możliwe) spis dokumentów przeznaczonych do ewakuacji „E” lub do zniszczenia „Z” (jak Załącznik nr 2); jeden egzemplarz pozostaje w miejscu pracy, drugi – przewozi wraz z materiałami ewakuowanymi, przy czym: materiały niejawne z zakresu zadań obronnych w warunkach zagrożenia oraz te z ostatnich 5 lat należy oznaczyć symbolem „E”, zaś inne materiały starsze - oznaczyć symbolem „Z” i zniszczyć np. w niszczarce.

9. Ewakuacja obejmuje:

- I. Zapakowanie materiałów do worków (opakowań)
- II. Przeniesienie na środek transportu
- III. Przewiezienie do wyznaczonego miejsca ewakuacji.

10. Proces ewakuacji przewiduje dokonanie przez osobę podejmującą decyzję o ewakuacji następujących czynności:

- a) wydanie stosownych poleceń przez Wójta Gminy Pełnomocnikowi Ochrony oraz innym odpowiedzialnym pracownikom, a w razie gdy ewakuacja ma odbywać się w godzinach pozasłużbowych - zarządzenie wezwania osób odpowiedzialnych za pomocą wszelkich dostępnych środków,
- b) zapewnienie niezbędnego środka transportu oraz pracowników niezbędnych do zapakowania i przeniesienia materiałów przeznaczonych do ewakuacji.

11. W przypadku nieobecności Pełnomocnika Ochrony Wójt Gminy wyznacza dwuosobową komisję (spośród osób posiadających upoważnienia dostępu do IN) uprawnioną do wejścia oraz komisyjnego otwarcia pomieszczenia i szaf z materiałami niejawnymi, korzystając z kluczy zapasowych.

12. Komisja ta sporządza protokół z dokonanych czynności, który powinien zawierać:

- zasadność otwarcia pomieszczenia i mebli biurowych
- określenie ilości i rodzaju materiałów podlegających ewakuacji (E)
- określenie ilości i rodzaju materiałów nie podlegające ewakuacji (Z)
- określenie sposobu zabezpieczenia ewakuowanych materiałów w nowym miejscu
- wskazanie sposobu zabezpieczenia materiałów pozostających bez ewakuacji.

13. W przypadku, w którym Komisja pozostawiłaby w pomieszczeniu przetwarzania część materiałów niejawnych (stwierdzając brak potrzeby ich przenoszenia), jest zobowiązana je zabezpieczyć poprzez zamknięcie szaf i zaplombowanie pomieszczenia.

§ 9

Odpowiedzialność karna dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych

Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, zostały określone przepisami ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2024 r., poz. 17 z późn. zm.) w zakresie przepisów art. 266 - 269, wśród których w szczególności art. 266 § 2 stanowi:

„funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację 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”.

§ 10

Okresy ochronne dla dokumentów niejawnych

1. Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności.
2. Zniesienie lub zmiana klauzuli tajności jest możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, która nadała klauzulę tajności i jest uprawniona do podpisywania dokumentu.

§ 11

Uwagi końcowe

1. Z niniejszym Planem ochrony zostają zapoznani wszyscy pracownicy oraz osoby związane z pracą w Urzędzie Gminy Brudzeń Duży.
2. Na stanowiskach, w których przetwarzane są lub tymczasowo przechowywane są informacje niejawne, obowiązuje wymóg przestrzegania postanowień Planu ochrony.
3. W razie potrzeby i w sytuacjach przewidzianych przepisami ustawy Pełnomocnik Ochrony organizuje szkolenia w temacie ochrony informacji niejawnych.
4. Dopuszczenie do prac związanych z dostępem danej osoby do informacji niejawnych w UG może nastąpić po pisemnym upoważnieniu Wójta Gminy na podstawie odbytego szkolenia Pełnomocnika Ochrony, jeśli osoba ta nie posiada poświadczenia bezpieczeństwa.
5. Wzory zaświadczeń o odbyciu szkolenia w zakresie ochrony IN oraz upoważnień do dostępu do IN, o których mowa wyżej, ustalane są przepisami ustawy i rozporządzenia Rady Ministrów.
6. Plan ochrony podlega przeglądowi przynajmniej raz w roku w celu jego uaktualnienia lub dokonania zmian. Sporządzenia i przeglądy Planu ochrony dokonuje Pełnomocnik Ochrony. Przeglądy notuje się w tzw. Karcie przeglądów (wzór Karty stanowi załącznik nr 3).
7. Plan ochrony podlega zatwierdzeniu przez Wójta Gminy Brudzeń Duży.

