ZARZĄDZENIE NR 45/2022/K

Wójta Gminy Miedzichowo

z dnia 5 grudnia 2022 r.

w sprawie: zatwierdzenia dokumentów z zakresu ochrony informacji niejawnych w Urzędzie Gminy Miedzichowo.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2022 r., poz. 559 ze zmianami) w związku z art. 14 ust. 1, art. 15 ust. 1 pkt 5 i art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2019 r., poz. 742 ze zmianami) zarządzam, co następuje:

§ 1.

W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych zatwierdzam:

1. „Plan ochrony informacji niejawnych w Urzędzie Gminy Miedzichowo", stanowiący załącznik nr 1 do niniejszego zarządzenia.
2. „Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" w Urzędzie Gminy Miedzichowo oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony ",stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuję pracowników Urzędu Gminy Miedzichowo do zapoznania się z dokumentami, o których mowa w § 1 i do stosowania ustaleń w nich zawartych.

§ 3.

Nadzór nad realizacją postanowień niniejszego zarządzenia powierzam Pełnomocnikowi Ochrony Informacji Niejawnych w Urzędzie Gminy Miedzichowo.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

Przygotowała: Karolina Łotecka

WÓJT GMINY
MIEDZICHOWO
64-361 Miedzichowo
Ul. Poznańska 12

WÓJT
dr Stanisław Piechota

Załącznik nr 2 do Zarządzenia Wójta
Gminy Miedzichowo z dnia 5 grudnia 2022r.

Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w Urzędzie Gminy Miedzichowo oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony

ZATWIERDZAM :

WÓJT
dr Stanisław Piechota

Opracował:

Pełnomocnik ds. Ochrony Informacji Niejawnych
Karolina Łotecka

Miedzichowo – listopad 2022

Zawartość

ROZDZIAŁ I Przepisy ogólne 3

ROZDZIAŁ II Zasady klasyfikowania informacji niejawnych o klauzuli „zastrzeżone" 3

ROZDZIAŁ III Dostęp do informacji niejawnych o klauzuli „zastrzeżone" 4

ROZDZIAŁ IV Obieg i udostępnianie dokumentów i materiałów oznaczonych klauzulą „zastrzeżone" . 5

ROZDZIAŁ V Wytwarzanie, oznaczanie i rejestrowanie dokumentów oznaczonych klauzulą „zastrzeżone" 7

ROZDZIAŁ VI Wysyłanie dokumentów oznaczonych klauzulą „zastrzeżone" 10

ROZDZIAŁ VII Przechowywanie, niszczenie i archiwizowanie dokumentów oznaczonych klauzulą zastrzeżone" 11

ROZDZIAŁ VIII Zasady ochrony fizycznej dokumentów oznaczonych klauzulą zastrzeżone" 13

ROZDZIAŁ IX Odpowiedzialność karna i dyscyplinarna 14

ROZDZIAŁ X Postanowienia końcowe 14

ROZDZIAŁ XI Załączniki 15

Załącznik nr 1 – Wzór upoważnienia do „zastrzeżonych" 15

Załącznik nr 2 – Wzór *Dziennika ewidencyjnego* 16

Załącznik nr 3 – Karta zapoznania z dokumentem niejawnym 17

Załącznik nr 4 – wzór pisma niejawnego jednostronicowego 18

Załącznik nr 5 – Wzór pisma niejawnego wielostronicowego 19

Załącznik nr 6 – Wzór opisanych kopert zewnętrznej/wewnętrznej 21

Karta zapoznania 22

ROZDZIAŁ I
Przepisy ogólne

§1

Podstawę prawną niniejszej instrukcji stanowi art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych.

§2

Niniejsza instrukcja określa zasady i sposób postępowania z informacjami niejawnymi oznaczonymi klauzulą „zastrzeżone" oraz zasady ochrony tych informacji w Urzędzie Gminy Miedzichowo.

§3

Instrukcja dotyczy wszystkich pracowników Urzędu Gminy, bez względu na zajmowane przez nich stanowiska czy pełnione funkcje, jeśli wiążą się one z wykonywaniem zadań związanych z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone". Wymienione osoby potwierdzają fakt zapoznania się z niniejszą instrukcją poprzez pisemne potwierdzenie tego faktu w załączonej do instrukcji *Kartą zapoznania.*

§4

Za weryfikację aktualności oraz aktualizację zapisów niniejszej instrukcji odpowiedzialny jest Pełnomocnik ds. ochrony informacji niejawnych Wójta.

§5

Kontrole w zakresie realizacji zapisów instrukcji przez pracowników zobowiązanych do jej przestrzegania przeprowadza Pełnomocnik ds. ochrony informacji niejawnych, w trybie i na zasadach określony w ustawie o ochronie informacji niejawnych, informując każdorazowo Wójta o jej wynikach.

ROZDZIAŁ II
Zasady klasyfikowania informacji niejawnych o klauzuli „zastrzeżone"

§6

Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczpospolitej Polskiej.

§7

Klauzulę tajności nadaje osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Osoba ta może określić datę lub zdarzenie, po wystąpieniu których nastąpi zniesienie lub zmiana klauzuli tajności.

§8

Zniesienie lub zmiana klauzuli tajności „zastrzeżone" możliwe jest wyłącznie po pisemnym wyrażeniu zgody przez osobę o której mowa w §7 albo przełożonego tej osoby – w przypadku ustania lub zmiany ustawowych przesłanek ochrony. Po zniesieniu lub zmianie klauzuli tajności wykonuje się czynności techniczne polegające na naniesieniu odpowiednich zmian na dokumencie oraz poinformowaniu ewentualnych odbiorców dokumentu/materiału o dokonanej zmianie/zniesieniu.

§9

Zbiorom dokumentów i materiałów, których częścią są dokumenty i materiały niejawne, przyznaje się klauzulę tajności równą najwyższej klauzuli tajności dokumentu lub materiału stanowiącego część tego zbioru.

ROZDZIAŁ III
Dostęp do informacji niejawnych o klauzuli „zastrzeżone"

§10

Dokumenty i materiały niejawne o klauzuli „zastrzeżone" są udostępnianie wyłącznie osobom, spełniającym łącznie wszystkie wymienione niżej warunki:

1. Posiadają ważne poświadczenie bezpieczeństwa lub upoważnienie Wójta wydane na podstawie art. 21 ust. 4 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych.
2. Zostały przeszkolone w zakresie ochrony informacji niejawnych i posiadają aktualne (nie starsze niż 5-cioletnie) zaświadczenie potwierdzające ten fakt.
3. Realizują zadania wymagające dostępu do konkretnej informacji niejawnej.

Wyjątek stanowi Wójt Gminy, który dostęp do informacji niejawnych o klauzuli „zastrzeżone" uzyskuje na mocy przepisów ustawy, po uprzednim przeszkoleniu przez POIN.

§11

Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa w §10 ust. 1, prowadzi Pełnomocnik ds. ochrony informacji niejawnych. Pracownik posiadający ważne poświadczenie bezpieczeństwa, otrzymane w innej jednostce organizacyjnej lub w wyniku postępowania sprawdzającego prowadzonego przez ABW/SKW, jest obowiązany do okazania oryginału dokumentu Pełnomocnikowi ds. ochrony informacji niejawnych w ciągu 5 dni od chwili przekazania informacji o posiadaniu tego dokumentu.

§12

Przełożeni pracowników Urzędu Gminy są zobowiązani do przekazywania Pełnomocnikowi ds. ochrony informacji niejawnych informacji o konieczności wydania przez Wójta upoważnienia pracownikom, których zakres zadań wymaga przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

§13

Upoważnienia Wójta wydane na podstawie art. 21 ust. 4 ustawy z dnia 5 sierpnia 2010 roku mogą być wystawione na czas zatrudnienia w Urzędzie, na czas określony datą końcową lub do wykonania określonej czynności. Wzór upoważnienia Wójta uprawniającego do dostępu do informacji niejawnych o klauzuli zastrzeżone zawarto w załączniku nr 1 do niniejszej instrukcji.

ROZDZIAŁ IV
Obieg i udostępnianie dokumentów i materiałów oznaczonych klauzulą „zastrzeżone"

§14

Korespondencja wpływająca do Urzędu, zawierająca informacje niejawne o klauzuli „zastrzeżone", wpływa do sekretariatu Wójta za pośrednictwem operatora pocztowego, firmy kurierskiej lub dostarczana jest bezpośrednio przez jej nadawcę, skąd po rozpakowaniu pierwszej koperty i stwierdzeniu drugiej koperty z gryfem niejawności jest przekazywana niezwłocznie w stanie nienaruszonym, za pokwitowaniem w dzienniku podawczym, do kancelarii niejawnej – pomieszczenie przy biurze nr 15.

§15

Pracownik kancelarii niejawnej, dokonując odbioru przesyłki, jest zobowiązany sprawdzić:

1. Prawidłowość adresu,
2. Całość pieczęci i opakowania pod kątem ewentualnych uszkodzeń, prób nieuprawnionego otwarcia,
3. Zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
4. Odcisnąć na przesyłce pieczęć oraz wpisać datę wpływu do Urzędu.

W przypadku stwierdzenia uszkodzenia przesyłki lub ujawnienia prób jej otwierania, odbierający przesyłkę pracownik kancelarii niejawnej sporządza wspólnie z doręczającym przesyłkę protokół uszkodzenia, którego egzemplarze otrzymują:

1. Nadawca przesyłki,
2. Pełnomocnik ds. ochrony informacji niejawnych,

3. Przedstawiciel przewoźnika, jeśli w doręczeniu przesyłki uczestniczył przewoźnik (operator pocztowy, firma kurierska).

§16

Pracownik kancelarii niejawnej, przyjąwszy przesyłkę, dokonuje jej rozpakowania oraz rejestracji w odpowiednim *Dzienniku ewidencyjnym*, którego wzór stanowi załącznik nr 2 do instrukcji, dokonując jednocześnie weryfikacji, czy:

1. Zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
2. Liczba stron oraz ewentualnych załączników jest zgodna z liczbą podaną na poszczególnych dokumentach.

W razie stwierdzenia nieprawidłowości lub rozbieżności co do ilości lub typu załączników, pracownik kancelarii niejawnej sporządza *protokół otwarcia przesyłki* zawierający opis nieprawidłowości, którego jeden egzemplarz przekazuje nadawcy a drugi Pełnomocnikowi ds. ochrony informacji niejawnych. Fakt sporządzenia protokołu odnotowuje w „Dzienniku ewidencyjnym" w rubryce *Informacje uzupełniające/uwagi.*

§17

Po zakończonej procedurze rejestracji, pracownik kancelarii niejawnej przedkłada dokument niejawny Wójtowi, który na dokumencie dokonuje dekretacji wskazując imiennie pracownika odpowiedzialnego za merytoryczne załatwienie danej sprawy, wpisując datę czynności oraz potwierdza podpisem oraz pieczęcią imienną.