Literatura

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 632 ze zm.)
2. 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)
3. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. 2017 r. poz. 1558)

4. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r, poz. 683 z późn. zm.)
5. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. nr 271 poz. 1603)
6. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U 2017 r. poz. 2334)
7. Rozporządzenie Prezesa Rady Ministrów z dnia 9 lipca 2020 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 2020 r. poz. 1256)
8. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. z 2015 r. poz. 220)
9. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. z 2010 r. nr 258 poz. 1753)
10. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. z 2010 r. poz. 1754)
11. Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2024 r. poz. 17 z późn. zm.)

*Załącznik 1
do „Planu ochrony informacji niejawnych”*

Określenie poziomu zagrożeń i dobór środków bezpieczeństwa fizycznego.

Część I. Określenie poziomu zagrożeń – analiza istotnych czynników ryzyka.

Tabela oceny istotności czynników zagrożeń w UG Brudzeń Duży						
Lp.	czynnik	Ocena czynnika			uzasadnienie	wskazówki
		bardzo istotny	istotny	mało istotny		

		(8 pkt)	(4 pkt)	(1 pkt)		
1.	Klauzula tajności informacji niejawnych		4		Czynnik średnio istotny, bowiem przetwarzane są tylko IN z klauzulą „zastrzeżone” („poufne” mogą być wyjątkowo)	<i>Ocena zagrożeń jest proporcjonalna do stopnia tajności informacji</i>
2.	Liczba materiałów niejawnych			1	W ewidencji jest mała ilość IN (dotąd w 2024 r. są same „zastrzeżone”)	<i>Ocena zagrożeń jest proporcjonalna do liczby wszystkich IN</i>
3.	Postać informacji niejawnych			1	Wszystkie dokumenty niejawne obecnie są w postaci papierowej (nieelektronicznej)	<i>Ocena zagrożeń jest proporcjonalna do ilości materiałów w formie elektronicznej</i>
4.	Liczba osób uprawnionych			1	Uprawnienia dostępu do informacji „zastrzeżone” ma niewielka liczba osób (ok. 15% załogi)	<i>Ocena istotności wprost proporcjonalna do liczby osób mających uprawnienia do IN</i>
5.	Lokalizacja obiektu i miejsca przetwarzania			1	Siedzibą UG jest cały budynek, który ma w sąsiedztwie parking i np. budynek Policji	<i>Ocena zagrożeń zależy od rodzaju sąsiedztwa budynku oraz od jego współużytkowników</i>
6.	Dostęp osób do budynku			1	Czynnik mało istotny - istnieje całodobowy monitoring budynku oraz korytarzy siedziby UG	<i>Ocena istotności proporcjonalna do stopnia tajności informacji</i>
7.	Inne czynniki *)			1	Na przestrzeni ostatnich 10 lat nie miały miejsca żadne włamania lub inne zdarzenia zagrażające bezpieczeństwu	<i>Inne czynniki mogące mieć istotny wpływ na bezpieczeństwo i ochronę informacji niejawnych w UG (włamania, losowe)</i>
	Suma punktów	10				

*) jeśli kierownik jednostki organizacyjnej uzna, że występują jeszcze inne czynniki mające istotny wpływ na zagrożenie ochrony IN, należy je określić i uzasadnić odpowiednio, oraz dokonać istotności tych czynników. Ocenie podlegają wszystkie czynniki łącznie.

Tabela poziomu zagrożeń dla IN w UG Brudzeń Duży		
NISKI	ŚREDNI	WYSOKI
7 – 16 pkt	17 – 32 pkt	pow. 32 pkt
10 pkt	← uzyskana ocena 10 pkt w UG określa NISKI poziom zagrożeń	

Część II. Kategorie środków bezpieczeństwa fizycznego – kryterium wymagań.

Punktacja wymagań wg kategorii środków bezpieczeństwa fizycznego				
Klauzula tajności (najwyższa) przetwarzanych informacji niejawnych	Wymagane kategorie Ki środków zabezpieczeń odp. do klauzul tajności	Minimalne kryterium oceny wymaganych zabezpieczeń dla poziomu zagrożeń:		
		Niski (min. pkt)	Średni (min. pkt)	Wysoki (min. pkt)
Ścisłe tajne	obowiązkowo kat. K1+K2+K3+K4+K5	16	18	20

	dodatkowo kat. K6	4	5	5
	Razem punktów	20	23	25
Tajne	obowiązkowo kat. K1+K2+K3+K4+K5	12	14	15
	dodatkowo kat. K6	4	5	5
	Razem punktów	16	19	20
Poufne	obowiązkowo kat. K1+K2+K3+K4+K5	8	11	12
	dodatkowo kat. K6	3	3	4
	Razem punktów	11	14	16
zastrzeżone	obowiązkowo kat. K1+K2+K3	2	2	2
	dodatkowo kat. K4 lub K5 lub K6	-	1	2
	Razem punktów	2	3	4