§18

Po wykonaniu dekretacji przez Wójta, pracownik kancelarii niejawnej wzywa osobę widniejącą w dekretacji do obioru dokumentu. W przypadku nieobecności osoby, dokument podlega przechowaniu w dedykowanej zamykanej szafie/meblu do czasu podjęcia przez osobę widniejącą w dekretacji.

§19

Pracownik kancelarii niejawnej jest odpowiedzialny za weryfikację formalnych uprawnień w zakresie dostępu do informacji niejawnych przez osobę widniejącą w dekretacji w zakresie ważności poświadczenia bezpieczeństwa/posiadania upoważnienia do „zastrzeżonych" oraz aktualnego szkolenia w zakresie ochrony informacji niejawnych. W przypadku braku spełnienia wymogów formalnych odmawia wydania dokumentu informując jednocześnie o sytuacji Pełnomocnika ds. OIN.

§20

W razie stwierdzenia konieczności zapoznania z treścią dokumentu większej liczby osób, należy dokonać uprzednio rozszerzenia dekretacji w sposób opisany w §18 a także dokonać weryfikacji formalnych uprawnień w zakresie dostępu do informacji niejawnych w sposób opisany w §19.

§21

W przypadku konieczności zapoznania większej liczby osób z treścią dokumentu niejawnego, pracownik kancelarii niejawnej zakłada do dokumentu *Kartę zapoznania* wg wzoru – załącznik nr 3 do instrukcji, oraz odpowiada za jej prawidłowe i kompletne wypełnienie przez osoby zapoznające się.

§22

W przypadku konieczności zmiany osoby merytorycznie realizującej dane zagadnienie i powiązanego z tym przekazania dokumentu lub materiału niejawnego, podlega on zwrotowi do komórki rejestrującej – kancelarii niejawnej Urzędu, gdzie dokonuje się adnotacji o zwrocie przez pracownika, zmiany dekretacji przez Wójta na kolejnego pracownika z uwzględnieniem odpowiednich zapisów w *Dzienniku ewidencyjnym.*

§23

Zabronione i niedopuszczalne jest samowolne przekazywanie dokumentów i materiałów niejawnych pomiędzy pracownikami z pominięciem komórki rejestrującej oraz bez zmiany lub rozszerzenia dekretacji Wójta.

§24

W przypadku konieczności zorganizowania spotkania, podczas którego będą omawiane lub przedstawiane informacje niejawne o klauzuli „zastrzeżone", wszyscy uczestnicy muszą:

1. Być poinformowani o jego niejawnym charakterze,
2. Spełniać wymogi formalne w zakresie dostępu do informacji niejawnych omówione w §10 niniejszej instrukcji.

ROZDZIAŁ V
Wytwarzanie, oznaczanie i rejestrowanie dokumentów oznaczonych klauzulą „zastrzeżone"

§25

Informacje niejawne w formie dokumentu pisanego, oznaczane klauzulą „zastrzeżone" mogą być sporządzane w formie pisma odręcznego drukowanymi literami, na maszynie do pisania niewyposażonej w moduł pamięci lub na akredytowanym przez Wójta stanowisku komputerowym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" – Bezpiecznej Stacji Komputerowej (BSK).

§26

Przetwarzanie dokumentów w formie elektronicznej oznaczonych klauzulą „zastrzeżone" jest dopuszczalne wyłącznie na BSK, zlokalizowanym w odrębnym pomieszczeniu przy biurze nr 15. Osobami dopuszczonymi do pracy na BSK są jego użytkownicy, którym uprzednio nadano uprawnienia do pracy zgodnie z dokumentacją bezpieczeństwa systemu.

§27

Przetwarzanie dokumentów i materiałów niejawnych jest dopuszczalne jedynie w pomieszczeniach lub obszarach objętych kontrolą dostępu, w przypadku systemu BSK dodatkowo z uwzględnieniem wyników szacowania ryzyka, lub strefie ochronnej. Do pomieszczeń tych zaliczono w szczególności:

1. Pomieszczenie kancelarii niejawnej zlokalizowane w pomieszczeniu przy biurze nr 15, jako komórki rejestrującej dokumenty „zastrzeżone", będącego jednocześnie pomieszczeniem BSK zlokalizowanym w pomieszczeniu odrębnym przy biurze nr 15.

Przetwarzanie winno odbywać się w warunkach zapewniających ochronę informacji niejawnych przed nieuprawnionym ujawnieniem.

§28

Zabronione jest przetwarzanie informacji niejawnych poza pomieszczeniami i obszarami wymienionymi w §26.

§29

Informacje niejawne utrwalone w formie pisemnej, oznacza się w następujący sposób:

1. Na każdej stronie pisma umieszcza się:
    a. Na środku strony, jako pierwszy element w nagłówku strony klauzulę tajności;
    b. W prawym górnym rogu numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu napis „Egz. Pojedynczy";
    c. W lewym górnym rogu sygnaturę literowo-cyfrową, na ka którą składa się oznaczenie jednostki lub komórki, symbol klauzuli (Z), numer pod którym zarejestrowano dokument oraz rok jego rejestracji, ponadto dopuszczalne inne oznaczenia ułatwiające ustalenia miejsca wykonania lub przynależność do określonej sprawy;
    d. Numer strony oraz liczbę stron całego dokumentu;
    e. Jako ostatni element stopi strony – ponownie klauzulę tajności.
2. Na pierwszej stronie pisma umieszcza się również:
    a. W lewym górnym rogu, nad sygnaturą literowo-cyfrową, nazwę jednostki lub komórki organizacyjnej;
    b. W prawym górnym rogu powyżej numeru egzemplarza lub oznaczenia egzemplarza pojedynczego nazwę miejscowości i datę podpisania dokumentu;
    c. W przypadku dokumentu, któremu nadano bieg korespondencyjny, pod numerem egzemplarza w kolejności pionowej: imię i nazwisko lub nazwę stanowiska adresata,

jednostkę organizacyjną; w przypadku wielu adresatów dopuszcza się umieszczenie adnotacji „adresaci wg rozdzielnika" który to rozdzielnik podpisany przez Wójta załącza się do pisma.

3. Na ostatniej stronie pisma, pod treścią, umieszcza się również:
   a. Liczbę załączników,
   b. Liczbę stron lub innych jednostek miary wszystkich załączników,
   c. Klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiedniej ewidencji oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
   d. W przypadku gdy adresatowi wysyła się inną liczbą załączników niż pozostawia w aktach, dodatkowo napis „Tylko adresat", jeżeli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach,
   e. Napis „do zwrotu" , jeżeli załączniki mają zostać zwrócone nadawcy,
   f. Stanowisko oraz imię i nazwisko lub inne oznaczenia wskazujące osobę uprawnioną do jego podpisania,
   g. Liczbę wykonanych egzemplarzy,
   h. adresatów poszczególnych egzemplarzy dokumentu lub adnotację „ adresaci według rozdzielnika",
   i. dyspozycję „ad acta" w przypadku egzemplarza pozostającego w aktach

W przypadku dokumentów nieelektronicznych o klauzuli tajności „zastrzeżone" dopuszcza się odstąpienie od umieszczania oznaczeń:

1. W prawym górnym rogu: numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu napis „Egz. pojedynczy",
2. W lewym dolnym rogu w kolejności pionowej: liczbę wykonanych egzemplarzy, adresatów poszczególnych egzemplarzy dokumentu, adnotację „adresaci według rozdzielnika pozostającego przy oryginale" lub wskazanie „ad acta", imię i nazwisko lub inne dane identyfikujące wykonawcę.

Na załącznikach do pisma na pierwszej stronie w prawym górnym rogu umieszcza się dodatkowo napis: „Załącznik nr ....do dokumentu nr..... z dnia.....". Jeżeli przy piśmie przewodnim przesyłane są załączniki oznaczone klauzulami tajności, to:

1. Klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula załącznika o najwyższym stopniu tajności,
2. Na piśmie przewodnim, jeżeli jego klauzula jest inna, po odłączeniu załącznika zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym ich odłączeniu: na każdej stronie pod numerem egzemplarza zamieszcza się napis: „.....(nazwa klauzuli tajności) po odłączeniu załączników" lub „Jawne po odłączeniu załączników".

W przypadku opisanym powyżej, przy rejestracji pisma przewodniego w „Dzienniku ewidencyjnym", w rubryce „Informacje uzupełniające/uwagi" wpisuje się adnotację o treści „(nazwa klauzuli tajności) po odłączeniu załączników" lub „Jawne po odłączeniu załączników".

Wzór pisma niejawnego:

1. Jednostronicowego – zawarto w załączniku nr 4 do instrukcji
2. Wielostronicowego – zawarto w załączniku nr 5 do instrukcji.

§30

W przypadku pisma , któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dodatkowe dyspozycje dla adresata o treści:

1. Udzielanie informacji, tylko za pisemną zgodą nadawcy,
2. Kopiowanie tylko za pisemną zgodą nadawcy,
3. Odpis tylko za pisemną zgodą nadawcy,
4. Kopiowanie stron od ... do ... tylko za pisemną zgodą nadawcy,
5. Odpis od ... do ... tylko za pisemną zgodą nadawcy,
6. Wypis(wyciąg) od ... do ... tylko za pisemną zgodą nadawcy.

§31

Kopie, wyciągi, odpisy, wypisy dokumentów niejawnych o klauzuli „zastrzeżone" następuje wyłącznie na podstawie pisemnego polecenia Wójta, odnotowanego na przedmiotowym dokumencie. Wykonaniem kopii zajmuje się pracownik wskazany w dekretacji Wójta. Wykonana kopia, odpis, wyciąg lub wypis podlega rejestracji w Dzienniku ewidencyjny pod kolejną liczbą.

ROZDZIAŁ VI
Wysyłanie dokumentów oznaczonych klauzulą „zastrzeżone"

§32

Materiały niejawne o klauzuli „zastrzeżone" przesyła się:

1. Jako listy polecone lub wartościowe, za zwrotnym potwierdzeniem odbioru, zapakowane w dwie nieprzeźroczyste koperty opisane:
    a. Na kopercie wewnętrznej:
        i. klauzulę tajności i ewentualne dodatkowe oznaczenia,
        ii. określenie adresata,
        iii. imię, nazwisko i podpis osoby pakującej,
        iv. numer, pod którym dokument został zarejestrowany;
    b. Na kopercie zewnętrznej:
        i. nazwę jednostki organizacyjnej adresata,
        ii. adres siedziby adresata,
        iii. numer wykazu i pozycji w wykazie przesyłek nadanych,
        iv. nazwę jednostki organizacyjnej nadawcy.

2. Jako paczki z zadeklarowaną wartością, opakowane w dwie warstwy nieprzezroczystego mocnego papieru, gdzie każda warstwa jest opisana analogicznie jak koperty w pkt. 1.

Wzór opisanych kopert zawarto w załączniku nr 6 do instrukcji.

§33

Kopertę wewnętrzną stempluje się na jej łączeniach pieczęcią do pakietów oraz okleja przeźroczystą taśmą samoprzylepną tak, by ewentualne próby nieuprawnionego otwarcia pozostawiły ślad.

§34

Przesyłki nadaje się za pomocą operatora pocztowego, firm kurierskiej bądź przewozi bezpośrednio ze Urzędu do Adresata. W przypadku przewożenia bezpośredniego, pracownik Urzędu dokonujący przewozu musi spełniać wymogi w zakresie dostępu do informacji niejawnych, opisane w §10 niniejszej instrukcji oraz posiadać Książkę doręczeń przesyłek lub inny dokument, w którym Adresat lub jego uprawniony przedstawiciel dokona pokwitowania przesyłki niejawnej. Przewiezienie przez pracownika Urzędu winno nastąpić najkrótszą możliwą drogą od Urzędu do siedziby adresata.

ROZDZIAŁ VII
Przechowywanie, niszczenie i archiwizowanie dokumentów oznaczonych klauzulą zastrzeżone"

§35

Dokumenty niejawne podlegają obowiązkowej ochronie przed utratą lub nieuprawnionym ujawnieniem. Po zakończonej pracy z dokumentem lub materiałem podlegają one przechowywaniu przez osoby, na których stanie się znajdują w indywidualnie użytkowanych, zamykanych na klucz meblach biurowych, szafach metalowych lub sejfach.

§36

Zabronione jest przechowywanie wspólnie z dokumentami jawnymi, chyba że dokumenty jawne i niejawne są częścią tego samego zbioru dokumentów w ramach jednej sprawy. W innym przypadku muszą być wyraźnie od siebie odseparowane/oddzielone.

§37

Szafy i meble, o których mowa w §35 znajdują się w obszarach lub pomieszczeniach o których mowa w §27, objętych organizacyjną kontrolą dostępu, do których samodzielny dostęp możliwy jest wyłącznie dla osób uprawnionych przez Wójta.

§38

Pomieszczenia biurowe oraz szafy i meble, służące do przechowywania informacji niejawnych są po zakończonym dniu pracy plombowane przez pracowników będących ich dysponentami.

§39

Zasady dostępu do pomieszczeń, sposób przechowywania i postępowania z kluczami do użytku bieżącego oraz zapasowymi do pomieszczeń i szaf/mebli do przechowywania informacji niejawnych opisano szczegółowo w *Planie ochrony informacji niejawnych.*

§40

W celu zniszczenia materiałów niejawnych nie podlegających trwałemu przechowywaniu oraz które utraciły znaczenie praktyczne Wójt powołuje komisję złożoną z co najmniej trzech pracowników, spełniających wymagania o których mowa w §10 instrukcji. W skład komisji obligatoryjnie wchodzi pracownik kancelarii niejawnej lub Pełnomocnik ds. ochrony informacji niejawnych. Powołana komisja sporządza protokoły oceny dokumentacji niearchiwalnej oraz spisy dokumentacji niearchiwalnej przeznaczonej do zniszczenia. W oparciu o przygotowaną dokumentację Wójt występuje z wnioskiem do dyrektora właściwego archiwum państwowego o wyrażenie zgody na zniszczenie.

§41

Niszczenie dokumentów i materiałów jest realizowane poprzez:

1. Dokumenty w formie papierowej są niszczone poprzez pocięcie w niszczarce spełniającej wymagania co najmniej dla klasy P4 wg normy DIN 66399 (DIN3 wg 32757),
2. Niszczenie nośników IND zawierających informacje niejawne następuje poprzez fizyczne niszczenie lub deklasyfikację nośnika wg sposobów opisanych w dokumentacji bezpieczeństwa BSK.

Fakt zniszczenia dokumentuje się protokolarnie, odnotowując fakt zniszczenia określonego dokumentu w *Dzienniku ewidencyjnym* z adnotacją „Zniszczono – protokół z dnia ...." w rubryce uwagi. Protokoły zniszczenia przechowuje Pełnomocnik ds. OIN.

§42

Niszczenia wadliwych lub niekompletnych wydruków powstałych w wyniku nieprawidłowego działania BSK lub jego komponentów dokonuje się niezwłocznie po ich wykonaniu/stwierdzeniu poprzez pocięcie w niszczarce wskazanej w §41 ust. 1. Fakt zniszczenia wadliwego wydruku odnotowuje się w *Dzienniku pracy dialogowej* stanowiska.

§43

Materiały spraw ostatecznie załatwionych, oznaczone klauzulą niejawności, podlegają przeglądowi przed przekazaniem do archiwizacji pod kątem ustalenia aktualności przesłanek dalszej ochrony dokumentu. W przypadku stwierdzenia, że zawarte w dokumentach informacje utraciły walory informacji niejawnej, należy znieść klauzulę z dokumentów w sposób opisany w instrukcji oraz dokonać odpowiednich czynności technicznych na dokumencie. Dokumenty po zniesieniu klauzuli przekazuje się do archiwum zakładowego. W przypadku utrzymania klauzuli tajności, materiały przechowuje Pełnomocnik ds. OIN zgodnie z kategorią archiwalną akt.

ROZDZIAŁ VIII
Zasady ochrony fizycznej dokumentów oznaczonych klauzulą zastrzeżone"

§44

Dokumenty i materiały niejawne podlegają ochronie bez względu na upływ czasu, do momentu zniesienia klauzuli tajności lub wystąpienia zdarzenia lub daty określonej przez osobę uprawnioną do jego podpisania lub oznaczenia.

§45

Przetwarzanie materiałów niejawnych odbywa się wyłącznie w obszarach lub pomieszczeniach objętych kontrolą dostępu, do których dostęp samodzielny mają osoby uprawnione przez Wójta.

§46

Po zakończonej pracy z dokumentami i materiałami, osoby w których dyspozycji pozostają przetwarzane materiały, zabezpieczają je przed utratą kontroli nad dokumentem i dostępem osób nieuprawnionych oraz nieuprawnionym ujawnieniem poprzez zamknięcie w indywidualnie użytkowanych meblach biurowych, szafach metalowych lub sejfach.

§47

Niedopuszczalne jest pozostawianie dokumentów i materiałów niejawnych na biurku bez nadzoru, nawet w przypadku chwilowego opuszczania pomieszczenia.

§48

Zasady bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym BSK zawarto w dokumentacji bezpieczeństwa systemu, tj. Szczególnych Wymaganiach Bezpieczeństwa oraz Procedurach Bezpiecznej Eksploatacji.

ROZDZIAŁ IX
Odpowiedzialność karna i dyscyplinarna

§49

Działania pracowników skutkujące nieuprawnionym ujawnieniem informacji niejawnej skutkować mogą skierowaniem wniosku do organów ścigania o dokonanie oceny prawno-karnej pod kątem popełnienia czynu lub czynów zabronionych opisanych w *Dziale XXXIII – Przestępstwa przeciwko ochronie informacji* ustawy *z dnia 6 czerwca 1997 roku Kodeks karny* i/lub z tytułu niedopełnienia obowiązków, skutkujących nieuprawnionym ujawnieniem informacji lub utratą kontroli nad dokumentem niejawnym.

§50

Niezależnie od działań opisanych w §49, wobec pracownika wskutek działań lub zaniedbań w wyniku którego doszło do utraty kontroli nad materiałem niejawnym lub nieuprawnionego ujawnienia jego treści, Wójt może wszcząć wobec pracownika postępowanie dyscyplinarne, z tytułu ciężkiego naruszenia obowiązków pracowniczych.

ROZDZIAŁ X
Postanowienia końcowe

§51

Wszelkie ujawnione nieprawidłowości bądź podejrzenia co do stanu zabezpieczeń i bezpieczeństwa informacji niejawnych winne być zgłaszane niezwłocznie Pełnomocnikowi ds. OIN.

§52

W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych, Pełnomocnik ds. OIN podejmuje działania na podstawie art. 17 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych działania zmierzające do ustalenia okoliczności naruszenia, osób odpowiedzialnych, skali naruszenia oraz podejmuje działania zmierzające do ograniczenia negatywnych skutków naruszania. Po zakończeniu czynności przedkłada Wójtowi sprawozdanie z wykonanych czynności wraz z wnioskami końcowymi w zakresie przeciwdziałaniu podobnym zdarzeniom lub wskazujące konieczność przeciwdziałaniu nowym zidentyfikowanym zagrożeniom.

§53

Wszelkie sprawy nieuregulowane niniejszą instrukcją podlegają indywidualnej ocenie i analizie dokonywanej przez Pełnomocnika ds. ochrony informacji niejawnych.

ROZDZIAŁ XI
Załączniki

Załącznik nr 1 – Wzór upoważnienia do „zastrzeżonych"

Miedzichowo, data.....

.....
Pieczęć nagłówkowa jednostki

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:

.....
Imię (imiona) i nazwisko (w tym przybrane), imię ojca

.....
Nr PESEL

Niniejsze upoważnienie wydane jest w celu ..... lub na okres:

- od dnia ..... do dnia .....
- od dnia ..... do odwołania
- zatrudnienia w Urzędzie Gminy Miedzichowo.[1]

.....
Wójt Gminy – pieczęć i podpis

[1] Niewłaściwe skreślić

WZÓR

DZIENNIK EWIDENCYJNY

Strona lewa

Symbol oznaczenia klauzuli tajności	Numer kolejny zapisu	Adnotacje dot. obowiązywania klauzuli tajności lub jej zniesienia albo zmiany	Data rejestracji dokumentu	Nazwa nadawcy/adresata	Numer i data dokumentu otrzymanego	Nazwa dokumentu lub czego dotyczy	Liczba egzemplarzy wytworzonego dokumentu	Liczba		
								stron dokumentu lub innych jednostek miary	załączników	stron wszystkich załączników lub innych jednostek miary
1	2	3	4	5	6	7	8	9	10	11

strona ...../.....