Legenda:

K1 – Szafy do przechowywania IN (*w szczególności*: S1 konstrukcja/rodzaj szafy, S2 jakość zamka)

np. S1: szafa stalowa spełniająca PN-EN 14450 – 3 pkt (tajne), .. S1: szafa drewniana biurowa – 1 pkt,
S2: zamki odporne na włamania specjalistów – 3 pkt (tajne), .. S2: zamek zwykły – 1 pkt (zastrzeżone)

K2 – Pomieszczenia przetwarzania, kancelaria (S1 konstrukcja pokoi, S2 zamek drzwi wejścia)

np. S1: konstrukcje pokoi odporne na włamania – 2 pkt (tajne), .. S1: typowe pomieszczenie – 1 pkt,
S2: zamki odporne na włamania specjalistów – 2 pkt (tajne), .. S2: zamek zwykły – 1 pkt (zastrzeżone)

K3 – Budynki - konstrukcja (zazwyczaj murowany – 2 pkt)

K4 – Kontrola dostępu (S1 zabezpieczenia wejścia, S2 kontrola wewnętrzna)

np. S1: system oparty na stale zamkniętych drzwiach z zamkiem szyfrowym – 1 pkt (tajne)
S2: goście poruszają się po obiekcie pod nadzorem uprawnionego pracownika firmy – 3 pkt (tajne)

K5 – Personel bezpieczeństwa (S1 agencja ochrony, S2 systemy sygnalizacji włamań i napadu)

np. S1: zatrudnienie agencji ochrony patrolującej teren firmy z zewnątrz i z reagowaniem na sygnały alarmowe systemu SSWiN poprzez wysłanie patrolu interwencyjnego – 1 pkt (tajne)
S2: zastosowany system SSWiN spełnia dodatkowo wymagania na poziomie 2 – 2 pkt (tajne)

K6 – Granice terenu obiektu (S1 ogrodzenie, S2 i S3 systemy kontroli osób przy wejściu/wyjściu, S4 system wykrywania naruszeń ogrodzenia, S5 oświetlenie obszaru, S6 dozór wizyjny)

Dobór środków bezpieczeństwa fizycznego dla IN „zastrzeżone” w UG		
Lp.	Kategorie K_i wymaganych środków bezpieczeństwa S_i	Pkt
1.	K1 Szafy do przechowywania materiałów niejawnych <i>Środek bezpieczeństwa K1S1: szafa pancerna</i>	3

	<i>Środek bezpieczeństwa K1S2: zamykana na zamek certyfikowany</i>	3
	Liczba punktów K1 = K1S1 x K1S2	9
2.	K2 Pomieszczenie do przetwarzania informacji niejawnych	
	<i>Środek bezpieczeństwa K2S1: murowane, wydzielona strefa II</i>	1
	<i>Środek bezpieczeństwa K2S2: zamek drzwi typowy</i>	1
	Liczba punktów K2 = K2S1 x K2S2	1
3.	K3 Budynek stanowiący siedzibę UG	
	<i>Konstrukcja budynku K3: murowany</i>	2
	Liczba punktów K3	2
4.	K4 Kontrola dostępu do pomieszczenia przetwarzania	
	<i>Środek bezpieczeństwa K4S1: brak szyfrowego systemu kontroli</i>	0
	<i>Środek bezpieczeństwa K4S2: wejście kontrolowane</i>	1
	Liczba punktów K4 = K4S1 + K4S2	1
5.	K5 Personel bezpieczeństwa - ochrona siedziby UG	
	<i>Środek bezpieczeństwa K5S1: agencja ochrony</i>	1
	<i>Środek bezpieczeństwa K5S2: system sygnalizacji włamań</i>	1
	Liczba punktów K5 = K5S1 + K5S2	2
6.	K6 Granice obiektu z budynkiem siedziby UG	
	<i>Środek bezpieczeństwa K6S1: brak ogrodzenia obiektu</i>	0
	<i>Środek bezpieczeństwa K6S2: brak kontroli we/wy</i>	0
	<i>Środek bezpieczeństwa K6S3: brak systemu kontroli we/wy</i>	0
	<i>Środek bezpieczeństwa K6S4: brak systemu naruszenia ogrodzenia</i>	0
	<i>Środek bezpieczeństwa K6S5: oświetlenie terenu wokół budynku</i>	1
	<i>Środek bezpieczeństwa K6S6: monitoring wizyjny w budynku</i>	1
	Liczba punktów K6 = K6S1 + K6S2	2
Ogólna liczba punktów za wszystkie kategorie:		17