Strona prawa

Nr dokumentu, z którego wykonano wydruk, kopię, wyciąg, wypis, odpis, tłumaczenie, lub numer nośnika	Imię i nazwisko lub inne dane identyfikujące wykonawcę dokumentu	Data, imię i nazwisko oraz podpis osoby pobierającej dokument	Potwierdzenie zwrotu dokumentu (data i podpis)	Adnotacje		Informacje uzupełniające/Uwagi (np. symbol klasyfikacyjny wykazu akt)
				o wysłaniu dokumentu lub załącznika (pozycja w książce doręczeń przesyłek miejscowych/ pozycja wykazu przesyłek nadanych/załącznik do pisma nr ...)	o wybrakowaniu lub przekazaniu do archiwum	
12	13	14	15	16	17	18

strona ...../.....

WZÓR

KARTA ZAPOZNANIA SIĘ Z DOKUMENTEM NR ....

Lp.	UDOSTĘPNIENIE DOKUMENTU			Uwagi
	imię i nazwisko osoby, której dokument udostępniono	data	podpis	

strona ...../.....

Załącznik nr 4 – wzór pisma niejawnego jednostronicowego

Zastrzeżone

Nazwa jednostki nadawcy
Nazwa komórki organizacyjnej
Sygnatura literowo-cyfrowa

Miejscowość, dnia .....

Egz. nr .....
(Jawne po odłączeniu załącznika)
(Podlega ochronie do dnia .....)

Imię i nazwisko adresata
Nazwa stanowiska adresata
Nazwa jednostki organizacyjnej

Treść pisma:

Bezpośrednio pod treścią pisma (przykładowo):
Załączników: ... na ... str.
zał. 1 – zastrzeżony ..... na .... str.
zał. 2 – jawny na .... str. – tylko adresat
zał. 3 – jawny na .... str. – do zwrotu

Pieczęć imienna oraz podpis osoby uprawnionej do podpisania dokumentu

Wykonano w 2 egz.:
Egz. nr 1 – nazwa jednostki organizacyjnej adresata
Egz. nr 2 – a/a
Wykonał:

strona 1/1
Zastrzeżone

Załącznik nr 5 – Wzór pisma niejawnego wielostronicowego

Zastrzeżone

Nazwa jednostki nadawcy
Nazwa komórki organizacyjnej
Sygnatura literowo-cyfrowa

Miejscowość, dnia .....

Egz. nr .....
(Jawne po odłączeniu załącznika)
(Podlega ochronie do dnia .....)

Imię i nazwisko adresata
Nazwa stanowiska adresata
Nazwa jednostki organizacyjnej

Treść pisma:

Zastrzeżone

Zastrzeżone

Egz. nr .....

Sygnatura literowo-cyfrowa

Treść pisma – jego dalszy ciąg

Bezpośrednio pod treścią pisma (przykładowo):

Załączników: ... na ... str.

zał. 1 – zastrzeżony ..... na .... str.

zał. 2 – jawny na .... str. – tylko adresat

zał. 3 – jawny na .... str. – do zwrotu

Pieczęć imienna oraz podpis osoby uprawnionej do podpisania dokumentu

Wykonano w 2 egz.:

Egz. nr 1 – nazwa jednostki organizacyjnej adresata

Egz. nr 2 – a/a

Wykonał:

Załącznik nr 6 – Wzór opisanych kopert zewnętrznej/wewnętrznej

Koperta zewnętrzna

Nazwa jednostki organizacyjnej
Nadawcy

Wykaz/pozycja przesyłek nadanych

Nazwa jednostki organizacyjnej Adresata
Adres siedziby Adresata

Koperta wewnętrzna

ZASTRZEŻONE

Sygnatura literowo cyfrowa
pod którą zarejestrowano dokument

Dokładne określenie adresata
(Imię Nazwisko i/lub
funkcja/stanowisko)

Pakował/a:
(imię i nazwisko osoby pakującej
oraz jej podpis)

Karta zapoznania

Karta zapoznania z niniejszą *Instrukcją (...)* osób realizujących zadania służbowe w Urzędzie Gminy Miedzichowo związane z dostępem do informacji niejawnych.

LP	Imię i nazwisko	Stanowisko	Data	Podpis
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Załącznik nr 1 do Zarządzenia Wójta Gminy
Miedzichowo z dnia 5 grudnia 2022r.

Plan ochrony informacji niejawnych w Urzędzie Gminy Miedzichowo

„ZATWIERDZAM"

WÓJT
dr Stanisław Piechota

Miedzichowo – listopad 2022

SPIS TREŚCI

1. **Wstęp.** **3**
   1.1. Podstawy prawne. 3
   1.2. Definicje. 4

2. **Opis stref ochronnych, pomieszczeń lub obszarów, o których mowa w §7 ust. 4, w tym określenie ich granic i wprowadzonego systemu kontroli dostępu.** **6**
   2.1. Opis budynku i jego sąsiedztwa. 6
   2.2. Opis pomieszczenia, w którym przetwarzane są informacje niejawne. 8

3. **Procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefach ochronnych.** **9**
   3.1. Osoby uprawnione. 9
   3.2. Osoby nieuprawnione. 9

4. **Określenie poziomu zagrożeń.** **10**
   4.1. Tabela oceny istotności czynników zagrożeń. 10
   4.2. Punktacja zastosowanych środków bezpieczeństwa fizycznego. 11

5. **Opis zastosowanych środków bezpieczeństwa fizycznego.** **13**

6. **Procedury zarządzania kluczami do szaf i pomieszczeń, w których przetwarzane są informacje niejawne.** **18**
   6.1. Zarządzanie kluczami do pomieszczenia. 18
   6.2. Zarządzanie kluczami do szafy metalowej/mebli biurowych do IN. 19

7. **Procedury reagowania osób odpowiedzialnych za ochronę informacji niejawnych w przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych.** **20**

8. **Bezpieczeństwo teleinformatyczne.** **22**

9. **Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym w razie wprowadzenia stanów nadzwyczajnych.** **23**

1. Wstęp.

W Urzędzie Gminy Miedzichowo przetwarzane są informacje niejawne o klauzuli „zastrzeżone", w tym w formie dokumentów elektronicznych z wykorzystaniem dedykowanego do tego celu stanowiska systemu teleinformatycznego przetwarzającego informacje niejawne – „Bezpiecznej Stacji Komputerowej - BSK".

1.1. Podstawy prawne.

Plan ochrony informacji niejawnych Urzędu Gminy Miedzichowo sporządzony 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)* z uwzględnieniem zapisów wynikających z aktów wykonawczych do przywołanej ustawy:

1) *Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r. poz. 683),*

2) *Rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 Nr 288, poz. 1692),*

3) *Rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603),*

4) *Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. z 2015 r. poz. 220),*

5) *Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. z 2010 r. Nr 258, poz. 1754),*

6) *Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. z 2010 r. Nr 258, poz. 1753),*

7) *Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).*

1.2. Definicje.

Użyte w niniejszym planie definicje oznaczają:

- **Dokument niejawny** – każda utrwalona informacja niejawna;

- **Materiały niejawne** - dokumenty lub przedmioty albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenia, wyposażenie a także składnik użyty do ich wytworzenia;

- **Informacje niejawne o klauzuli „zastrzeżone"** - informacje, których nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej;

- **Przetwarzanie informacji niejawnych** - wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

- **Rękojmia zachowania tajemnicy** - zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;

- **System teleinformatyczny** – system teleinformatyczny w rozumieniu *art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344)* tj. zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu *ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 ze zm.);*

- **Dostępność informacji niejawnej** - właściwość określająca dostępność informacji niejawnej na każde żądanie podmiotu uprawnionego;

- **Integralność informacji niejawnej** – właściwość określająca brak nieuprawnionej modyfikacji informacji niejawnej;

- **Poufność informacji niejawnej** – właściwość określająca, że informacja niejawna nie jest ujawniana podmiotom do tego nieuprawnionym;

- **Incydent bezpieczeństwa** – zdarzenie lub seria zdarzeń mających związek z bezpieczeństwem informacji niejawnych, mających zagrażających ich dostępności, integralności lub poufności;

- **Ryzyko** - kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

- **Szacowanie ryzyka** - całościowy proces analizy i oceny ryzyka;

- **Zarządzanie ryzykiem** - skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

- **Informatyczny nośnik danych (IND)** - materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

- **Bezpieczna Stacja Komputerowa (BSK)** - to stanowisko komputerowe służące do opracowywania dokumentów niejawnych o klauzuli „zastrzeżone";

- **Jednostka organizacyjna** – Urząd Gminy Miedzichowo;

- **Kierownik jednostki organizacyjnej (KJO)** – Wójt Gminy;

- **Pełnomocnik do spraw ochrony informacji niejawnych (POIN)** – pełnomocnik ochrony - osoba bezpośrednio podlegająca kierownikowi jednostki organizacyjnej, która odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

2. Opis stref ochronnych, pomieszczeń lub obszarów, o których mowa w §7 ust. 4[1], w tym określenie ich granic i wprowadzonego systemu kontroli dostępu.

2.1. Opis budynku i jego sąsiedztwa.

Budynek Urzędu Gminy Miedzichowo zlokalizowany jest przy ul. Poznańskiej 12 w miejscowości Miedzichowo (64-361) w odległości:

- Ok. 30 m od jednostki Policji – Posterunek Policji w Miedzichowie, ul. Poznańska 36;
- Ok. 30 m od najbliższej jednostki Straży Pożarnej - OSP Miedzichowo, ul. Poznańska 10.

W otoczeniu Urzędu budynki handlowo-usługowe, oświatowe oraz zabudowa mieszkalna. Brak obiektów, które ze względu na przeznaczenie lub charakter prowadzonej działalności mogłyby stwarzać dodatkowe zagrożenie dla Urzędu. Na terenie budynku Urzędu prowadzą działalność następujące jednostki/podmioty nadzorowane przez Wójta – Urząd Stanu Cywilnego, Gminny Ośrodek Pomocy Społecznej oraz Gminny Zespół Obsługi Szkół. W budynku znajduje się lokal mieszkalny wynajmowany mieszkańcom gminy.

Działka, na której znajduje się budynek urzędu nie jest ogrodzona – do budynku jest bezpośredni dostęp z okalających Urząd ulic i chodników.

Obiekt Urzędu jest budynkiem czterokondygnacyjnym (częściowo podziemna piwnica, parter oraz dwa piętra). Wykonany w technologii murowanej, dach płaski kryty papą. Stolarka okienna PCV, okna i szyby niecertyfikowane, wybrane pomieszczenia posiadają okna wyposażone w zewnętrzne kraty z prętów stalowych.

Do budynku Urzędu prowadzą wejścia:

- Główne od ulicy Poznańskiej, zamykanymi drzwiami z profili aluminiowych, z przeszkleniami, zamykanymi na dwa zamki z wkładką bębenkową, całość niecertyfikowana. Wewnątrz przedsionek tworzący wiatrołap, oddzielony od reszty ciągów komunikacyjnych drzwiami pełnymi drewnianymi, zamykanymi na zamek z wkładką bębenkową, niecertyfikowane. Przejście/wiatrołap zabezpieczone czujką ruchu systemu alarmowego, w zasięgu której znajduje się opisany hol oraz główne drzwi wejściowe do obiektu.
- Wejście od tyłu obiektu, przez kotłownię, zabezpieczone drzwiami metalowymi przeciwpożarowymi, zamykanymi na jeden zamek z wkładką bębenkową.

[1] *Rozporządzenia Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.*

Wewnątrz dostęp ograniczają zamykane na zamki zwykłe drzwi wewnętrzne drewniane.

Obiekt objęty elektronicznym system alarmowym – obejmującym szereg czujek ruchu zabezpieczających ciągi komunikacyjne (w tym klatkę schodową) oraz wybrane pomieszczenia biurowe, centralką alarmową oraz sygnalizatory optyczno-akustyczne umieszczone na elewacji budynku od ul. Poznańskiej oraz na tylnej ścianie Urzędu. Czujki ruchu rozmieszczono w sposób zapewniający pokrycie wewnątrz obiektu w taki sposób, że niemożliwe jest przedostanie się do chronionych pomieszczeń bez wyzwolenia alarmu. Wyzwolenie alarmu powoduje uruchomienie sygnalizatorów optyczno-akustycznych oraz przekazanie sygnału do centrum monitorowania firmy ochrony osób i mienia Hunters24, której grupa interwencyjna realizuje podjazdy do obiektu Urzędu w celu weryfikacji przyczyn wyzwolenia alarmu/podjęcia interwencji w czasie:

- 15 minut w godzinach od 06:00 do 22:00
- 10 minut w godzinach od 22:00 do 6:00.

Otwarcia/zamknięcia obiektu Urzędu oraz rozbrojenia/uzbrojenia systemu alarmowego dokonują upoważnieni pracownicy Urzędu dysponujący kluczami do obiektu oraz indywidualnymi kodami do alarmu.

Awaryjne zasilanie w energię elektryczną obiektu (cały obiekt Urzędu, w tym elektroniczny system alarmowy) realizowane jest za pomocą agregatu prądotwórczego o mocy 48kW usytuowanego za obiektem Urzędu. Agregat zasilany jest paliwem w postaci oleju napędowego oraz wyposażony w mechanizm autostartu (automatyczne uruchomienie zasilania w przypadku niestabilności/zaniku zasilania z sieci energetycznej operatora energetycznego).

2.2. Opis pomieszczenia, w którym przetwarzane są informacje niejawne.

Pomieszczenie przetwarzania informacji niejawnych znajdują się na piętrze obiektu Urzędu – pomieszczenie przy biurze nr 15, stanowiące pomieszczenie kancelarii niejawnej oraz jednocześnie pomieszczenie systemu TI do przetwarzania informacji niejawnych – BSK.

Pomieszczenie kancelarii niejawnej/BSK jest pomieszczeniem, którego ściany wykonano z pełnych materiałów budowlanych. Nie posiada okien. Drzwi do pomieszczenia niecertyfikowane, pełne, obite obustronnie blachą o grubości 1 mm. Zamki drzwi niecertyfikowane, patentowe. W pomieszczeniu certyfikowana szafa

metalowa klasy A – Konsmetal MS1/A-K (P41/309/2005(1934); P41/315/2005(1940)), służąca do przechowywania materiałów niejawnych.

Dostęp do chronionego pomieszczenia możliwy jedynie poprzez poprzedzające pomieszczenie przechodnie, będące stałym miejscem pracy osoby odpowiedzialnej za prowadzenie ewidencji materiałów niejawnych. W pomieszczeniu tym znajduje się czujka ruchu systemu alarmowego, w jej polu widzenia znajduje się podejście do drzwi pomieszczenia kancelarii niejawnej/BSK. Okno pomieszczenia powyżej 5,5 metra od poziomu gruntu, zabezpieczone kratą z prętów stalowych o średnicy ok. 10mm, wymiary oczka ok. 150x150mm. Okno niecertyfikowane, wykonane z profili PCV. Przed podglądem z zewnątrz zabezpieczają żaluzje pionowe. Drzwi wejściowe do pomieszczenia przechodniego pełne biurowe, niecertyfikowane, zamykane na jeden zamek zwykły z wkładką bębenkową.

3. Procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefach ochronnych.

Z uwagi na publiczny charakter Urzędu oraz jego działalności nie wprowadzono kontroli ruchu osobowego na terenie całego obiektu. Kontrolą dostępu objęto wybrane pomieszczenia i obszary obiektu, w których przetwarzane są informacje niejawne o klauzuli „zastrzeżone". Kontrola dostępu do wymienionego pomieszczenia odbywa się w formie organizacyjnej.

3.1. Osoby uprawnione.

Osoby uprawnione przez Wójta do wejścia i przebywania w pomieszczeniu przetwarzania informacji niejawnych znajdują się na przygotowanej i zatwierdzonej przez Wójta liście osób uprawnionych.

Klucze do pomieszczeń przetwarzania informacji niejawnych wydawane są przez pracownika kancelarii niejawnej a w przypadku jego nieobecności przez Pełnomocnika ds. OIN, osobom uprawnionym przez Wójta do pobrania kluczy, wg zatwierdzonej przez Wójta listy osób uprawnionych. Fakt wydania/zdania klucza podlega odnotowaniu w rejestrze pobranych kluczy do pomieszczeń przetwarzania IN. Rejestr zawiera imię i nazwisko pobierającego, datę i godzinę operacji, podpis pobierającego. W przypadku zdania klucza przyjmujący go w depozyt pracownik uzupełnia wiersz o datę i godzinę zdania klucza oraz potwierdza ten fakt własnym podpisem.

3.2. Osoby nieuprawnione.

Osoby nieuprawnione do samodzielnego przebywania w pomieszczeniu, w którym przetwarzane są informacje niejawne, mogą wejść i przebywać w nim wyłącznie w towarzystwie osób uprawnionych, które to są odpowiedzialne za nadzór nad pobytem osoby nieuprawnionej. Osobami nieuprawnionymi będą interesanci, personel techniczny, sprzątający oraz pozostali pracownicy Urzędu, którzy nie zostali wyznaczeni jako osoby uprawnione. Fakt ich wejścia podlega odnotowaniu w odpowiednim rejestrze.

4. Określenie poziomu zagrożeń.

4.1. Tabela oceny istotności czynników zagrożeń.

	Czynnik	Ocena istotności czynnika			Uzasadnienie
		Bardzo istotny (8 pkt.)	Istotny (4 pkt.)	Mało istotny (1pkt)	
1	Klauzula tajności przetwarzanych informacji niejawnych			1	Urząd przetwarza wyłącznie informacje niejawne o klauzuli **„Zastrzeżone"**
2	Liczba materiałów niejawnych			1	W Urzędzie występuje tylko niewielka liczba dokumentów, wg stanu na koniec 2020 roku:31 dokumentów
3	Postać informacji niejawnych			1	W chwili sporządzenia niniejszego planu wyłącznie forma papierowa w niewielkich ilościach.
4	Liczba osób			1	W Urzędzie zatrudnionych jest obecnie osób 21 z czego poświadczenie bezpieczeństwa posiada 1 osoba (około 4,8% zatrudnionych) i 6 osób upoważnionych jest do dostępu do informacji niejawnych o klauzuli zastrzeżone.
5	Lokalizacja			1	Budynek Urzędu położony jest w centrum miejscowości (posesja otwarta, nieogrodzona).
6	Dostęp osób do budynku		4		Dostęp do budynku w czasie jego pracy dwoma wejściami. Po godzinach pracy obiekt zamknięty i zabezpieczony systemem alarmowym.
7	Inne czynniki:			1	**OGÓŁEM (maksymalna ocena dla czynników od 7.1. do 7.7.)**
7.1.	Działanie obcych służb specjalnych			1	Z uwagi na lokalny charakter działalności Urzędu oraz rodzaj i zakres przetwarzanych informacji niejawnych brak realnych obszarów zainteresowania obcych służb specjalnych.
7.2.	Sabotaż			1	Nie odnotowano w ciągu ostatnich 5 lat prób sabotażu, zjawisko o małym stopniu prawdopodobieństwa.
7.3.	Zamach terrorystyczny			1	Niski poziom prawdopodobieństwa wystąpienia zamachu na ternie Urzędu.
7.4.	Kradzież lub inna działalność przestępcza			1	W okresie ostatnich 5 lat nie odnotowano prób włamań do pomieszczeń zajmowanych przez obie jednostki organizacyjne ani też innych symptomów działalności przestępczej.
7.5.	Pożar			1	Budynek wyposażony w wymagane przepisami urządzenia gaśnicze i środki ochrony ppoż. Na terenie obiektu obowiązuje zakaz palenia. Instalacje objęte regularnymi przeglądami w bardzo dobrym stanie technicznym.
7.6.	Działanie sił przyrody – zagrożenie powodzią, szkody górnicze itp.			1	Siedziba Urzędu nie jest zagrożona żadnymi z wymienionych.

7.7.	Strajki, akcje protestacyjne, próby okupacji budynku			1	W okresie ostatnich 5 lat nie odnotowano przypadków strajków lub akcji protestacyjnych, które mogłyby się wiązać z próbami okupacji budynku Urzędu, a tym samym stwarzać zagrożenie dla znajdujących się w nim informacji niejawnych.
Suma punktów		**11**			

Na podstawie oceny istotności czynników zagrożeń ustalono poziom zagrożeń na poziomie **niskim – 11 punktów.**

Minimalna łączna suma punktów do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich kombinacji środków bezpieczeństwa fizycznego wynosi **2 punkty** (obowiązkowe kategorie: K1+K2+K3=2).