Załącznik 2
do „Planu ochrony informacji niejawnych”

Wykaz dokumentów zawierających informacje niejawne oznaczonych klauzulą „Zastrzeżone” oraz „Poufnych” przechowywanych w Urzędzie Gminy Brudzeń Duży dla celów ewakuacji z dnia

L.p.	Nazwa dokumentu	Nr ewidencyjny	Ilość stron	Oznaczenie E v Z	Uwagi
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					

*Załącznik 3
do „Planu ochrony informacji niejawnych”*

Karta przeglądów i zmian Planu ochrony informacji niejawnych w UG

L.p.	Data przeglądu lub zmian	Uwagi do zakresu aktualizacji lub zmian	Osoba dokonująca przeglądu Planu	Podpis
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Załącznik nr 2 do Zarządzenia 44/24
Wójta Gminy Brudzeń Duży
z dnia 18 grudnia 2024 r.

INSTRUKCJA

dot. SPOSOBU I TRYBU PRZETWARZANIA INFORMACJI NIEJAWNYCH
o klauzuli „Zastrzeżone” i „Poufne” w podległych komórkach organizacyjnych
oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony

Nazwa i dane Jednostki organizacyjnej	
Nazwa	Urząd Gminy Brudzeń Duży
Adres	ul. Toruńska 2, 09-414 Brudzeń Duży
e - mail	sekretariat@brudzen.pl
Telefon	24 360 47 20

Dokument	
Podstawa prawna Akt wprowadzający	Art. 43 ust. 4 i 5 Ustawy z dnia 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. 2024 r. poz. 632 z późn. zm.) Zarządzenie nr .../2024 Wójta Gminy ws. wprowadzenia dokumentacji dot. ochrony informacji niejawnych w Urzędzie Gminy Brudzeń Duży
Sporządził:	Pełnomocnik Ochrony IN Tadeusz Borowicki
Zatwierdził:	Wójta Gminy Brudzeń duży Michał Twardy
data sporządzenia:	17 grudnia 2024 r.
data aktualizacji:	

Sporządził

17.12.2024 r.
data, podpis Pełnomocnika Ochrony

ZATWIERDZIŁ

.....
data, podpis Wójta Gminy Brudzeń Duży

SPIS TREŚCI

Definicje pojęć używanych w dokumencie	3
I. Zasady i warunki przetwarzania informacji niejawnych	4
II. Zasady ochrony fizycznej dokumentów zawierających informacje niejawne	6
III. Zasady ewidencjonowania, przekazywania, kompletowania i niszczenia dokumentów	8
IV. Postępowanie w przypadkach naruszenia zasad ochrony lub ujawnienia informacji niejawnych	9
Literatura	10

Definicje pojęć

Na użytek niniejszego dokumentu:

- **Ustawa** – oznacza ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024r. poz. 632 z późn. zm.)
- **Rozporządzenie** – oznacza rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r, poz. 683 z późn. zm.)
- **Rękojmia zachowania tajemnicy** – zdolność osoby do spełnienia ustawowych wymogów dla zabezpieczenia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem
- **IN** – oznacza informacje niejawne podlegające ochronie w procesie ich przetwarzania
- **Dokument** – każda utrwalona informacja niejawna
- **Materiał** – dokument lub przedmiot chroniony jako informacja niejawna
- **Przetwarzanie** [informacji niejawnych] – wszelkie operacje wykonywane na informacjach niejawnych, w szczególności: wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie
- **Wykonawca** – pracownik zajmujący określone stanowisko służbowe, wykonujący swe zadania zgodnie z zakresem obowiązków, w tym przetwarzania informacji niejawnych, który posiada poświadczenie bezpieczeństwa osobowego do dostępu do informacji niejawnych z odpowiednią klauzulą tajności lub stosowne upoważnienie Wójta wraz z przeszkoleniem przez Pełnomocnika Ochrony w zakresie ochrony informacji niejawnych
- **UG [Urząd]** – Urząd Gminy Brudzeń Duży, jednostkę pomocniczą Gminy (organu samorządu terytorialnego), o której mowa w art. 1 ust. 2 ustawy o ochronie informacji niejawnych
- **Wójt** – Wójt Gminy Brudzeń Duży
- **Pełnomocnik Ochrony** – Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie
- **Plan ochrony** – Plan ochrony informacji niejawnych w Urzędzie Gminy
- **Instrukcja przetwarzania** – niniejsza Instrukcja dot. sposobu i trybu przetwarzania IN „Zastrzeżone” (ewentualnie „Poufnych”) w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony
- **Strefa ochronna III** – obszar korytarzy i pomieszczeń, w którym ruch jest kontrolowany przez system monitoringu i urzędujących pracowników UG,
- **Strefa ochronna II** – wydzielone pomieszczenie w Urzędzie, w którym przechowywane są materiały niejawne oznaczone klauzulą „Zastrzeżone” i „Poufne”, stanowiące miejsce pracy Pełnomocnika Ochrony, poddane szczególnej kontroli wejść i przebywania.