4.2. Punktacja zastosowanych środków bezpieczeństwa fizycznego.

ŚRODEK BEZPIECZEŃSTWA	PKT
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	1
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	1
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3 = 5, 3, 2 lub 1 pkt)	2
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	1

Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	0
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	1
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	2
Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	2
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	0
Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	0
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY=K1+K2+K3+K4+K5+K6	**7**

Wniosek: zastosowane środki bezpieczeństwa fizycznego pozwalają uzyskać minimalną wymaganą liczbę punktów dla ustalonego poziomu zagrożeń (2 pkt) a nawet znacznie je przewyższają.

5. Opis zastosowanych środków bezpieczeństwa fizycznego.

W celu zapewnienia odpowiedniego poziomu ochrony przetwarzanych informacji niejawnych, podjęto lub zastosowano następujące środki:

- Zarządzeniem nr 44/2022/K Wójta Gminy Miedzichowo z dnia 2 grudnia 2022 roku utworzono Pionu Ochrony Informacji Niejawnych w Urzędzie Gminy Miedzichowo - w ramach którego wyznaczono osoby odpowiedzialne za zapewnienie bezpieczeństwa przetwarzanych informacji niejawnych, tj.:

    - pełnomocnika ds. ochrony informacji niejawnych, odpowiedzialnego m.in. za zapewnienie ochrony informacji niejawnych, w tym stosowania środków bezpieczeństwa fizycznego, ochronę systemów teleinformatycznych przetwarzających informacje niejawne, zarządzanie bezpieczeństwem informacji niejawnych; pełnomocnik musi posiadać ważne poświadczenie bezpieczeństwa wydane przez Agencję Bezpieczeństwa Wewnętrznego oraz aktualne – nie starsze niż 5-cio letnie przeszkolenie ABW w zakresie ochrony informacji niejawnych),

    - inspektora bezpieczeństwa teleinformatycznego odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania BSK ze szczególnymi wymaganiami bezpieczeństwa (SWB) oraz przestrzegania procedur bezpiecznej eksploatacji (PBE), posiadającego odpowiednie poświadczenie bezpieczeństwa lub upoważnienie do przetwarzania informacji o klauzuli „zastrzeżone", posiada zaświadczenie potwierdzające odbycie specjalistycznego szkolenia dla inspektorów BTI/administratorów systemów przetwarzających informacje niejawne, organizowane i prowadzone przez DBTI ABW, posiadający aktualne – nie starsze niż 5-cio letnie zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych,

    - administratora systemu teleinformatycznego (pozostający poza pionem ochrony) przetwarzającego informacje niejawne – „Bezpiecznej Stacji Komputerowej", odpowiedzialnego za funkcjonowanie systemu oraz przestrzeganie zasad

i wymagań bezpieczeństwa przewidzianych dla systemu, posiadającego odpowiednie poświadczenie bezpieczeństwa lub upoważnienie do przetwarzania informacji o klauzuli „zastrzeżone", posiada zaświadczenie potwierdzające odbycie specjalistycznego szkolenia dla inspektorów BTI/administratorów systemów przetwarzających informacje niejawne, organizowane i prowadzone przez DBTI ABW, posiadający aktualne –nie starsze niż 5-cio letnie zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych,

- pracownika Urzędu – posiadającego odpowiednie uprawnienia do dostępu do informacji niejawnych (poświadczenie lub upoważnienie, przeszkolenie w zakresie oin) odpowiedzialnego za:

  - prowadzenie urządzeń ewidencyjnych służących rejestrowaniu wszystkich materiałów przetwarzanych w jednostce organizacyjnej – w tym materiałów wpływających do jednostki, materiałów wytwarzanych w jednostce, materiałów wychodzących z jednostki organizacyjnej,

  - przedkładanie do dekretacji pism kierownika jednostki organizacyjnej lub innej uprawnionej osoby, a następnie ich wydawanie wg dekretacji (po weryfikacji aktualności poświadczenia/upoważnienia oraz przeszkolenia w zakresie OIN),

  - odpowiednie, zgodne z rozporządzeniem, oznaczanie i pakowanie przesyłek niejawnych, w celu ich przesłania za pomocą operatora pocztowego,

  - egzekwowanie zwrotu niepotrzebnych do dalszej pracy materiałów niejawnych w celu ich archiwizacji;

- Stosowana jest procedura dopuszczenia do informacji niejawnych osób posiadających odpowiednie uprawnienia w postaci odpowiedniego poświadczenia bezpieczeństwa lub upoważnienia kierownika jednostki organizacyjnej uprawniającego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", posiadających przeszkolenie w zakresie ochrony informacji niejawnych potwierdzone odpowiednim

zaświadczeniem (przeszkolenie realizowane nie rzadziej niż raz na 5 lat), a sam dostęp do określonych materiałów niejawnych odbywa się zgodnie z zasadą „need to know" – dany materiał niejawny jest niezbędny do realizacji zadań na danym stanowisku lub czynności zleconych przez daną osobę;

- Opracowano i wprowadzono do stosowania instrukcję obiegu materiałów niejawnych, zapewniających odpowiedni poziom bezpieczeństwa oraz rozliczalność, zapisy której wykonuje pracownik kancelarii niejawnej oraz osoby przetwarzające informacje niejawne;

- Zgodnie z rozporządzeniem Rady Ministrów z dnia 29 maja 2012 roku w sprawie stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych określony został poziom zagrożeń, wg którego – adekwatnie do ustalonych zagrożeń – wprowadzono środki techniczne i organizacyjne służące fizycznemu zabezpieczeniu przetwarzanych w jednostce informacji niejawnych;

- W ramach wymienionych wyżej zabezpieczeń zastosowano i zorganizowano:

    - system alarmowy z bezpośrednim powiadomieniem do firmy ochrony osób i mienia z reakcją grupy interwencyjnej, obejmujący działaniem ciągi komunikacyjne oraz wybrane pomieszczenia biurowe,

    - pomieszczenie przetwarzania informacji niejawnych objęto organizacyjną kontrolą dostępu zgodnie z przepisami o ochronie informacji niejawnych,

    - pomieszczenia służbowe Urzędu są zamykane (okna i drzwi) każdorazowo po zakończonej pracy, za co odpowiedzialni są użytkownicy danych pomieszczeń.

Ponadto wprowadza się następujące zasady przetwarzania informacji niejawnych:

- Niedopuszczalne jest opuszczenie pomieszczenia służbowego bez uprzedniego odpowiedniego zabezpieczenia materiałów niejawnych przed nieuprawnionym ujawnieniem poprzez zamknięcie w użytkowanej szafie metalowej lub meblu biurowym zamykany na klucz;

- Niedopuszczalne jest opuszczanie pomieszczenia z uruchomionym Bezpiecznym Stanowiskiem w trakcie trwającej edycji dokumentu niejawnego bez uprzedniego zastosowania się do procedur SWB/PBE i odpowiedniego zabezpieczenia zarówno dokumentu jak i stanowiska na czas jego opuszczenia;

- Zabronione jest wynoszenie materiałów niejawnych poza siedzibę Urzędu za wyjątkiem sytuacji osobistego doręczania odpowiednio zapakowanej przesyłki niejawnej do jej adresata (za wiedzą i zgodą kierownika jednostki) lub podjęcia przesyłki przez adresata w siedzibie Urzędu;

- Zabronione jest sporządzanie kopii, odpisów lub wyciągów za pomocą telefonów komórkowych, biurowych urządzeń telekopiowych (fax) lub innych urządzeń teleinformatycznych niebędących częścią akredytowanego systemu teleinformatycznego przetwarzającego informacje niejawne;

- Zabronione jest przetwarzanie informacji niejawnych na stanowiskach komputerowych innych niż Bezpieczna Stacja Komputerowa.

Z uwagi na brak kontroli ruchu osobowego w pozostałych częściach Urzędu, jego pracownicy zobowiązani są:

- zwracać uwagę na nietypowe zachowania osób wchodzących lub przebywających w budynku Urzędu;

- reagować na osoby będące pod wpływem alkoholu lub innych środków odurzających;

- reagować na próby niszczenia, wynoszenia bądź wywożenia mienia z budynku Urzędu;

- reagować na próby wnoszenia do budynku niebezpiecznych przedmiotów, materiałów lub substancji budzących podejrzenie odnośnie ich działania i pochodzenia itp.;

- natychmiast reagować poprzez powiadomienie odpowiednich służb o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

Wszyscy pracownicy Urzędu zobowiązani są do przestrzegania regulaminu pracy, regulaminu BHP, stosowania się do instrukcji ppoż. Odpowiedzialni są za zabezpieczenie pomieszczeń służbowych poprzez zamknięcie drzwi (zamki) i okien po zakończonej pracy oraz wyłączenie wszystkich urządzeń elektrycznych.

6. Procedury zarządzania kluczami do szaf i pomieszczeń, w których przetwarzane są informacje niejawne.

W dyspozycji upoważnionych pracowników Urzędu pozostają dwa rodzaje kluczy:

- Klucze do użytku bieżącego,
- Klucze zapasowe do awaryjnego otwierania pomieszczeń i szaf.

W przypadku zagubienia któregokolwiek klucza lub konieczności jego wymiany, zalecana jest wymiana wkładki zamka drzwi lub wymiana zamka użytkowanej szafy metalowej. W przypadku wymiany wkładki, należy niezwłocznie wymienić klucze zapasowe tak, aby zestawy były właściwe.

Zabronione i niedopuszczalne jest:

- Wynoszenie kluczy do chronionych pomieszczeń i szafy metalowej poza teren Urzędu, za wyjątkiem wyjazdów w czasie pracy w celach służbowych;
- Dorabianie kluczy we własnym zakresie.

6.1. Zarządzanie kluczami do pomieszczenia.

Klucze do użytku bieżącego do pomieszczeń przetwarzania informacji niejawnych wydawane są przez pracownika sekretariatu Wójta, na podstawie listy osób upoważnionych, zatwierdzonej przez kierownika jednostki organizacyjnej. Fakt wydania i przyjęcia klucza odnotowywany jest w odpowiednim rejestrze, zawierającym imię i nazwisko pobierającego, datę i godzinę pobrania klucza, podpis pobierającego. W przypadku zdania osoba odpowiedzialna za wydawanie kluczy uzupełnia wiersz o datę i godzinę zdania oraz potwierdza wpis własnym podpisem.

Klucze zapasowe do chronionego pomieszczenia pozostają w dyspozycji Sekretarza Gminy. Klucze te mogą być użyte na polecenie kierownika jednostki organizacyjnej w sytuacji szczególnej (awarie, ewakuacja, itp.) lub innej osoby uprawnionej do podjęcia merytorycznej decyzji w tym zakresie. Fakt wykorzystania klucza zapasowego winien być odnotowany w rejestrze wydanych/zdanych kluczy do pomieszczenia.

6.2. Zarządzanie kluczami do szafy metalowej do przechowywania BSK oraz szaf do przechowywania informacji niejawnych.

Klucz do użytku bieżącego do szafy metalowej służącej do przechowywania komputera BSK pozostają w dyspozycji pracownika kancelarii niejawnej.

Klucze do mebli biurowych, w których przechowywane są informacje niejawne, pozostają w dyspozycji pracowników, na stanie których znajdują się przechowywane w nich materiały niejawne. Odpowiedzialni są oni za ich należyte zabezpieczenie przed nieuprawnionym dostępem.

W przypadku konieczności otwarcia indywidualnie użytkowanej szafy metalowej/mebla biurowego pod nieobecność użytkownika (awaryjnie lub w celu przekazania dokumentów innej osobie) – czynności należy dokonać komisyjnie a po jej wykonaniu sporządzić protokół komisyjnego otwarcia szafy. Protokół, sporządzony w trzech egzemplarzach, powinien zawierać informacje:

- Informację o dacie i przyczynie wykonania czynności,
- Wykaz zawartości szafy,
- Wykaz dokumentów pobranych z szafy do przekazania nowemu dysponentowi,
- Podpisy członków komisji.

Egzemplarze protokołu otrzymują:

- Kierownik jednostki organizacyjnej,
- Dysponent szafy metalowej poprzez pozostawienie egzemplarza w szafie po jej komisyjnym otwarciu.
- Pracownik prowadzący ewidencję materiałów niejawnych w celu przerejestrowania dokumentu na nową osobę.

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

Osoby odpowiedzialne za bezpieczeństwo przetwarzanych informacji niejawnych (pracownik, w dyspozycji którego materiały niejawne pozostają, pełnomocnik ds. oin, inspektor BTI, administrator BSK, kierownik jednostki organizacyjnej, pracownik odpowiedzialny za prowadzenie ewidencji materiałów niejawnych) winny reagować niezwłocznie na stwierdzone zagrożenia i podejmować działania adekwatne do sytuacji im przeciwdziałające.

W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych pełnomocnik ds. oin na mocy art. 17 ust. 1 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych informuje niezwłocznie kierownika jednostki organizacyjnej o tym fakcie i podejmuje działania zmierzające do ustalenia:

- okoliczności ewentualnego naruszenia,
- osób odpowiedzialnych,
- oszacowania negatywnych skutków naruszenia.

W przypadku np. stwierdzenia braku dokumentu niejawnego szczególnie istotnym jest, czy np. mogło dojść do jego omyłkowego zniszczenia czy też doszło do utraty kontroli nad dokumentem, co skutkować może ujawnieniem informacji niejawnych osobom nieuprawnionym. Równolegle do działań związanych z wyjaśnieniem okoliczności naruszenia podejmuje się działania związane z ograniczeniem skutków ewentualnego nieuprawnionego ujawnienia treści dokumentu, tak by ujawnienie nie miało negatywnego wpływu na planowane działania.

Czynności realizowane w ramach prowadzonych czynności winny być rzetelnie dokumentowane, a ewentualne wyjaśnienia osób należy przyjmować w formie pisemnej. Po zakończeniu czynności pełnomocnik ds. oin sporządza sprawozdanie ze wskazaniem szczegółowych okoliczności naruszenia, zrealizowanych czynności, ustaleń dokonanych w trakcie czynności, treści oświadczeń osób mających wiedzę na temat naruszenia, jego skutków oraz propozycji przeciwdziałania podobnym incydentom w przyszłości. Sprawozdanie przedkładane jest kierownikowi jednostki organizacyjnej celem zapoznania i zatwierdzenia (w szczególności wniosków).

W sytuacji, gdy incydent był skutkiem ujawnienia się zagrożeń, których wcześniej z różnych względów nie wzięto pod uwagę w procesie analizy zagrożeń, należy niezwłocznie przeprowadzić analizę zagrożeń z uwzględnieniem nowego czynnika i podjąć działania przeciwdziałające temu zagrożeniu poprzez uzupełnienie środków ochrony fizycznej o adekwatne środki lub wdrożenie procedur przeciwdziałających.

W przypadku oceny, iż mogło dojść do ujawnienia informacji niejawnej o klauzuli „zastrzeżone" nieuprawnionej osobie lub wątpliwości w tym zakresie, należy rozważyć przesłanie materiałów z ustaleń do właściwiej miejscowo prokuratury celem oceny prawno-karnej, czy nie doszło do popełnienia przestępstwa z art. 266 §2 kodeksu karnego.

8. Bezpieczeństwo teleinformatyczne.

Nadzór w zakresie zapewnienia bezpieczeństwa informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych sprawuje Pełnomocnik ochrony informacji niejawnych oraz inspektor bezpieczeństwa teleinformatycznego (IBTI).

Przetwarzanie informacji niejawnych w Urzędzie Gminy Miedzichowo odbywa się na przygotowanym zgodnie z dokumentacją bezpieczeństwa systemu (SWB/PBE) oraz akredytowanych przez kierownika jednostki organizacyjnej Bezpiecznym Stanowisku do przetwarzania informacji niejawnych z klauzulą „zastrzeżone".

Zasady funkcjonowania i kontroli określone zostały w dokumentacji bezpieczeństwa: „Szczególne Wymagania Bezpieczeństwa (SWB)" i „Procedury Bezpiecznej Eksploatacji (PBE)", z którymi zapoznawany jest każdy użytkownik BSK. Użytkownikiem systemu może być wyłącznie osoba posiadająca odpowiednie poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji o klauzuli „zastrzeżone", przeszkolona w zakresie ochrony informacji niejawnych – potwierdzone odpowiednim zaświadczeniem (nie starsze niż 5-cio letnie).

Ponadto funkcjonowanie w/w systemu teleinformatycznego, na którym przetwarzane są informacje niejawne opiera się na stosownych aktach wewnętrznego kierowania, wydanych przez Wójta, w których uwzględniono i usystematyzowano m. in. informacje dotyczące wyznaczenia osób pełniących funkcje Administratora, Inspektora Bezpieczeństwa Teleinformatycznego oraz zadania i obowiązki przewidziane w dokumentacji bezpieczeństwa, jak również zakres odpowiedzialności wynikający z pełnionej funkcji.

9. Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym w razie wprowadzenia stanów nadzwyczajnych.

Określenie niniejszych norm postępowania z informacjami niejawnymi w razie wystąpienia sytuacji szczególnych oraz wprowadzenia stanów nadzwyczajnych podyktowane jest wymogami *ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (art. 15 ust. 1 pkt 5)* oraz *rozporządzenia Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (§9 ust. 1 pkt 7).*

Rodzaje prawdopodobnych sytuacji szczególnych.

Zgodnie z przyjętymi regulacjami w planie ochrony informacji niejawnych, dokumenty i materiały zawierające/stanowiące informacje niejawne winny być przechowywane w dedykowanej do tego celu szafie metalowej, meblu biurowym zamykanym na klucz (w zależności od klauzuli niejawności, jaki na danym dokumencie został nadany), nawet w sytuacji chwilowego opuszczania przydzielonego pomieszczenia służbowego.

Stopień zabezpieczenia oraz ilość i rodzaj zastosowanych środków ochrony fizycznej informacji niejawnych pomieszczeń oraz Urzędu powinien być adekwatny do ustalonych i ocenionych czynników zagrożeń i spełniać wymaganą minimalną łączną sumę punktów.

Działanie to minimalizuje ryzyko ewentualnego zniszczenia chronionych materiałów w sytuacji innej niż pożar, ponadto znacznie ogranicza ryzyko dostępu do tych informacji przez osoby nieuprawnione w wyniku włamania, aktu wandalizmu, wtargnięcia osoby nieuprawnionej do urzędu czy pomieszczenia w którym przetwarzane są informacje niejawne.

Pełnomocnik ds. ochrony informacji niejawnych na mocy obwiązujących przepisów o ochronie informacji niejawnych jest obowiązany monitorować stale stopień ochrony informacji niejawnych oraz ryzyka z tym związane, w przypadku potrzeby dokonywać zmian w systemie ochrony informacji niejawnych adekwatnie do nowych zagrożeń oraz sytuacji.

Każdorazowo w sytuacjach wymagających podjęcia działań chroniących informacje niejawne, może być zarządzona przez Wójta decyzja o ewakuacji chronionych materiałów z obiektu Urzędu do zapasowego miejsca pracy (ZMP), uzgodnionego miejsca ewakuacji materiałów niejawnych lub innego wskazanego przez kierownika jednostki organizacyjnej (lub osobę upoważnioną) miejsca. Przy zarządzonej ewakuacji stosuje się zasady opisane w informacji o ewakuacji materiałów niejawnych.

Pożar.

Obiekt Urzędu jest obiektem w bardzo dobrym stanie technicznym, którego instalacje poddawane są wymaganym przepisami prawa przeglądom i konserwacjom. Na terenie Urzędu zabronione jest palenie wyrobów tytoniowych. Wyposażenie obiektu w urządzenia i instalacje gaśnicze (gaśnice) jest adekwatne do instalacji użytkowanych w oblekcie (rodzaj środka gaśniczego) oraz zgodne z obowiązującymi przepisami. Mając wymienione czynniki na uwadze, ryzyko wystąpienia pożaru oceniane jest jaki niskie.

W przypadku stwierdzenia pożaru na terenie obiektu (lub jego sąsiedztwie) należy postępować zgodnie z przyjętą w Urzędzie instrukcją przeciwpożarową, a w przypadku jej braku – dążyć do:

- Zgłoszenia na numer alarmowy 112 ,
- Powiadomienie kierownika o pożarze,
- Poinformowania innych osób w obiekcie o zagrożeniu (okrzykiem lub poprzez użycie ROP – ręcznego ostrzegacza pożarowego),
- Podjęcia próby gaszenia źródła ognia przy wykorzystaniu urządzeń i sprzętu gaśniczego będącego na wyposażeniu jednostki.

Jeśli pożarem objęta jest inna część budynku/obiektu i nie ma ryzyka przeniesienia ognia do danego pomieszczenia służbowego oraz sytuacja na to pozwala, a działanie nie rodzi zagrożenia dla życia ludzkiego, należy przetwarzane materiały niejawne schować na czas akcji gaśniczej i czasowej ewakuacji personelu do zamykanego na klucz mebla biurowego lub użytkowanej indywidualnie szafy metalowej oraz zamknąć je na klucz.