I. Zasady i warunki przetwarzania informacji niejawnych

1. W Urzędzie Gminy Brudzeń Duży przetwarzane są informacje niejawne oznaczone klauzulą „Zastrzeżone” w rozumieniu Ustawy, przy czym założyć trzeba, że Gmina (jako Organ) może również przetwarzać informacje „Poufne”, które mogą się pojawiać w zależności od sytuacji geopolitycznej.
 2. Klauzulę „Zastrzeżone” nadaje się informacjom niejawnym, jeśli 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 RP.
 3. Klauzulę „Poufne” nadaje się informacjom niejawnym, jeśli ich nieuprawnione ujawnienie spowoduje szkodę dla RP przez to, że:
 - utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
 - utrudni realizację przedsięwzięć obronnych;
 - zakłóci porządek publiczny i zagrazi bezpieczeństwu obywateli lub utrudni wykonywanie zadań służbom odpowiedzialnym za ściganie sprawców;
 - wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.
 4. Dokumenty opatrzone klauzulą „Zastrzeżone” oraz „Poufne” oznacza się zgodnie z zasadami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności – odp. „Z” lub „Pf”.
 5. Klauzulę informacjom niejawnym przyznaje kierownik jednostki lub uprawnione przez niego osoby, które są upoważnione do podpisywania dokumentu lub oznaczania innego materiału.
 6. Uprawnienia dostępu do informacji niejawnych w Urzędzie posiadają osoby, które mają:
 - stosowne poświadczenie bezpieczeństwa do dostępu do informacji niejawnych, lub
 - pisemne upoważnienie Wójta przy warunku posiadanego aktualnego zaświadczenia o odbytych przeszkoleniu z zakresu ochrony IN prowadzonym przez Pełnomocnika Ochrony.
 7. Informacje niejawne z klauzulą „Zastrzeżone” / „Poufne” w UG są przetwarzane przez osoby uprawnione jedynie w celu wykorzystania ich w zakresie niezbędnym do wykonywania przedmiotowych obowiązków służbowych na swoich stanowiskach służbowych. Pracownicy ci wykonują swe obowiązki tylko w obszarze odpowiednio strefy III (*informacje zastrzeżone*) lub w strefie II (*informacje poufne*).
1. Osoby, które zapoznały się z informacjami niejawnymi są zobowiązane do:
 - a) nie ujawniania ich osobom nieuprawnionym w każdym czasie (ani prowadzenia o ich treści rozmów), także po rozwiązaniu umowy o pracę lub po przejściu na emeryturę;
 - b) nie wykorzystywania informacji niejawnych (przetwarzanych w Urzędzie) w publikacjach,

- na wykładach i innych wystąpieniach publicznych;
- c) powiadamiania swych przełożonych lub Pełnomocnika Ochrony o wszelkich przypadkach naruszenia przepisów o ochronie IN w związku z wykonywaniem swych obowiązków.
8. Dokumenty niejawne, wpływające do UG w korespondencji przychodzącej, są kierowane przez Wójta lub Sekretarza Gminy do Pełnomocnika Ochrony, gdzie podlegają ewidencjonowaniu w Dzienniku ewidencji oraz dalszej realizacji.
Pełnomocnik Ochrony przekazuje lub udostępnia je do dalszego wykonania zgodnie z zawartą w dokumencie treścią przeznaczenia - odpowiednio do klauzuli „Poufne” lub „Zastrzeżone”.
 9. Każdorazowe przekazanie lub udostępnienie dokumentu musi być odpowiednio wpisane do Dziennika ewidencyjnego IN z adnotacją dot. zdarzeń pobrania i zwrotu danego dokumentu.
 10. System obiegu dokumentów zapewnia możliwość ustalenia (w każdych okolicznościach) gdzie znajduje się materiał zawierający informacje niejawne pozostający w dyspozycji Urzędu oraz kto z tym materiałem się zapoznał.
 11. Prowadzi się dwa wykazy: dokumentów wytworzonych w Urzędzie z nadaną klauzulą tajności „Zastrzeżone” i dokumentów przychodzących oznaczonych daną klauzulą tajności. Dopuszcza się jeden rejestr dla dokumentów niejawnych otrzymywanych i wysyłanych.
 12. Informacje niejawne o klauzuli „Zastrzeżone” mogą być przetwarzane w miejscach o strefie ochronnej III zaś stale przechowywane w strefie II w sposób uniemożliwiający ich ujawnienie. Dokumenty zawierające informacje o klauzuli „Poufne” mogą być przetwarzane i przechowywane wyłącznie w strefie ochronnej II.
 13. Wykonanie kopii, odpisu, wypisu lub wyciągu dokumentu o klauzuli „Zastrzeżone” lub „Poufne” może nastąpić za zgodą Wójta Gminy lub Pełnomocnika Ochrony, o ile Wykonawca dokumentu nie dokonał jasnego doń zastrzeżenia. Za zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza Wójt Gminy.
Oznaczanie kopii, odpisów, wypisów i wyciągów dokumentów niejawnych oraz zasady ich ewidencjonowania określono w rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.
 14. Przetwarzanie IN w Urzędzie dokonuje się bez wykorzystania systemu teleinformatycznego.
 15. Wykonanie kopii dokumentów niejawnych winno być wykonywane tylko na wskazanej kserokopiarce uzgodnionej z kierownikiem jednostki (przy zapewnieniu ochrony treści przed ujawnieniem osobom nieuprawnionym) i tylko przez osobę do tego uprawnioną.
 16. Dokumenty niejawne mogą być wykonywane metodą ręcznego pisania, zaś w razie konieczności wykonania dokumentu zawierającego informacje niejawne „Zastrzeżone” z pomocą komputera musi się odbywać z zabezpieczeniem dysku/katalogu hasłem w ochronie przed nieuprawnionym doń dostępem osób nieupoważnionych.
 17. Liczbę wytwarzanych dokumentów „Zastrzeżonych” oraz zasięg ich obiegu ogranicza się do minimum niezbędnego dla realizacji zadań służbowych, wykorzystując (w miarę, na ile to

możliwe) inne możliwości załatwienia sprawy. Dokumenty niejawne należy sporządzać w ściśle określonej liczbie egzemplarzy.

II. Zasady ochrony fizycznej dokumentów zawierających informacje niejawne oznaczonych klauzulą „Zastrzeżone” lub „Poufne”

1. Dokumenty oznaczone klauzulą „Poufne” przechowuje się w kasecie metalowej wewnątrz szafy pancernej tylko u Pełnomocnika Ochrony w strefie ochronnej II. Dokumenty z klauzulą „Zastrzeżone” - w szafie pancernej u Pełnomocnika Ochrony, przy czym czasowo mogą być przechowywane także w zamkniętych szafach biurowych w pomieszczeniach służbowych Wykonawców zlokalizowanych w strefie ochronnej III.
2. Dokumenty i materiały niejawne oraz dokumenty jawne co do zasady należy przechowywać oddzielnie, jednakże z zastrzeżeniem niżej pkt 3.
3. Materiały oznaczone danymi klauzulami tajności i materiały jawne, które dotyczą jednej i tej samej sprawy, mogą być przechowywane wspólnie.
4. Odpowiedzialność za otrzymany materiał niejawny oznaczony klauzulą „Zastrzeżone” ponosi Wykonawca, który go otrzymał. Wykonawca może, jeśli wynika to z jego kompetencji, udostępnić robocze dokumenty niejawne osobie z innej komórki Urzędu, spełniającym ustawowe wymagania dostępu do tychże informacji niejawnych.
5. Każdorazowo, po zakończeniu godzin pracy, Wykonawcy mają obowiązek zabezpieczenia posiadanych materiałów niejawnych poprzez umieszczenie ich w zamykanych szafach biurowych oraz zamykania pomieszczeń.
6. Klucze od pomieszczeń przechowuje się w sposób zgodny z funkcjonującymi w Urzędzie zasadami polityki kluczy, o której mowa w Planie ochrony. Klucze do szafy pancernej i kasy w strefie II są w dyspozycji i przechowywane w specjalnym miejscu znanym Pełnomocnikowi i najwyższemu kierownictwu.
7. Szafy, w których przechowywane są dokumenty niejawne oznaczone klauzulą „Zastrzeżone”, może otworzyć (w razie potrzeby podczas nieobecności Wykonawcy) komisja powołana przez Wójta, składająca się co najmniej z dwu osób (z udziałem lub za wiedzą bezpośredniego przełożonego Wykonawcy), korzystając z kluczy zapasowych.
8. Komisja sporządza i przekazuje Pełnomocnikowi Ochrony protokół z podjętych czynności, który powinien zawierać:
 - i) datę dokonania czynności;
 - ii) listę numerów ewidencyjnych pobranych dokumentów oraz wskazanie osoby, której materiały powierzono;
 - iii) podpisy członków komisji.
9. Zabrania się wynoszenia dokumentów oznaczonych klauzulą tajności poza strefę ochronną

III bez wiedzy Pełnomocnika Ochrony i zgody Wójta (i należytego zabezpieczenia).