Jeśli sytuacja pozwala i nie stwarza zagrożenia dla zdrowia i życia ludzkiego, w uzgodnieniu z kierownikiem jednostki organizacyjnej, można zastosować ewakuację jako działanie zabezpieczające materiały na czas sytuacji szczególnej.

Awaria techniczna skutkująca zalaniem pomieszczeń.

W przypadku wystąpienia awarii technicznej skutkującej zalaniem wodą pomieszczeń należy:

a) W przypadku wycieku wody zimnej (rura wody zimnej zasilająca obiekt lub pomieszczenia, pęknięcie węża zasilającego rezerwuary WC, uszkodzenie pokrycia dachu skutkującego przeciekiem wody deszczowej – niezwłocznie powiadomić kierownika jednostki organizacyjnej oraz pracownika obsługi technicznej obiektu. Jeśli są

dostępne – użyć zaworu zamykającego dopływ wody zimnej w celu ograniczenia skutków awarii.

b) W przypadku wycieku wody ciepłej (z instalacji c.o.) należy zachować szczególną ostrożność z uwagi na wysoką temperaturę wody (55-70°C) istnieje ryzyko poparzenia. Należy powiadomić kierownika jednostki organizacyjnej oraz pracownika obsługi technicznej obiektu, odpowiedzialnego za eksploatowane w obiekcie instalacje wodne.

W przypadku konieczności osuszenia i posprzątania pomieszczenia służbowego, w którym przechowywane są materiału niejawne można w zależności od sytuacji – przenieść je do innej szafy metalowej/zamykanego na klucz mebla biurowego w wyznaczonym pomieszczeniu zastępczym. Jeśli sytuacja nie wymaga czasowego przeniesienia materiałów – personel techniczny usuwający awarię lub personel sprzątający pomieszczenie winien być nadzorowany przez osobę uprawnioną do przebywania w pomieszczeniu lub pełnomocnika ds. oin lub inną wyznaczoną przez kierownika jednostki organizacyjnej osobę.

Z uwagi na bardzo dobry stan obiektu i jego instalacji, ryzyko przedmiotowego zjawiska jest oceniane jako niskie. Jeśli materiały niejawne będą przechowywane w sposób prawidłowy, tzn. zamknięte w szafach metalowych lub meblach biurowych, sytuacja w której uległyby zniszczeniu jest mało prawdopodobna (woda spływać będzie do najniżej położonych punktów obiektu).

Awaria techniczna – zacięcie zamka.

W przypadku awarii wkładki zamka, zamka lub innego mechanizmu ryglującego drzwi do użytkowanej szafy metalowej, mebla biurowego lub pomieszczenia służbowego, skutkującej brakiem możliwości jego otwarcia, należy poinformować kierownika jednostki organizacyjnej oraz personel techniczny obiektu, odpowiedzialny za eksploatację tego typu urządzeń lub zewnętrzny podmiot świadczący usługi ślusarskie w celu awaryjnego otwarcia zamka.

W trakcie pracy personelu technicznego lub zewnętrznego podmiotu należy sprawować nadzór nad pracą tych osób.

Istotna będzie wstępna ocena, czy do awarii zamka mogło dojść samoistnie w skutek np. zużycia, czy też do uszkodzenia zamka doszło w wyniku nieuprawnionej manipulacji mającej na celu jego otwarcie narzędziem innym niż właściwy klucz.

Awaria techniczna – systemu alarmowego

W przypadku stwierdzenia nieprawidłowego działania któregoś z wymienionych systemów niezwłocznie zlecić przeprowadzanie naprawy. Po dokonanej zrealizowanej naprawie przeprowadzić testy skuteczności/poprawnego działania systemu.

Włamanie – akty wandalizmu.

Budynek urzędu chroniony jest systemem alarmowym z powiadomieniem firmy ochroniarskiej. W przypadku wyzwolenia alarmu w określonym czasie powinna dojechać grupa interwencyjna firmy ochroniarskiej, podejmująca dalsze działania w celu ujęcia sprawców, zabezpieczenia obiektu, powiadomienia Policji oraz kierownika jednostki organizacyjnej lub innej osoby upoważnionej.

W przypadku stwierdzenia włamania do obiektu Urzędu, lub aktu wandalizmu połączonego z włamaniem na teren obiektu, należy powiadomić jednostkę Policji o stwierdzonym przestępstwie. W czasie czynności procesowych realizowanych przez funkcjonariuszy Policji należy stosować się do ich poleceń oraz w miarę możliwości dokonać oceny, czy doszło do kradzieży lub zniszczenia materiałów niejawnych przetwarzanych w Urzędzie. W sytuacji stwierdzenia, że doszło do utraty materiałów niejawnych należy podjąć działania zmierzające do ograniczenia możliwych negatywnych skutków ich nieuprawnionego ujawnienia, np. poprzez zmianę zaplanowanych w materiałach działań tak, by ujawnione informacje nie były w stanie zaszkodzić działaniom Urzędu.

Kierownik jednostki organizacyjnej lub inna uprawniona osoba po przybyciu na miejsce i ocenie szkód, podejmuje decyzję w sprawie dalszego postępowania z materiałami niejawnymi.

Powódź o lokalnym charakterze bez ogłoszenia stanu klęski żywiołowej.

W przypadku zagrożenia obiektu powodzią o lokalnym charakterze, należy ściśle współpracować ze służbami odpowiedzialnym za przeciwdziałanie i usuwanie skutków tego typu zjawiska – Straż Pożarna, Policja, Wojsko.

Monitorować sytuację i przeciwdziałać ewentualnemu zagrożeniu poprzez:

- Zabezpieczenie obiektu poprzez ułożenie barier i zapór mających powstrzymać wodę (np. worki z piaskiem),
- Przeniesienie materiałów na wyższe piętra obiektu, z zachowaniem poziomu zabezpieczeń fizycznych (wydzielenie pomieszczeń na czas przeniesienia materiałów do czasu ustąpienia zagrożenia),
- Ewakuację materiałów zgodnie z poleceniami kierownika jednostki organizacyjnej.

Awaria BSK.

W przypadku awarii BSK należy postępować zgodnie z przyjętymi w dokumentacji bezpieczeństwa systemu (SWB/PBE) regułami, w zależności od rodzaju występującej sytuacji awaryjnej i jej skutków.

Postępowanie w przypadku wprowadzenia stanów nadzwyczajnych.

W przypadku wprowadzenia stanu nadzwyczajnego, rozumianego jako szczególny reżim prawny, służący zmniejszeniu skutków szczególnych zagrożeń, wobec których zwykłe środki konstytucyjne okazały się niewystarczające, należy w sposób ciągły i we współpracy z odpowiednimi organami (Policja, Wojsko Polskie, Straż Pożarna, Centrum Zarządzania Kryzysowego) monitorować zagrożenia i dostosowywać na bieżąco poziom zabezpieczeń oraz reguły postępowania – adekwatnie do ustalonych zagrożeń, w szczególności:

- W razie wprowadzenia stanu wojennego – dostosować się do przepisów prawa wydanych w trakcie jego prowadzenia i narzuconych procedur, na bieżąco w uzgodnieniu z odpowiednimi organami monitorować możliwe zagrożenia i odpowiednio im przeciwdziałać (np. poprzez wzmocnienie środków ochrony fizycznej);

- W razie wprowadzenia stanu wyjątkowego – analogicznie jak w sytuacji wprowadzenia stanu wojennego;

- W razie wprowadzenia stanu klęski żywiołowej – monitorować we współpracy z odpowiednimi organami sytuację i podejmować odpowiednie działania (np. przeniesienie dokumentów i materiałów niejawnych, bBSK na wyższe kondygnacje obiektu, tak, by np. w razie trwającej powodzi nie uległy zniszczeniu poprzez zalanie).

Ewakuacja materiałów niejawnych.

W razie ogłoszenia ewakuacji, osoby odpowiedzialne (na których stanie są podlegające ewakuacji materiały niejawne) lub członkowie grupy ewakuacyjnej, powołanej doraźnie przez kierownika jednostki organizacyjnej lub inną uprawnioną osobę, dokonują oddzielenia materiałów podlegających ewakuacji (oznaczonych symbolem „E") i materiałów podlegających zniszczeniu na miejscu w jednostce (oznaczonych symbolem „Z").

Materiały podlegające ewakuacji pakuje się, w zależności od ilości i rodzaju do worków, skrzyń lub innych pojemników zapewniających odpowiedni poziom bezpieczeństwa i zabezpieczających przed nieuprawnionym ujawnieniem, które na czas transportu powinny być zaplombowane w sposób umożliwiający stwierdzenie faktu ich nieuprawnionego otwarcia.

Dokumenty i materiały niejawne, podlegające ewakuacji lub zniszczeniu w przypadku jej zarządzenia znajdują się w pomieszczeniu:

- W pomieszczeniu przy biurze nr 15 – w szafie metalowej -osoba odpowiedzialna Zbigniew Oses – tel. 614410247
  przydzielono worek ewakuacyjny, który znajduje się w pomieszczeniu przy biurze nr 15 (szafa z materiałami niejawnymi)

- W pomieszczeniu przy biurze nr 15 - BSK znajduje się w szafie metalowej osoba odpowiedzialna – Zbigniew Oses – tel. 614410247

Do ewakuacji materiałów niejawnych z uwagi na brak samochodu służbowego wykorzystany zostanie samochód prywatny pracownika kancelarii materiałów niejawnych nr rej. PNT 76550 .

Do niszczenia materiałów niejawnych podlegających zniszczeniu w miejscu pracy „Z" przeznaczona jest niszczarka marki Fellowes 8c klasy P-4 znajdująca się w pomieszczeniu przy biurze nr 15.

Osoba odpowiedzialna za ewakuację materiałów niejawnych – Pełnomocnik ds. ochrony informacji niejawnych – Karolina Łotecka - tel. 614410243 .

W przypadku ewakuacji do zapasowego miejsca pracy (ZMP) ewakuowane materiały podlegają przewiezieniu do wyznaczonego obiektu, tj. Szkoły Podstawowej im. Powstańców Wielkopolskich w Miedzichowie , w pozostałych przypadkach miejsce ewakuacji materiałów wskaże kierownik jednostki organizacyjnej lub inna uprawniona osoba, działająca w jego imieniu.

Pełnomocnik ds. ochrony informacji niejawnych