10. Wykonawcy przechowujący materiały o klauzuli „Zastrzeżone” w swych pomieszczeniach służbowych w strefie III, udający się na urlopy lub szkolenia albo podróże służbowe, mają obowiązek przekazania ich osobie zastępującej lub zdania do Pełnomocnika Ochrony, jeśli czas nieobecności Wykonawcy w Urzędzie wyniesie więcej, niż dwa tygodnie.
11. Wypożyczenie oficjalne informacji niejawnych o klauzuli „Zastrzeżone” poza Urząd Gminy odbywa się wyłącznie za pośrednictwem Pełnomocnika Ochrony za zgodą Wójta Gminy lub osoby przez niego upoważnionej na zasadach określonych w rozporządzeniu Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.
12. W przypadku potrzeby przewozu materiałów niejawnych – zgodnie z postanowieniami rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne, mogą być one powierzone:
 - podmiotom prowadzącym działalność w zakresie usług pocztowych,
 - przedsiębiorcom prowadzącym działalność w zakresie usług transportowych lub ochrony osób i mienia,
a także przekazywane
 - bez pośrednictwa uprawnionych przewoźników.

W tym ostatnim przypadku materiały niejawne przewozi się na teren poza Urząd Gminy przez osobę uprawnioną posiadającą stosowne poświadczenie bezpieczeństwa ABW (w zakresie dostępu do informacji niejawnych o klauzuli odpowiedniej do materiałów niejawnych) lub stosowne pisemne upoważnienie Wójta – przy spełnieniu warunków określonych w tymże rozporządzeniu Prezesa Rady Ministrów.

Materiały te przewozi się najkrótszą drogą do odbiorcy z wykorzystaniem nesesera (teczki) z zachowaniem adekwatnych środków bezpieczeństwa zapewniających ochronę informacji przed nieuprawnionym dostępem.

13. Wszelkie nieprawidłowości związane z naruszeniem zasad, o których mowa w tym rozdziale, należy niezwłocznie zgłaszać Pełnomocnikowi Ochrony.

III. Zasady ewidencjonowania, przekazywania, kompletowania i niszczenia dokumentów oznaczonych klauzulą „Zastrzeżone”

1. Dokumenty wytworzone przez pracowników UG (Wykonawców) zawierające informacje niejawne o klauzuli „Zastrzeżone”, a także dokumenty niejawne wpływające do Urzędu wraz z korespondencją przychodzącą (zgodnie z zasadami przetwarzania w części I oraz ochrony fizycznej dokumentów niejawnych w części II) ewidencjonuje się w Dzienniku ewidencyjnym informacji niejawnych (Dzienniki ewidencyjne podlegają Rejestrowi dzienników ewidencji).
2. Dokument dodatkowo wytworzony (kopia, wyciąg) ewidencjonuje się każdorazowo pod oddzielną pozycją w Dzienniku ewidencyjnym IN.
3. Dopuszcza się czasowe przekazanie dokumentów „Zastrzeżonych” pomiędzy uprawnionymi Wykonawcami za pokwitowaniem (strefie III), z jednoczesnym obowiązkiem przekazania tego faktu Pełnomocnikowi Ochrony celem dokonania wpisu w Dzienniku ewidencyjnym.
4. Przekazywanie dokumentów oznaczonych klauzulą „Zastrzeżone” podległym komórkom organizacyjnym następuje za pośrednictwem Pełnomocnika Ochrony (lub osoby uprawnionej wskazanej przez Wójta osoby) na zasadach określonych w rozporządzeniu Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.
5. Udostępnienie dokumentów niejawnych oznaczonych klauzulą „Zastrzeżone” jest możliwe wyłącznie Wykonawcom posiadającym stosowne poświadczenie bezpieczeństwa (np. ABW) lub pisemne upoważnienie Wójta oraz zaświadczenie o odbyciu szkolenia z zasad ochrony informacji niejawnych wydane przez Pełnomocnika Ochrony za podpisem we właściwym rejestrze ewidencyjnym szkoleń. W przypadku, gdy pobierający dokument niejawny nie ma możliwości właściwego jego zabezpieczenia, zapoznaje się z jego treścią w obszarze przetwarzania strefy ochronnej II (w pomieszczeniu Pełnomocnika Ochrony).
6. Dokumenty niejawne o klauzuli „Zastrzeżone” zarówno te wytworzone jak i otrzymane od innych jednostek organizacyjnych, po ich wykorzystaniu podlegają:
 - skompletowaniu w teczki akt lub segregatory – jeśli posiadają wartość praktyczną,
 - zwrotowi do nadawcy – jeśli tak określił on sposób postępowania z materiałami, lub
 - bieżącemu zniszczeniu – jeśli dokument nie posiada wartości użytkowej lub archiwalnej.
7. Ewentualne niszczenie dokumentów dokonuje się przez komisję powołaną przez Wójta oraz udokumentowaną odpowiednio w protokole zgodnie z przepisami rozporządzenia RM z dnia 7 grudnia 2011 r. Członkowie komisji muszą posiadać co najmniej Upoważnienie dostępu do

informacji niejawnych lub odp. poświadczenie bezpieczeństwa osobowego uprawniające do dostępu do IN, tj. z klauzulą tajności co najmniej „Zastrzeżone”.

8. Fakt zniszczenia dokumentów niejawnych dokumentuje się w Protokole zniszczenia, na podstawie którego Pełnomocnik Ochrony wnosi wpis w rubryce „Adnotacje o zniszczeniu” Rejestru ewidencji (adnotacje o treści „*Protokół zniszczenia nr z dnia poz. Nr*”) oraz uwierzytelnia ten wpis własnym podpisem z datą i pieczęcią.

IV. Postępowanie w przypadkach naruszenia zasad ochrony lub ujawnienia informacji niejawnych w Urzędzie Gminy

1. Kierownicy jednostek organizacyjnych Urzędu mają obowiązek powiadomić Pełnomocnika Ochrony o każdym stwierdzonym fakcie:
 - a) naruszenia bezpieczeństwa informacji oznaczonych klauzulą „Zastrzeżone” polegającym na zaniechaniu właściwego działania lub działaniu niezgodnym z przepisami o ochronie informacji niejawnych, mogących spowodować ujawnienie tych informacji,
 - b) ujawnienia informacji oznaczonych klauzulą „Zastrzeżone” poprzez zagubienie, utratę lub kradzież dokumentu lub innego materiału niejawnego albo udostępnienia go osobie nieupoważnionej.
2. Pełnomocnik Ochrony powiadamia o fakcie naruszenia przepisów o ochronie informacji niejawnych Wójta oraz podejmuje niezwłocznie postępowanie wyjaśniające do:
 - a) wyjaśnienia okoliczności naruszenia przepisów i ustalenia osób winnych tej sytuacji,
 - b) określenia stopnia szkody, jaką poniósł lub może ponieść dana komórka organizacyjna UG lub jej pracownicy,
 - c) zminimalizowania ewentualnych skutków powstałych szkód,
 - d) podjęcia przedsięwzięć prewencyjnych.
3. Po zakończeniu postępowania wyjaśniającego, o którym owa wyżej, Pełnomocnik Ochrony występuje do Wójta o wszczęcie postępowania dyscyplinarnego przeciwko osobom winnym naruszeń.
4. W stosunku do osób posiadających poświadczenie bezpieczeństwa, które w sposób rażący dopuściły się naruszenia przepisów o ochronie informacji niejawnych, Pełnomocnik Ochrony lub ABW (SKW) przeprowadzają kontrolne postępowanie sprawdzające (z pominięciem terminów określonych w art. 33 ust. 9 i 10 Ustawy, a stąd z obowiązkiem wypełniania nowej ankiety bezpieczeństwa osobowego przez osobę sprawdzaną).
5. W stosunku do osób posiadających upoważnienie do dostępu do informacji niejawnych o danej klauzuli tajności, które w rażący sposób naruszyły przepisy o ochronie informacji niejawnych, Wójt wydaje decyzję o cofnięciu Upoważnienia w trybie określonym w Kodeksie postępowania administracyjnego.
6. Ponadto, zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, zostały określone przepisami

ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2022 r., poz. 1138 z późn. zm.) w zakresie przepisów art. 266 - 269, w szczególności art. 266 § 2, który stanowi:

„funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację 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”.

Literatura

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 z późn. zm.)
2. 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)
3. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. 2017 r. poz. 1558)
4. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r, poz. 683 z późn. zm.)
5. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. nr 271 poz. 1603)
6. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U 2017 r. poz. 2334)
7. Rozporządzenie Prezesa Rady Ministrów z dnia 9 lipca 2020 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 2020 r. poz. 1256)
8. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. z 2015 r. poz. 220)
9. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. z 2010 r. nr 258 poz. 1753)
10. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. z 2010 r. poz. 1754)

11. Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2024 r. poz. 17 z późn. zm.)